ABSTRACT

Title of dissertation: INFORMATION-THEORETIC SECRECY IN MULTI-USER CHANNELS

Ersen Ekrem, Doctor of Philosophy, 2012

Dissertation directed by: Professor Şennur Ulukuş
Department of Electrical and Computer Engineering

Inherent openness of the wireless medium imposes stronger challenges on the security of wireless communications. Information-theoretic security addresses these challenges at the physical layer by using tools from wireless communication theory, signal processing and information theory. In information-theoretic security, physical layer communication is intelligently designed to exploit the characteristics of the wireless medium, such as fading, interference, cooperation, and multi-dimensional signaling, in order to provide or improve security. In this dissertation, we study the security of several fundamental wireless network configurations from an information-theoretic perspective.

First, we study the Gaussian multiple-input multiple-output (MIMO) wiretap channel. In this channel, the transmitter sends a common message to both the legitimate user and the eavesdropper. In addition to the common message, a private message is sent only to the legitimate user, which needs to be kept hidden as much as possible from the eavesdropper. We obtain the entire capacity-equivocation region for this channel model. In particular, we show the sufficiency of jointly Gaussian

auxiliary random variables and channel input to evaluate the existing single-letter description of the capacity-equivocation region due to Csiszar-Korner.

Next, we study the secure broadcasting problem, where a transmitter wants to have secure communication with multiple legitimate users in the presence of an external eavesdropper. We study several special cases of the secure broadcasting problem. First, we consider the degraded multi-receiver wiretap channel, and establish its secrecy capacity region. Second, we consider the parallel less noisy multi-receiver wiretap channel, and obtain its common message secrecy capacity and sum secrecy capacity. Third, we consider the parallel degraded multi-receiver wiretap channel for the two-user and two-sub-channel case, and obtain its entire secrecy capacity region. Finally, we consider a parallel channel model with two sub-channels, where the transmitter can use only one of the subchannels at any time, and characterize its secrecy capacity region.

Then, we study the two-user Gaussian MIMO broadcast channel with common and confidential messages. In this channel model, the transmitter sends a common message to both users, and a confidential message to each user which needs to be kept perfectly secret from the other user. We obtain the entire capacity region of this channel. We also explore the connections between this channel model and its non-confidential counterpart, i.e., the Gaussian MIMO broadcast channel with common and private message.

Next, we consider the Gaussian MIMO multi-receiver wiretap channel and obtain its secrecy capacity region for the most general case. We first show that even for the single-input single-output (SISO) case, existing converse techniques

fall short of proving the secrecy capacity region, to emphasize the need for a new proof technique, which we develop by using the relationships between the Fisher information and the differential entropy. Using this new proof technique, we obtain the secrecy capacity region of the degraded MIMO channel. We then establish the secrecy capacity region of the general MIMO channel by using the channel enhancement technique in conjunction with the capacity result we obtained for the degraded MIMO channel. For the general MIMO channel, we show that dirty-paper coding (DPC) combined with stochastic encoding attains the entire secrecy capacity region.

Then, we study the multi-receiver wiretap channel for a more general scenario, where, in addition to confidential messages, the transmitter sends public messages to the legitimate users, on which there are no secrecy constraints. First, we consider the degraded discrete memoryless channel, and obtain inner and outer bounds for the capacity region. These inner and outer bounds match for certain cases, providing the capacity region. Second, we obtain an inner bound for the general discrete memoryless channel by using Marton's inner bound. Third, we consider the degraded Gaussian MIMO channel, and show that jointly Gaussian auxiliary random variables and channel input are sufficient to exhaust the inner and outer bounds. Finally, we provide an inner bound for the capacity region of the general Gaussian MIMO channel.

Next, we focus on the multiple access wiretap (MAC-WT) channel whose capacity region is unknown. We consider a special class of MAC-WT channels which we call the weak eavesdropper class, where each user's link to the legitimate

receiver is stronger than its link to the eavesdropper. For this class of channels, we develop an outer bound for the secrecy capacity region, which partially matches the achievable region in an n-letter form. We evaluate a looser version of our outer bound for the Gaussian case, and show that our outer bound is within 0.5 bits/channel use of the achievable rates along the individual secrecy rates for all weak eavesdropper Gaussian MAC-WT.

Then, we investigate the effects of user cooperation on the secrecy of broadcast channels by considering the cooperative relay broadcast channel (CRBC). We propose an achievable scheme that combines Marton's coding scheme for broadcast channels and Cover and El Gamal's compress-and-forward (CAF) scheme for relay channels. For the Gaussian CRBC, we show that both users can have positive secrecy rates, which is not possible for scalar Gaussian broadcast channels without cooperation.

We further investigate the effects of user cooperation on secrecy by considering the multiple access channel with generalized feedback (MAC-GF), which can be viewed as the MAC-dual of the CRBC. We propose a CAF-based achievable secrecy rate region for the MAC-GF. Specializing our results to a Gaussian MAC-GF, we present numerical results which demonstrate that cooperation can improve secrecy for the MAC-GF.

Next, we study the two-user one-eavesdropper discrete memoryless compound wiretap channel, and provide the best known lower bound for the secrecy capacity of this compound channel. We evaluate this achievable secrecy rate for the Gaussian MIMO case by using DPC. We show that this achievable secrecy rate achieves at

least half of the secrecy capacity of this Gaussian MIMO compound wiretap channel, and also attains the secrecy capacity when the eavesdropper is degraded with respect to one of the two users.

Then, we study the degraded compound multi-receiver wiretap channel (DCMRWC), which, in addition to a group of eavesdroppers, has two groups of users, namely the stronger group and the weaker group. We study two different communication scenarios for this channel. In the first scenario, there is only one eavesdropper, and the transmitter sends a confidential message to each group of legitimate users while keeping both messages secret from the eavesdropper. In the second scenario, we study the DCMRWC with layered messages without any restriction on the number of eavesdroppers. For both scenarios, we obtain the secrecy capacity region for the discrete memoryless channel, the parallel channel, and the Gaussian parallel channel. For the Gaussian MIMO channel, we obtain the secrecy capacity region when there is only one user in the second group.

Next, we study the two-user fading broadcast channel and obtain its ergodic secrecy capacity region. We show that, thanks to fading, both users can have simultaneous secure communication with the transmitter, although this is not possible in the scalar non-fading Gaussian broadcast channel where only one user can have secure communication. This simultaneous secrecy of both users is achieved by an opportunistic communication scheme, in which, at each time instant, the transmitter communicates with the user having a better channel gain.

Then, we study the secure lossy transmission of a vector Gaussian source to a legitimate user in the presence of an eavesdropper, where both the legitimate

user and the eavesdropper have vector Gaussian side information. We obtain an outer bound for the rate, equivocation and distortion region. Moreover, we obtain the maximum equivocation at the eavesdropper when there is no constraint on the transmission rate. By using this maximum equivocation result, we show two facts. First, for this problem, in general, Wyner-Ziv scheme is suboptimal, although, it is optimal in the absence of an eavesdropper. And, second, even when there is no transmission rate constraint, an uncoded transmission scheme is suboptimal; the presence of an eavesdropper necessitates the use of a coded scheme to attain the maximum equivocation.

Finally, we revisit the secure lossy source coding problem. In all works on this problem, either the equivocation of the source at the eavesdropper or the equivocation of the legitimate user's reconstruction of the source at the eavesdropper is used to measure secrecy. We first propose the relative equivocation of the source at the eavesdropper with respect to the legitimate user as a new secrecy measure. We argue that this new secrecy measure is the one that corresponds to the natural generalization of the equivocation in a wiretap channel to the context of secure lossy source coding. Under this new secrecy measure, we provide a single-letter description of the rate, relative equivocation and distortion region, as well as its specializations to degraded and reversely degraded cases. We investigate the relationships between the optimal scheme that attains this region and the Wyner-Ziv scheme.

INFORMATION-THEORETIC SECRECY IN MULTI-USER CHANNELS

by

Ersen Ekrem

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2012

Advisory Committee:
Professor Şennur Ulukuş, Chair/Advisor
Professor Alexander Barg
Professor Armand Makowski
Professor Prakash Narayan
Professor Lawrence C. Washington

DEDICATION

To my father Hasan Ekrem.

ACKNOWLEDGEMENT

First of all, I would like to thank my advisor Professor Şennur Ulukuş providing me the opportunity to do a graduate study, which made this dissertation possible. Throughout five years, she always provided me what I needed. Her support, dedication and availableness eased my path to obtain my results, and gave me courage to pursue my research ideas. Her openness and readiness to listen to me, even to my most non-sense arguments, gave me confidence to express myself. The right amount of freedom she let me in enabled me to strengthen my personality. I am grateful to her for being my advisor.

I would like to thank Professors Alexander Barg, Armand Makowski, Prakash Narayan, and Lawrence C. Washington for being in my dissertation committee and providing me useful comments about my work. I am especially grateful to Professors Prakash Narayan and Armand Makowski for the conversations we had on various topics, which broaden my knowledge and understanding. I also want to thank Professor Adrian Papamarcou for co-teaching an undergraduate probability course with me, which was a useful experience for me.

I would like to thank all members of both Prof. Ulukus' group and CSPL for the nice atmosphere I enjoyed for the last five years. My special thanks go to Alkan Soysal, Wei Kang, Anna Pantelidou, N. Prasanth Anthapadmanabhan, Ravi Tandon, Raef Bassily, Shalab Jain, and Filiz Yeşilköy for their nice company. Besides his friendship, I also thank Ömür Özel for our joint work.

During my graduate studies, I was lucky to make new friends with whom our

friendships will resist against the friction of time and distance. I owe endless thanks to Osman Yağan, with whom, as quoted from him, "we started this journey together", and walked together. I am grateful to him for his unconditional friendship, which goes far beyond being a roommate. I thank Yalın Sağduyu for his sincere friendship, and especially for his help during the last years of my PhD. I thank Himanshu Tyagi for his genuine friendship, and the long conversations that I enjoyed a lot. I thank Berk Gürakan for his sincere friendship, and cheerful company during my stressful last year. I thank Deniz Gündüz for making our annual ISIT gatherings so joyful.

In the last five years, when I got bored with my life at College Park, I always found one of my friends Burak Eskici, Erdal Yılmaz, Onur Özyeşil, Özlem Karadaş, Kıvanç Mıhçak, and Osman Kaytazoğlu ready to listen to me. I thank them for being in my life.

Finally, I thank my mother Fatma Ekrem, my sister Senem Ekrem and my brother-in-law Fehmi Gedik for their unconditional support and love. Without them, there would be no light in my life.

Table of Contents

List of Figures

Chapter 1

Introduction

Information-theoretic secrecy was initiated by Shannon [1], who considered a special case of the now so-called wiretap channel where both the legitimate user and the eavesdropper observe the transmitted signal through noise-free links. Shannon showed that to be able to transmit the message securely to the legitimate user, the transmitter and the legitimate user need to share a secret key whose entropy should be equal to the entropy of the message. In other words, the length of this secret key should be as long as the size of the message, which is too demanding for many communication systems.

After this pessimistic result, Wyner studied a noisy wiretap channel, where the eavesdropper gets a degraded version of the legitimate receiver's observation [2]. For this degraded model, he found the capacity-equivocation region where the equivocation refers to the portion of the message rate that can be delivered to the legitimate receiver, while the eavesdropper is kept totally ignorant of this part. His result uncovered the fact that if the eavesdropper's observation is a degraded version of the legitimate user's observation, information-theoretically secure communication between the transmitter and the legitimate user is possible while keeping the eavesdropper completely ignorant of this secure message, without using any keys.

Later, Wyner's result is generalized to general, not necessarily degraded, wire-

tap channels by Csiszar and Korner [3]. In particular, they considered the general wiretap channel, where there is no presumed degradation order between the legitimate user and the eavesdropper. They found the capacity-equivocation region of this general wiretap channel. Their result proved that even when the eavesdropper is not degraded with respect to the legitimate user, secure communication between the transmitter and the legitimate user is still possible by exploiting the inherent randomness of the channel.

In recent years, information-theoretic secrecy has gained a renewed interest as a methodology to study secure communications over wireless networks. Wireless communication channel brings unique challenges as well as opportunities to the secure communication problem. The inherent openness of the wireless medium makes it easier to launch eavesdropping attacks, as all transmitted signals are overheard at all receivers in the network, due to the broadcast nature of wireless communications. On the other hand, wireless medium provides ample amount of additional randomness, e.g., fading and interference, as well as opportunities for vector communications via multiple antennas, and cooperative communications via overheard signals and relaying, all of which can be utilized for secrecy.

Along this direction, in this dissertation, we study several fundamental multi-user channel models from an information-theoretic secrecy point of view. For each channel model, we either determine the exact capacity region, or provide lower and upper bounds on the capacity region. In the latter case, we investigate the conditions under which these bounds match. In this dissertation, we develop achievable schemes for secure communications and determine achievable rates they provide,

as well as converse techniques to establish secure capacity limits of some network structures. In addition, we develop communication techniques, such as opportunistic communications in fading channels, cooperative relaying in broadcast and multiple access channels, and directional communications in multiple antenna channels, that enable multiple user pairs have simultaneous secure communications.

In Chapter 2, we consider the Gaussian multiple-input multiple-output (MIMO) instance of the wiretap channel. This model consists of a transmitter, a legitimate user, and an eavesdropper. In this channel, the transmitter sends a common message to both the legitimate user and the eavesdropper in addition to a private message which is directed to only the legitimate user. There is a secrecy concern regarding this private message in the sense that the private message needs to be kept secret as much as possible from the eavesdropper. The secrecy of the private message is measured by its equivocation at the eavesdropper.

We obtain the entire capacity-equivocation region of the Gaussian MIMO wiretap channel. This region is known in a single-letter form due to [3]. In Chapter 2, we show that jointly Gaussian auxiliary random variables and channel input are sufficient to evaluate this single-letter description for the capacity-equivocation region of the Gaussian MIMO wiretap channel. We prove the sufficiency of the jointly Gaussian auxiliary random variables and channel input by using channel enhancement [4] and an extremal inequality from [5]. In our proof, we also use the equivalence between the Gaussian MIMO wiretap channel and the Gaussian MIMO wiretap channel with *public* messages [6, Problem 33-c], [7]. In the latter channel model, the transmitter has three messages, a common, a confidential, and a public message.

The common message is sent to both the legitimate user and the eavesdropper, while the confidential and public messages are directed to only the legitimate user. Here, the confidential message needs to be transmitted in perfect secrecy, whereas there is no secrecy constraint on the public message. Since the Gaussian MIMO wiretap channel and the Gaussian MIMO wiretap channel with public messages are equivalent, i.e., there is a one-to-one correspondence between the capacity regions of these two models, in our proof, we obtain the capacity region of the Gaussian MIMO wiretap channel with public messages, which, in turn, gives us the capacity-equivocation region of the Gaussian MIMO wiretap channel.

In Chapter 3, we consider the secure broadcasting problem, where one transmitter wants to have confidential communication with an arbitrary number of users in a broadcast channel, while this communication is being eavesdropped by an external entity. Characterizing the secrecy capacity region of this channel model in its most general form is difficult, because the version of this problem without any secrecy constraints, is the broadcast channel with an arbitrary number of receivers, whose capacity region is unknown. Consequently, to have progress in understanding the limits of secure broadcasting, we resort to studying several special classes of channels, with increasing generality. Precisely, the channel models we consider and the corresponding results we obtain in Chapter 3 are as follows.

First, we consider the degraded multi-receiver wiretap channel with an arbitrary number of users and one eavesdropper, where users are arranged according to a degradedness order, and each user has a less noisy channel with respect to the eavesdropper. We find the secrecy capacity region when each user receives both an

independent message and a common confidential message. Second, we focus on a class of parallel multi-receiver wiretap channels with an arbitrary number of legitimate receivers and an eavesdropper, where in each sub-channel, for any given user, either the user's channel is less noisy with respect to the eavesdropper's channel, or vice versa. We establish the common message secrecy capacity of this channel. Then, we study the scenario where each legitimate receiver wishes to receive an independent message for another sub-class of parallel multi-receiver wiretap channels. For channels belonging to this sub-class, in each sub-channel, there is a less noisiness order which is not necessarily the same for all sub-channels. We find the sum secrecy capacity for this class. Third, we investigate a class of parallel multi-receiver wiretap channels with two sub-channels, two users and one eavesdropper. For the channels in this class, there is a specific degradation order in each sub-channel such that in the first (resp. second) sub-channel the second (resp. first) user is degraded with respect to the first (resp. second) user, while the eavesdropper is degraded with respect to both users in both sub-channels. For this class, we determine the entire secrecy capacity region when each user receives both an independent message and a common message. We discuss the generalization of this result to arbitrary numbers of users and sub-channels. Finally, we consider the parallel multi-receiver wiretap channel with two sub-channels, two users and one eavesdropper, and the degradation order in each sub-channel is exactly the same as in the previous item. However, in this case, the input and output alphabets of one sub-channel are non-intersecting with the input and output alphabets of the other sub-channel, and in addition, we can use only one of these sub-channels at any time. We determine the secrecy capac-

ity region of this channel when the transmitter sends both an independent message to each receiver and a common message to both receivers.

In Chapter 4, we study the two-user Gaussian MIMO broadcast channel, where the transmitter sends a common message to both users, and a confidential message to each user which needs to be kept perfectly secret from the other user. We call the corresponding channel model the Gaussian MIMO broadcast channel with common and confidential messages. We obtain the capacity region of this chanel model. In particular, we show that a variant of the secret dirty-paper coding (S-DPC) scheme proposed in [8] is capacity-achieving. Similar to [8], we also notice an invariance property of this achievable scheme with respect to the encoding order used in the S-DPC scheme. In other words, two achievable rate regions arising from two possible encoding orders used in the S-DPC scheme are identical, and equal to the capacity region. We provide the proof of this statement as well as the converse proof for the capacity region of the Gaussian MIMO broadcast channel with common and confidential messages by using the channel enhancement technique [4] and an extremal inequality from [5].

In Chapter 4, we also explore the connections between the Gaussian MIMO broadcast channel with common and confidential messages and its non-confidential counterpart, i.e., the (two-user) Gaussian MIMO broadcast channel with common and private messages. In the latter model, the transmitter again sends a common message to both users, and a private message to each user, for which there is no secrecy constraint now, i.e., private message of each user does not need to be kept secret from the other user. We note that although there are partial results for

the Gaussian MIMO broadcast channel with common and private messages [9, 10], its capacity region is not known completely. However, in Chapter 4, we are able to obtain the entire capacity region of its confidential version, i.e., of the Gaussian MIMO broadcast channel with common and confidential messages. In Chapter 4, we provide an intuitive explanation of this at-first-sight surprising point as well as the invariance property of the achievable rate region with respect to the encoding orders that can be used in the S-DPC scheme, by using the sum capacity result from [10] for the Gaussian MIMO broadcast channel with common and private messages.

In Chapter 5, we study the Gaussian MIMO multi-receiver wiretap channel, where the transmitter wants to send a confidential message to each legitimate user while there is an external eavesdropper listening to this on-going communication between the transmitter and the legitimate users. We obtain the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel for the most general case. Towards obtaining the secrecy capacity region, we come up with a new technique to evaluate the single-letter descriptions for the (vector) Gaussian models. This new technique uses the Fisher information and the de Bruijn identity (a differential connection between the Fisher information and the differential entropy) to evaluate the single-letter expressions. To be able to present this new technique in a simple setting, in Chapter 5, we first obtain the secrecy capacity region of the Gaussian single-input single-output (SISO) multi-receiver wiretap channel.

After introducing this new technique through the SISO case, we consider the MIMO channel in two main steps: First, we consider the degraded Gaussian MIMO multi-receiver wiretap channel, for which, a single-letter description of the secrecy

capacity region exists due to our results in Chapter 3. At this step, we use our new technique to evaluate this single-letter description and show that superposition coding with Gaussian signals attains the secrecy capacity region of the degraded Gaussian MIMO channel. Next, we consider the non-degraded Gaussian MIMO multi-receiver wiretap channel for which there is no single-letter description of the secrecy capacity region. Despite the lack of such a description, we obtain the secrecy capacity region for the non-degraded case by using the channel enhancement technique [4] in conjunction with the capacity result for the degraded case. In particular, we show that DPC scheme with Gaussian signals can attain the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel.

The proof technique introduced in Chapter 5 can be used in other vector Gaussian network information theory problems. In particular, we use our new technique to provide an alternative proof for the capacity region of the degraded Gaussian MIMO broadcast channel, which was originally proved in [4], and an outer bound for the rate-distortion region of the vector Gaussian CEO problem. We provide the application of our new technique to these vector Gaussian models in Appendix 5.9.7 and Appendix 5.9.8.

In Chapter 6, we study the multi-receiver wiretap channel for a more general scenario than we did in Chapters 3 and 5. In these previous chapters, we consider the multi-receiver wiretap channel for the scenario where the transmitter wants to send a confidential message to each legitimate user. On the other hand, in Chapter 6, we study the multi-receiver wiretap channel with public and confidential messages, in which, the transmitter sends a pair of *public* and *confidential* messages

to each legitimate user. While there are no secrecy concerns on the public messages, confidential messages need to be transmitted in perfect secrecy.

In Chapter 6, we first consider the degraded discrete memoryless multi-receiver wiretap channel and its MIMO instance. We propose inner and outer bounds for its capacity region. Although these inner and outer bounds do not match in general, we show that under certain conditions, these bounds match providing the exact capacity region. For the degraded Gaussian MIMO channel, we evaluate these inner and outer bounds explicitly, and show that it is sufficient to consider jointly Gaussian auxiliary random variables and channel input for the evaluation of both the inner and outer bounds. We prove the sufficiency of Gaussian auxiliary random variables and channel input by using our methodology, that was proposed in Chapter 5 to evaluate the single-letter expressions for vector Gaussian models. Second, we consider the general, not necessarily degraded, discrete memoryless multi-receiver wiretap channel as well as its MIMO instance. For the general, not necessarily degraded, channel, we propose an inner bound for its capacity region by using Marton's inner bound [11], superposition coding, rate-splitting and binning. This inner bound generalizes the inner bound we proposed for the degraded case by using Marton's coding. We evaluate this achievable scheme for the Gaussian MIMO multi-receiver wiretap channel by using DPC [12], and obtain an inner bound for its capacity region.

In Chapter 7, we consider the multiple access wiretap (MAC-WT) channel, in which there is a legitimate multiple access channel whose communication is being listened by an external eavesdropper. In Chapter 7, we study a special class of

MAC-WT channels called the *weak eavesdropper* class. For channels belonging to this class, each user's link to the legitimate receiver is stronger than its link to the eavesdropper. We provide an n-letter outer bound for the secrecy capacity region of channels belonging to this class, which partially matches the achievable region. Then, we consider the weak eavesdropper Gaussian MAC-WT, for which, we evaluate our n-letter outer bound. This evaluation reveals that the gap between our inner and outer bounds is independent of the channel parameters, and is less than 0.5 bits/channel use along individual rate dimensions. Moreover, we show that if the links of users to the legitimate receiver are orthogonal, the gap between our outer bound and inner bound becomes less than 0.5 bits/channel use along all dimensions, i.e., both along the individual rate dimensions and the sum rate line. In Chapter 7, we also show that our outer bound improves the existing our outer bounds for the degraded MAC-WT, which is subsumed by the weak eavesdropper MAC-WT.

In addition, we note in Chapter 7 that the weak eavesdropper MAC-WT resembles the interference wiretap channel (IC-WT) which consists of an ordinary interference channel (IC) and an eavesdropper listening to the ongoing communication on this IC. The similarity between the IC-WT with *very strong* interference among the users and the weak eavesdropper Gaussian MAC-WT with orthogonal components enables us to adapt our outer bound technique we used for the MAC-WT to the IC-WT, and consequently, to get an outer bound for the secrecy capacity region of the IC-WT.

In Chapters 8 and 9, we study the interaction between cooperation and secrecy, more precisely the effects of cooperation on secrecy. Since it is well-known

that cooperation improves the users' throughput in a typical wireless medium, by studying the effects of cooperation on secrecy, we aim to understand whether it improves secrecy as well, i.e., whether there is a parallelism or trade-off between cooperation and secrecy.

For that purpose, in Chapter 8, we consider the cooperative relay broadcast channel (CRBC) where there is a broadcast channel with receivers that are able to cooperate with each other. Although these users cooperate with each other, for the secrecy of their messages, they treat each other as an eavesdropper. In other words, users in the system are untrusted (since each one can eavesdrop on the other one), however, not malicious (since users cooperate). We provide an achievable secrecy rate region by using the compress-and-forward (CAF) scheme for the CRBC. We then evaluate this region for the Gaussian CRBC to demonstrate that, in fact, there is a parallelism between cooperation and secrecy, in the sense that, by cooperating, users can improve their individual secrecy rates. In particular, we show that by means of cooperation, both users can have secure communication with the transmitter in a Gaussian CRBC, although this is not possible without cooperation, i.e., in the underlying Gaussian broadcast channel. Hence, this Gaussian example shows that a synergy between cooperation and secrecy can be generated by using CAF as the cooperative strategy.

In Chapter 9, we consider the multiple access dual of the CRBC to study the effects of cooperation on secrecy to determine whether the synergy between user cooperation and secrecy we observe for the CRBC can be created in a multiple access setting as well. In particular, we study the multiple access channel with generalized

feedback (MAC-GF), where the users can cooperate through the feedback links they have. Similar to the CRBC setting, in this model also, users cooperate with each other, although they do not trust each other, and hence, each user treats the other as an eavesdropper. For the MAC-GF, we propose an achievable secrecy rate region relying on the CAF scheme, and evaluate it for the Gaussian MAC-GF. This evaluation for Gaussian channels shows that although, without cooperation, the users cannot have simultaneous secure communication with the receiver, by means of cooperation, simultaneous secrecy for both users is possible. Hence, this result implies that, in the MAC-GF also, a synergy can be created between user cooperation and secrecy.

In Chapter 10, we study the compound wiretap channel, in which, the transmitter wants to multicast a single confidential message to a group of legitimate users in the presence of a group of eavesdroppers. We first consider the two-user one-eavesdropper discrete memoryless compound wiretap channel and propose a lower bound for its secrecy capacity by using indirect decoding [13] and Marton's inner bound for discrete memoryless broadcast channels [11]. This lower bound is the best known lower bound for the secrecy capacity of the two-user one-eavesdropper compound wiretap channel. We next consider the Gaussian MIMO instance of the aforementioned compound wiretap channel, and propose an achievable secrecy rate by using DPC [12] in the achievable scheme we obtained for the discrete memoryless channel. We address the tightness of the resulting achievable secrecy rate by showing that it can achieve at least half of the secrecy capacity. We also consider a special class of two-user one-eavesdropper Gaussian MIMO compound wiretap

channels, where the eavesdropper is degraded with respect to one of the two users. We obtain the secrecy capacity for this class of channels as the minimum of the secrecy capacities of the two underlying wiretap channels in the compound wiretap channel.

In Chapter 11, we generalize the compound wiretap channel we studied in Chapter 10 to a multi-user setting by incorporating multiple groups of legitimate users, each group getting a different confidential message from the transmitter. In particular, we introduce the degraded compound multi-receiver wiretap channel (DCMRWC) which consists of two groups of users and a group of eavesdroppers. DCMRWC exhibits a certain degradation order such that an arbitrary user from each group and an arbitrary eavesdropper satisfy a certain Markov chain. We consider two different communication scenarios for the DCMRWC: In the first scenario, the transmitter sends a confidential message to the users in the first group, and a different confidential message to the users in the second group, where both messages need to be kept confidential from the eavesdroppers. In the second scenario, the transmitter sends a confidential message to the users in the first group which needs to be kept confidential from the users in the second group and the eavesdroppers. Moreover, the transmitter sends a different confidential message to the users in the second group, which needs to be kept confidential from the eavesdroppers.

For the first scenario, we assume that there exists only one eavesdropper and obtain the secrecy capacity region in a single-letter form. Then, we specialize this single-letter form to the parallel DCMRWC by establishing the optimality of independent signaling in each sub-channel. We evaluate the corresponding secrecy

capacity region for the Gaussian parallel DCMRWC by showing the optimality of jointly Gaussian auxiliary random variables and channel input. Finally, we obtain the secrecy capacity region of the Gaussian MIMO DCMRWC when there is only one user in the second group by again showing the optimality of jointly Gaussian distribution for auxiliary random variables and channel inputs. For the second scenario also, we obtain the secrecy capacity region in a single-letter form for a general discrete memoryless setting. Then, we specialize this single-letter form to the parallel DCMRWC by showing the optimality of independent signaling in each sub-channel. We evaluate the resulting secrecy capacity region for the Gaussian parallel DCMRWC by showing the optimality of jointly Gaussian distribution for auxiliary random variables and channel inputs. Finally, we establish the secrecy capacity region of the Gaussian MIMO DCMRWC when there is only one user in the second group by again proving the optimality of jointly Gaussian auxiliary random variables and channel inputs.

In Chapter 12, we consider the two-user fading broadcast channel with confidential messages where the transmitter sends a confidential message to each user that needs to be kept hidden from the other user. Towards obtaining the secrecy capacity region of this channel, we first consider the parallel broadcast channel with less noisy sub-channels, where in each sub-channel, one of the users' channel is less noisy with respect to the other user. We establish the secrecy capacity region of this channel for the case where the transmitter sends a common message to both users and an individual confidential message to each user. Next, using this capacity result, we obtain the secrecy capacity region of the parallel Gaussian broadcast channel.

Finally, noting that the fading Gaussian broadcast channel is equivalent to a parallel Gaussian broadcast channel from an ergodic capacity perspective, we explicitly evaluate the ergodic secrecy capacity region of the fading broadcast channel. This result demonstrates that, thanks to fading, the transmitter can have secure communication with both users simultaneously, although this is not possible without fading. This simultaneous secrecy can be achieved by an opportunistic communication scheme, in which, at each time instant, the transmitter sends the message of the user having a stronger channel gain.

In Chapter 13, we study the secure lossy transmission of a vector Gaussian source, when both the legitimate user and the eavesdropper have vector Gaussian side information. In this model, the transmitter wants to enable the legitimate user to reconstruct the source within a distortion level while keeping the equivocation of the source at the eavesdropper as high as possible. A single-letter characterization of the rate-equivocation region for this setting is given in [14]. We obtain an outer bound for the rate-equivocation region by optimizing the rate and equivocation constraints separately. As a consequence of these separate optimizations, we obtain the maximum achievable equivocation at the eavesdropper when there is no rate constraint on the transmitter to describe the source to the legitimate user. We show that even in the absence of a rate constraint on the transmitter, the transmitter still needs to use a coded scheme to obtain the maximum equivocation by showing the strict sub-optimality of uncoded schemes. Finally, by further studying the maximum equivocation result we obtained, we show that in general, Wyner-Ziv coding, which is optimal in the absence of an eavesdropper, is strictly sub-optimal for the vector

Gaussian model, since it cannot yield the maximum equivocation. In other words, the presence of an eavesdropper necessitates more sophisticated coding schemes than the Wyner-Ziv scheme.

In Chapter 14, we revisit the secure lossy source coding problem that we consider in Chapter 13, and reformulate the problem by defining the *relative* equivocation of the source at the eavesdropper with respect to the legitimate user as the secrecy measure. In previous works, the equivocation of the source at the eavesdropper is used as the secrecy measure, as a direct generalization of the one used for the wiretap channel [2, 3], where secrecy is measured by the equivocation of the message at the eavesdropper. However, in a wiretap channel, since the message is decoded at the legitimate user, the equivocation of the message at the legitimate user is zero, and hence, the equivocation of the message at the eavesdropper and the relative equivocation of the source at the eavesdropper with respect to the legitimate user are equivalent; both measuring the relative confusion of the eavesdropper. On the other hand, in the secure *lossy* source coding problem, since the legitimate user does not reconstruct the source in a lossless fashion, the equivocation of the source at the legitimate user is not necessarily zero, and consequently, there is no such equivalence between the equivocation and the relative equivocation.

Motivated by these observations, in Chapter 14, we propose the relative equivocation of the source as the secrecy measure for the secure lossy source coding problem, and obtain the corresponding rate, relative equivocation and distortion region in a single-letter form. In addition, we provide specializations of this single-letter description to the degraded and reversely degraded cases. Finally, we show that

Wyner-Ziv scheme is not optimal in general, although it is optimal for the degraded and reversely degraded cases as well as in the absence of an eavesdropper.

In Chapter 15, we provide conclusions of this dissertation.

Chapter 2

Capacity-Equivocation Region of the Gaussian MIMO Wiretap Channel

2.1 Introduction

In this chapter, we consider the Gaussian MIMO wiretap channel, which consists of a transmitter, a legitimate user, and an eavesdropper. In this channel, the transmitter sends a common message to both the legitimate user and the eavesdropper in addition to a private message which is directed to only the legitimate user. There is a secrecy concern regarding this private message in the sense that the private message needs to be kept secret as much as possible from the eavesdropper. The secrecy of the private message is measured by its equivocation at the eavesdropper.

Here, we consider the entire capacity-equivocation region of the Gaussian MIMO wiretap channel. This region contains all achievable rate triples (R_0, R_1, R_e), where R_0 denotes the common message rate directed to both the legitimate user and the eavesdropper, R_1 denotes the private message rate directed to only the legitimate user, and R_e denotes the private message's equivocation (secrecy) rate.

Our result generalizes several previous partial results on the capacity-equivocation region of the Gaussian MIMO wiretap channel. In particular, our result subsumes the following previous findings about the capacity-equivocation region of the Gaus-

sian MIMO wiretap channel: i) The secrecy capacity of this channel, i.e., $\max R_1$ when $R_0 = 0, R_e = R_1$, is obtained in [15, 16] for the general case, and in [17] for the 2-2-1 case. ii) The common and confidential rate region under perfect secrecy, i.e., (R_0, R_1) region with $R_e = R_1$, is obtained in [18]. iii) The capacity-equivocation region without a common message, i.e., (R_1, R_e) region with $R_0 = 0$, is obtained in [7]. iv) The capacity region of the Gaussian MIMO broadcast channel with degraded message sets without a secrecy concern, i.e., (R_0, R_1) region with no consideration on R_e, is obtained in [9]. Here, we obtain the entire (R_0, R_1, R_e) region. Our result as well as the previous results listed above hold when there is a covariance constraint on the channel input as well as when there is a total power constraint on the channel input.

2.2 Discrete Memoryless Wiretap Channels

The discrete memoryless wiretap channel consists of a transmitter, a legitimate user and an eavesdropper; see Figure 2.1. The channel transition probability is denoted by $p(y, z|x)$, where $x \in \mathcal{X}$ is the channel input, $y \in \mathcal{Y}$ is the legitimate user's observation, and $z \in \mathcal{Z}$ is the eavesdropper's observation. We consider the following scenario for the discrete memoryless wiretap channel: The transmitter sends a common message to both the legitimate user and the eavesdropper, and a private message to the legitimate user which is desired to be kept hidden as much as possible from the eavesdropper.

An $(n, 2^{nR_0}, 2^{nR_1})$ code for this channel consists of two message sets $\mathcal{W}_0 =$

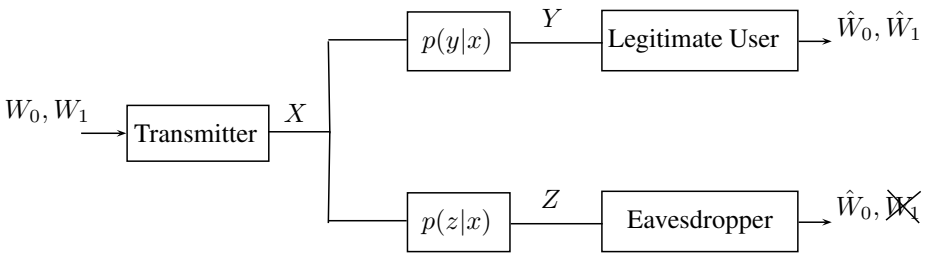

Figure 2.1: The wiretap channel.

$\{1, \ldots, 2^{nR_0}\}$, $\mathcal{W}_1 = \{1, \ldots, 2^{nR_1}\}$, one encoder at the transmitter $f : \mathcal{W}_0 \times \mathcal{W}_1 \to \mathcal{X}^n$, one decoder at the legitimate user $g_u : \mathcal{Y}^n \to \mathcal{W}_0 \times \mathcal{W}_1$, and one decoder at the eavesdropper $g_e : \mathcal{Z}^n \to W_0$. The probability of error is defined as $P_e^n = \max\{P_{e,u}^n, P_{e,e}^n\}$, where $P_{e,u}^n = \Pr[g_u(Y^n) \neq (W_0, W_1)], P_{e,e}^n = \Pr[g_e(Z^n) \neq W_0]$, and W_j is a uniformly distributed random variable in $\mathcal{W}_j$, $j = 0, 1$. We note that W_0 corresponds to the common message that is transmitted to both the legitimate user and the eavesdropper, and W_1 denotes the private message sent only to the legitimate user, on which there is a secrecy constraint. The secrecy of the legitimate user's private message is measured by its equivocation at the eavesdropper [2, 3], i.e.,

$$\frac{1}{n} H(W_1|W_0, Z^n) \tag{2.1}$$

A rate triple (R_0, R_1, R_e) is said to be achievable if there exists an $(n, 2^{nR_0}, 2^{nR_1})$ code such that $\lim_{n\to\infty} P_e^n = 0$, and

$$R_e \leq \lim_{n\to\infty} \frac{1}{n} H(W_1|W_0, Z^n) \tag{2.2}$$

The capacity-equivocation region of the discrete memoryless wiretap channel is defined as the convex closure of all achievable rate triples (R_0, R_1, R_e), and denoted by $\mathcal{C}$. The capacity-equivocation region of the discrete memoryless wiretap channel, which is obtained in [3], is stated in the following theorem.

Theorem 2.1 ([3, Theorem 1]) *The capacity-equivocation region of the discrete memoryless wiretap channel $\mathcal{C}$ is given by the union of rate triples (R_0, R_1, R_e) satisfying*

$$0 \leq R_e \leq R_1 \tag{2.3}$$

$$R_e \leq I(V;Y|U) - I(V;Z|U) \tag{2.4}$$

$$R_0 + R_1 \leq I(V;Y|U) + \min\{I(U;Y), I(U;Z)\} \tag{2.5}$$

$$R_0 \leq \min\{I(U;Y), I(U;Z)\} \tag{2.6}$$

for some U, V, X such that

$$U \to V \to X \to (Y, Z) \tag{2.7}$$

We next provide an alternative description for $\mathcal{C}$. This alternative description will arise as the capacity region of a different, however related, communication scenario for the discrete memoryless wiretap channel. In this communication scenario, the transmitter has three messages, W_0, W_p, W_s, where W_0 is the common message sent to both the legitimate user and the eavesdropper, W_p is the public message sent only to the legitimate user on which there is no secrecy constraint, and W_s is

the confidential message sent only to the legitimate user in perfect secrecy. In this scenario, since W_s needs to be transmitted in perfect secrecy, it needs to satisfy the following condition

$$\lim_{n\to\infty} \frac{1}{n} I(W_s; Z^n, W_0) = 0 \tag{2.8}$$

As we noted before, unlike W_s, there is no secrecy constraint on the *public* message W_p. We also note that the perfect secrecy on a message is attained when the equivocation of this message is equal to its rate, i.e., when we have $R_e = R_s$, which can be seen by comparing (2.2) and (2.8). To distinguish this communication scenario from the previous one, we call the channel model arising from this scenario the discrete memoryless wiretap channel with *public* messages. We note that this alternative description for wiretap channels has been previously considered in [6, Problem 33-c], [7].

An $(n, 2^{nR_0}, 2^{nR_p}, 2^{nR_s})$ code for this scenario consists of three message sets $\mathcal{W}_0 = \{1, \ldots, 2^{nR_0}\}, \mathcal{W}_p = \{1, \ldots, 2^{nR_p}\}, \mathcal{W}_s = \{1, \ldots, 2^{nR_s}\}$, one encoder at the transmitter $f : \mathcal{W}_0 \times \mathcal{W}_p \times \mathcal{W}_s \to \mathcal{X}^n$, one decoder at the legitimate user $g_u : \mathcal{Y}^n \to \mathcal{W}_0 \times \mathcal{W}_p \times \mathcal{W}_s$, and one decoder at the eavesdropper $g_e : \mathcal{Z}^n \to \mathcal{W}_0$. The probability of error is defined as $P_e^n = \max\{P_{e,u}^n, P_{e,e}^n\}$, where $P_{e,u}^n = \Pr[g_u(Y^n) \neq (W_0, W_p, W_s)]$ and $P_{e,e}^n = \Pr[g_e(Z^n) \neq W_0]$. A rate triple (R_0, R_p, R_s) is said to be achievable if there exists an $(n, 2^{nR_0}, 2^{nR_p}, 2^{nR_s})$ code such that $\lim_{n\to\infty} P_e^n = 0$ and (2.8) is satisfied. The capacity region $\mathcal{C}_p$ of the discrete memoryless wiretap channel with *public* messages is defined as the convex closure of all achievable rate triples

(R_0, R_p, R_s). The following lemma establishes the equivalence between $\mathcal{C}$ and $\mathcal{C}_p$.

Lemma 2.1 *$(R_0, R_p, R_s) \in \mathcal{C}_p$ iff $(R_0, R_s + R_p, R_s) \in \mathcal{C}$.*

The proof of this lemma is given in Appendix 2.7.1. This proof consists of two steps. In the first step, we note that if $(R_0, R_p, R_s) \in \mathcal{C}_p$, then in the corresponding achievable scheme attaining this rate triple, we can combine the messages W_s, W_p to obtain $W_1 = (W_s, W_p)$, whose equivocation will be as least R_s due to the perfect secrecy requirement on W_s. Hence, this argument proves the inclusion $\mathcal{C}_p \subseteq \mathcal{C}$. In the second step, we show the reverse inclusion $\mathcal{C} \subseteq \mathcal{C}_p$. To this end, we consider the achievable scheme that attains the entire region $\mathcal{C}$, and call this achievable scheme the optimal achievable scheme. If the rate triple $(R_0, R_1, R_e) \in \mathcal{C}$, in the corresponding optimal achievable scheme, the private message W_1 can be divided into two parts $W_1 = (\tilde{W}_p, \tilde{W}_s)$ where the rate of $\tilde{W}_s$ is sufficiently close to R_e and satisfies the perfect secrecy requirement. Hence, this argument shows that $(R_0, R_1 - R_e, R_e) \in \mathcal{C}_p$, i.e., $\mathcal{C} \subseteq \mathcal{C}_p$; completing the proof of Lemma 2.1. Using Lemma 2.1 and Theorem 2.1, we can express $\mathcal{C}_p$ as stated in the following theorem.

Theorem 2.2 *The capacity region of the discrete memoryless wiretap channel with public messages $\mathcal{C}_p$ is given by the union of rate triples (R_0, R_p, R_s) satisfying*

$$0 \leq R_s \leq I(V;Y|U) - I(V;Z|U) \tag{2.9}$$

$$R_0 + R_p + R_s \leq I(V;Y|U) + \min\{I(U;Y), I(U;Z)\} \tag{2.10}$$

$$R_0 \leq \min\{I(U;Y), I(U;Z)\} \tag{2.11}$$

for some (U, V, X) *such that*

$$U \to V \to X \to (Y, Z) \tag{2.12}$$

2.3 Gaussian MIMO Wiretap Channel

The Gaussian MIMO wiretap channel is defined by, see Figure 2.2,

$$\mathbf{Y} = \mathbf{H}_Y \mathbf{X} + \mathbf{N}_Y \tag{2.13}$$

$$\mathbf{Z} = \mathbf{H}_Z \mathbf{X} + \mathbf{N}_Z \tag{2.14}$$

where the channel input $\mathbf{X}$ is a $t \times 1$ vector, $\mathbf{Y}$ is an $r_Y \times 1$ column vector denoting the legitimate user's observation, $\mathbf{Z}$ is an $r_Z \times 1$ column vector denoting the eavesdropper's observation, $\mathbf{H}_Y, \mathbf{H}_Z$ are the channel gain matrices of sizes $r_Y \times t, r_Z \times t$, respectively, and $\mathbf{N}_Y, \mathbf{N}_Z$ are Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_Y, \mathbf{\Sigma}_Z$[1], respectively, which are assumed to be strictly positive-definite, i.e., $\mathbf{\Sigma}_Y \succ \mathbf{0}, \mathbf{\Sigma}_Z \succ \mathbf{0}$. We consider a covariance constraint on the channel input as follows

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{2.15}$$

where $\mathbf{S} \succeq \mathbf{0}$. The capacity-equivocation region of the Gaussian MIMO wiretap channel is denoted by $\mathcal{C}(\mathbf{S})$ which contains all achievable rate triples (R_0, R_1, R_e). The main result of this paper is the characterization of the capacity-equivocation

[1]Without loss of generality, we can set $\mathbf{\Sigma}_Y = \mathbf{\Sigma}_Z = \mathbf{I}$. However, we let $\mathbf{\Sigma}_Y, \mathbf{\Sigma}_Z$ be arbitrary for ease of presentation.

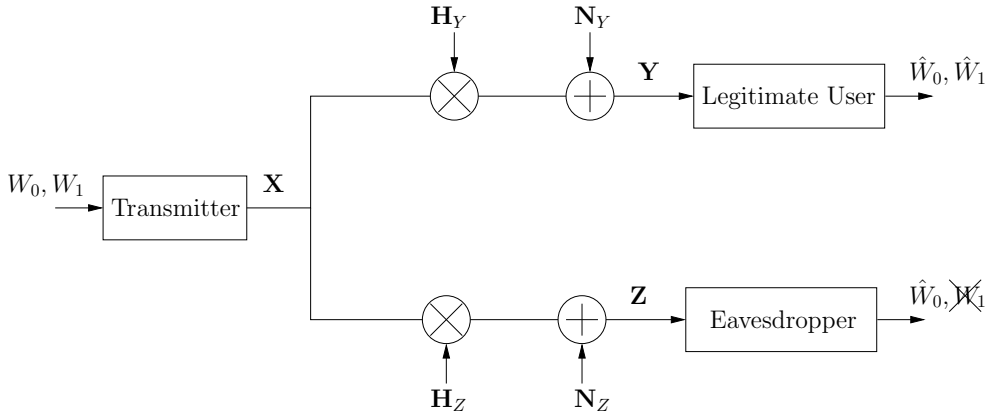

Figure 2.2: The Gaussian MIMO wiretap channel.

region $\mathcal{C}(\mathbf{S})$ which is stated in the following theorem.

Theorem 2.3 *The capacity-equivocation region of the Gaussian MIMO wiretap channel* $\mathcal{C}(\mathbf{S})$ *is given by the union of rate triples* (R_0, R_1, R_e) *satisfying*

$$0 \leq R_e \leq \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{2.16}$$

$$\begin{aligned} R_0 + R_1 \leq{}& \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} \\ &+ \min\left\{\frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \end{aligned} \tag{2.17}$$

$$R_0 \leq \min\left\{\frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \tag{2.18}$$

for some positive semi-definite matrix $\mathbf{K}$ *such that* $\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}$.

Similar to what we did in the previous section, we can establish an alternative statement for Theorem 2.3 by considering the Gaussian MIMO wiretap channel with *public* messages, where the legitimate user's private message is divided into two parts such that one part (confidential message) needs to be transmitted in perfect secrecy

and there is no secrecy constraint on the other part (public message). The capacity region for this alternative scenario is denoted by $\mathcal{C}_p(\mathbf{S})$. We note that Lemma 2.1 provides a one-to-one connection between the capacity regions $\mathcal{C}$ and $\mathcal{C}_p$, and this equivalence can be extended to the capacity regions $\mathcal{C}(\mathbf{S})$ and $\mathcal{C}_p(\mathbf{S})$ by incorporating the covariance constraint on the channel input in the proof of Lemma 2.1. Thus, using Lemma 2.1 and Theorem 2.3, $\mathcal{C}_p(\mathbf{S})$ can be obtained as follows.

Theorem 2.4 *The capacity region of the Gaussian MIMO wiretap channel with public messages $\mathcal{C}_p(\mathbf{S})$ is given by the union of rate triples (R_0, R_p, R_s) satisfying*

$$0 \leq R_s \leq \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{2.19}$$

$$\begin{aligned} R_0 + R_p + R_s \leq{}& \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} \\ &+ \min\left\{\frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \end{aligned} \tag{2.20}$$

$$R_0 \leq \min\left\{\frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{S}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \tag{2.21}$$

for some positive semi-definite matrix $\mathbf{K}$ such that $\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}$.

We next define a sub-class of Gaussian MIMO wiretap channels called the aligned Gaussian MIMO wiretap channel, which can be obtained from (2.13)-(2.14) by setting $\mathbf{H}_Y = \mathbf{H}_Z = \mathbf{I}$,

$$\mathbf{Y} = \mathbf{X} + \mathbf{N}_Y \tag{2.22}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{2.23}$$

In this work, we first prove Theorems 2.3 and 2.4 for the aligned Gaussian MIMO wiretap channel. Then, we establish the capacity region for the general channel model in (2.13)-(2.14) by following the analysis in Section V.B of [4] and Section 7.1 of [19] in conjunction with the capacity result we obtain for the aligned channel.

2.3.1 Capacity Region under a Power Constraint

We note that the covariance constraint on the channel input in (2.15) is a rather general constraint that subsumes the average power constraint

$$E\left[\mathbf{X}^{\top}\mathbf{X}\right] = \mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^{\top}\right]\right) \leq P \tag{2.24}$$

as a special case, see Lemma 1 and Corollary 1 of [4]. Therefore, using Theorem 2.3, the capacity-equivocation region arising from the average power constraint in (2.24), $\mathcal{C}(P)$, can be found as follows.

Corollary 2.1 *The capacity-equivocation region of the Gaussian MIMO wiretap channel subject to an average power constraint P, $\mathcal{C}(P)$, is given by the union of*

rate triples (R_0, R_1, R_e) *satisfying*

$$0 \leq R_e \leq \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_1\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{K}_1\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{2.25}$$

$$\begin{aligned} R_0 + R_1 \leq{}& \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_1\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} \\ &+ \min\left\{\frac{1}{2}\log\frac{|\mathbf{H}_Y(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}_1\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \frac{1}{2}\log\frac{|\mathbf{H}_Z(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}_1\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \end{aligned} \tag{2.26}$$

$$R_0 \leq \min\left\{\frac{1}{2}\log\frac{|\mathbf{H}_Y(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}{|\mathbf{H}_Y\mathbf{K}_1\mathbf{H}_Y^\top + \mathbf{\Sigma}_Y|}, \frac{1}{2}\log\frac{|\mathbf{H}_Z(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z\mathbf{K}_1\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}\right\} \tag{2.27}$$

for some positive semi-definite matrices $\mathbf{K}_1, \mathbf{K}_2$ *such that* $\mathrm{tr}(\mathbf{K}_1 + \mathbf{K}_2) \leq P$.

2.4 Proof of Theorem 2.3 for the Aligned Case

Instead of proving Theorem 2.3, here we prove Theorem 2.4, which implies Theorem 2.3 due to Lemma 2.1. Achievability of the region given in Theorem 2.4 can be shown by setting $\mathbf{V} = \mathbf{X}$ in Theorem 2.2, and using jointly Gaussian $(\mathbf{U}, \mathbf{X} = \mathbf{U}+\mathbf{T})$, where $\mathbf{U}, \mathbf{T}$ are independent Gaussian random vectors with covariance matrices $\mathbf{S}-\mathbf{K}, \mathbf{K}$, respectively. In the rest of this section, we provide the converse proof. To this end, we note that since $\mathcal{C}_p(\mathbf{S})$[2] is convex by definition, it can be characterized

[2]Although $\mathcal{C}_p(\mathbf{S})$ is originally defined for the general, *not necessarily aligned*, Gaussian wiretap channel with public messages, here we use $\mathcal{C}_p(\mathbf{S})$ to denote the capacity region of the *aligned* Gaussian MIMO wiretap channel with public messages as well.

by solving the following optimization problem[3]

$$f(R_0^*) = \max_{(R_0^*,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad \mu_p R_p + \mu_s R_s \tag{2.29}$$

for all $\mu_p \in [0,\infty), \mu_s \in [0,\infty)$, and all possible common message rates R_0^*, which is bounded as follows

$$0 \leq R_0^* \leq \min\{C_Y(\mathbf{S}), C_Z(\mathbf{S})\} \tag{2.30}$$

where $C_Y(\mathbf{S}), C_Z(\mathbf{S})$ are the single-user capacities for the legitimate user and the eavesdropper channels, respectively, i.e.,

$$C_Y(\mathbf{S}) = \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} \tag{2.31}$$

$$C_Z(\mathbf{S}) = \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{2.32}$$

[3]Although characterizing $\mathcal{C}_p(\mathbf{S})$ by solving the following optimization problem

$$\max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \mu_0 R_0 + \mu_p R_p + \mu_s R_s \tag{2.28}$$

for all μ_0, μ_p, μ_s seems to be more natural, we find working with (2.29) more convenient. Here, we characterize $\mathcal{C}_p(\mathbf{S})$ by solving (2.29) for all μ_p, μ_s, for all fixed feasible R_0^*.

We note that the optimization problem in (2.29) can be expressed in the following more explicit form

$$f(R_0^*) = \max_{\substack{U \to V \to \mathbf{X} \to (\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}}} \quad \mu_p R_p + \mu_s R_s \tag{2.33}$$

$$\text{s.t.} \begin{cases} 0 \le R_s & \le & I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U) \\ R_0^* + R_p + R_s & \le & I(V;\mathbf{Y}|U) + \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} \\ R_0^* & \le & \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} \end{cases} \tag{2.34}$$

We also consider the Gaussian rate region $\mathcal{R}^G(\mathbf{S})$ which is defined as

$$\mathcal{R}^G(\mathbf{S})$$

$$= \left\{ (R_0, R_p, R_s) : \begin{array}{rcl} 0 \le R_s & \le & R_s(\mathbf{K}) \\ R_0 + R_p + R_s & \le & R_s(\mathbf{K}) + R_p(\mathbf{K}) + \min\{R_{0Y}(\mathbf{K}), R_{0Z}(\mathbf{K})\} \\ R_0 & \le & \min\{R_{0Y}(\mathbf{K}), R_{0Z}(\mathbf{K})\} \\ \multicolumn{3}{c}{\text{for some } \mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \end{array} \right\} \tag{2.35}$$

where $R_s(\mathbf{K}), R_p(\mathbf{K}), R_{0Y}(\mathbf{K}), R_{0Z}(\mathbf{K})$ are given as follows

$$R_s(\mathbf{K}) = \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{2.36}$$

$$R_p(\mathbf{K}) = \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{2.37}$$

$$R_{0Y}(\mathbf{K}) = \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{K}+\mathbf{\Sigma}_Y|} \tag{2.38}$$

$$R_{0Z}(\mathbf{K}) = \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{2.39}$$

To provide the converse proof, i.e., to prove the optimality of jointly Gaussian $(U, V = \mathbf{X})$ for the optimization problem in (2.33)-(2.34), we will show that

$$f(R_0^*) = g(R_0^*), \quad 0 \le R_0^* \le \min\{C_Y(\mathbf{S}), C_Z(\mathbf{S})\} \tag{2.40}$$

where $g(R_0^*)$ is defined as

$$g(R_0^*) = \max_{(R_0^*, R_p, R_s)\in\mathcal{R}^G(\mathbf{S})} \mu_p R_p + \mu_s R_s \tag{2.41}$$

We show (2.40) in two parts:

- $\mu_s \le \mu_p$
- $\mu_p < \mu_s$

2.4.1 $\mu_s \leq \mu_p$

In this case, $f(R_0^*)$ can be written as

$$f(R_0^*) = \max_{\substack{U \to V \to \mathbf{X} \to (\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}}} \mu_p(R_p + R_s) \tag{2.42}$$

$$\text{s.t.} \begin{cases} R_0^* + R_p + R_s & \leq & I(\mathbf{X};\mathbf{Y}|U) + \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} \\ R_0^* & \leq & \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} \end{cases} \tag{2.43}$$

where we use the fact that $\mu_s \leq \mu_p$, and the secret message rate R_s can be given up in favor of the private message rate R_p. In other words, we use the fact that when $\mu_p \geq \mu_s$, the maximum of $\mu_p R_p + \mu_s R_s$ is given by $\mu_p R_p'$, where $R_p' = R_s + R_p$ is an achievable public message rate since the secret message can be converted into a public message. This optimization problem gives us the capacity region of the two-user Gaussian MIMO broadcast channel with degraded message sets, where a common message is sent to both users, and a private message, on which there is no secrecy constraint, is sent to one of the two users [20]. The optimization problem for this case given in (2.42)-(2.43) is solved in [9] by showing the optimality of jointly Gaussian $(U, \mathbf{X})$, i.e., $f(R_0^*) = g(R_0^*)$. This completes the converse proof for the case $\mu_s \leq \mu_p$.

2.4.2 $\mu_p < \mu_s$

In this case, we first study the optimization problem in (2.41). We rewrite $g(R_0^*)$ as follows

$$g(R_0^*) = \max_{\substack{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S} \\ R_p}} \quad \mu_p R_p + \mu_s R_s(\mathbf{K}) \tag{2.44}$$

$$\text{s.t.} \quad \begin{cases} R_0^* + R_p & \leq & R_p(\mathbf{K}) + \min\{R_{0Y}(\mathbf{K}), R_{0Z}(\mathbf{K})\} \\ R_0^* & \leq & \min\{R_{0Y}(\mathbf{K}), R_{0Z}(\mathbf{K})\} \end{cases} \tag{2.45}$$

where we use the fact that since $\mu_s > \mu_p$, the secret message rate should be set as high as possible to maximize $\mu_p R_p + \mu_s R_s$, i.e., we should set $R_s = R_s(\mathbf{K})$. Let $(\mathbf{K}^*, R_p^*)$ be the maximizer for this optimization problem. The necessary KKT conditions that $(\mathbf{K}^*, R_p^*)$ needs to satisfy are given in the following lemma.

Lemma 2.2 $\mathbf{K}^*$ *needs to satisfy*

$$(\mu_s - \mu_p\lambda - \beta_Y)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} = (\mu_s - \mu_p\lambda + \beta_Z)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{2.46}$$

for some positive semi-definite matrices $\mathbf{M}, \mathbf{M}_S$ *such that*

$$\mathbf{K}^*\mathbf{M} = \mathbf{M}\mathbf{K}^* = \mathbf{0} \tag{2.47}$$

$$(\mathbf{S} - \mathbf{K}^*)\mathbf{M}_S = \mathbf{M}_S(\mathbf{S} - \mathbf{K}^*) = \mathbf{0} \tag{2.48}$$

and for some $\lambda = 1 - \bar{\lambda}$ *such that it satisfies* $0 \leq \lambda \leq 1$ *and*

$$\lambda \begin{cases} = & 0 \quad \text{if} \quad R_{0Y}(\mathbf{K}^*) > R_{0Z}(\mathbf{K}^*) \\ = & 1 \quad \text{if} \quad R_{0Y}(\mathbf{K}^*) < R_{0Z}(\mathbf{K}^*) \end{cases} \tag{2.49}$$

and (β_Y, β_Z) *are given as follows*

$$(\beta_Y, \beta_Z) = \begin{cases} (0,0) & \text{if} \quad R_0^* < \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\} \\ (0, \geq 0) & \text{if} \quad R_0^* = R_{0Z}(\mathbf{K}^*) < R_{0Y}(\mathbf{K}^*) \\ (\geq 0, 0) & \text{if} \quad R_0^* = R_{0Y}(\mathbf{K}^*) < R_{0Z}(\mathbf{K}^*) \\ (\geq 0, \geq 0) & \text{if} \quad R_0^* = R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*) \end{cases} \tag{2.50}$$

R_p^* *needs to satify*

$$R_p^* = R_p(\mathbf{K}^*) + \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\} - R_0^* \tag{2.51}$$

The proof of Lemma 2.2 is given in Appendix 2.7.2. We treat three cases separately:

- $R_0^* < \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\}$
- $R_0^* = R_{0Y}(\mathbf{K}^*) \leq R_{0Z}(\mathbf{K}^*)$
- $R_0^* = R_{0Z}(\mathbf{K}^*) < R_{0Y}(\mathbf{K}^*)$

2.4.2.1 $R_0^* < \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\}$

In this case, we have $\beta_Y = \beta_Z = 0$, see (2.50). Thus, the KKT condition in (2.46) reduces to

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{2.52}$$

We first note that $\mathbf{K}^*$ satisfying (2.52) achieves the secrecy capacity of this Gaussian MIMO wiretap channel [21], i.e.,

$$\begin{aligned} R_s^* &= R_s(\mathbf{K}^*) && (2.53)\\ &= C_S(\mathbf{S}) && (2.54)\\ &= \max_{\mathbf{0}\preceq\mathbf{K}\preceq\mathbf{S}} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (2.55)\end{aligned}$$

Next, we define a new covariance matrix $\tilde{\mathbf{\Sigma}}_Z$ as follows

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{2.56}$$

which is similar to the channel enhancement done in [21]. This new covariance matrix $\tilde{\mathbf{\Sigma}}_Z$ has some useful properties which are listed in the following lemma.

Lemma 2.3 *We have the following facts.*

- $\mathbf{0} \preceq \tilde{\mathbf{\Sigma}}_Z$
- $\tilde{\mathbf{\Sigma}}_Z \preceq \mathbf{\Sigma}_Z$

- $\tilde{\mathbf{\Sigma}}_Z \preceq \mathbf{\Sigma}_Y$

- $(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1}(\mathbf{S} + \tilde{\mathbf{\Sigma}}_Z) = (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1}(\mathbf{S} + \mathbf{\Sigma}_Z)$

The proof of Lemma 2.3 is given in Appendix 2.7.3. Thus, we have

$$R_{0Z}(\mathbf{K}^*) = \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_Z|} \tag{2.57}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_Z|}{|\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z|} \tag{2.58}$$

$$\geq \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Y|}{|\mathbf{K}^* + \mathbf{\Sigma}_Y|} \tag{2.59}$$

$$= R_{0Y}(\mathbf{K}^*) \tag{2.60}$$

where (2.58) comes from the third part of Lemma 2.3, (2.59) is due to the fact that

$$\frac{|\mathbf{A} + \mathbf{B} + \mathbf{\Delta}|}{|\mathbf{B} + \mathbf{\Delta}|} \leq \frac{|\mathbf{A} + \mathbf{B}|}{|\mathbf{B}|} \tag{2.61}$$

for $\mathbf{A} \succeq \mathbf{0}$, $\mathbf{\Delta} \succeq \mathbf{0}$, $\mathbf{B} \succ \mathbf{0}$ by noting the second part of Lemma 2.3. Therefore, we have

$$R_{0Z}(\mathbf{K}^*) \geq R_{0Y}(\mathbf{K}^*) \tag{2.62}$$

where $\mathbf{K}^*$ satisfies (2.52). Using (2.62) in (2.51), we find R_p^* as follows

$$R_p^* = R_p(\mathbf{K}^*) + R_{0Y}(\mathbf{K}^*) - R_0^* \tag{2.63}$$

We also note the following

$$R_0^* + R_p^* + R_s^* = R_{0Y}(\mathbf{K}^*) + R_p(\mathbf{K}^*) + R_s(\mathbf{K}^*) \tag{2.64}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} \tag{2.65}$$

$$= C_Y(\mathbf{S}) \tag{2.66}$$

Now, we show that

$$g(R_0^*) = f(R_0^*) \tag{2.67}$$

To this end, we assume that

$$g(R_0^*) < f(R_0^*) \tag{2.68}$$

which implies that there exists a rate triple $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$ such that

$$\mu_p R_p^* + \mu_s R_s^* < \mu_p R_p^o + \mu_s R_s^o \tag{2.69}$$

To prove (2.67), i.e., that (2.68) is not possible, we note the following bounds

$$R_s^o \leq C_S(\mathbf{S}) = R_s^* \tag{2.70}$$

$$R_p^o + R_s^o \leq C_Y(\mathbf{S}) - R_0^* = R_p^* + R_s^* \tag{2.71}$$

where (2.70) comes from (2.55) and the fact that the rate of the confidential message, i.e., R_s, cannot exceed the secrecy capacity, and (2.71) is due to (2.66) and the fact that the sum rate $R_0 + R_p + R_s$ cannot exceed the legitimate user's single-user capacity. Thus, in view of $\mu_s > \mu_p$, we can multiply (2.70) and (2.71) by $\mu_s - \mu_p$ and μ_p, respectively, and add the corresponding inequalities to obtain

$$\mu_p R_p^o + \mu_s R_s^o \leq \mu_p R_p^* + \mu_s R_s^* \tag{2.72}$$

which contradicts with (2.69); proving (2.67). This completes the converse proof for this case.

Before starting the proofs of the other two cases, we now recap our proof for the case $R_0^* < \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\}$. We note that we did not show the optimality of Gaussian signalling directly, instead, we prove it indirectly by showing the following

$$g(R_0^*) = f(R_0^*) \tag{2.73}$$

First, we show that for the given common message rate R_0^*, we can achieve the secrecy capacity, i.e., $R_s^* = C_S(\mathbf{S})$, see (2.53)-(2.55). In other words, we show that $(R_0^*, 0, R_s^*)$ is on the boundary of the capacity region $\mathcal{C}_p(\mathbf{S})$. Secondly, we show that for the given common message rate R_0^*, (R_p^*, R_s^*) achieve the sum capacity of the public and confidential messages, i.e., $R_s^* + R_p^*$ is sum rate optimal for the given common message rate R_0^*, see (2.64)-(2.66) and (2.71). These two findings lead to

the inequalities in (2.70)-(2.71). Finally, we use a time-sharing argument for these two inequalities in (2.70)-(2.71) to obtain (2.73), which completes the proof.

2.4.2.2 $R_0^* = R_{0Y}(\mathbf{K}^*) \leq R_{0Z}(\mathbf{K}^*)$

We first rewrite the KKT condition in (2.46) as follows

$$(\mu_s - \mu_p\lambda - \mu_0\beta)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} = (\mu_s - \mu_p\lambda + \mu_0\bar{\beta})(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{2.74}$$

by defining $\mu_0 = \beta_Y + \beta_Z$, $\mu_0\beta = \beta_Y$, and $\mu_0\bar{\beta} = \beta_Z$. We note that if $R_{0Y}(\mathbf{K}^*) < R_{0Z}(\mathbf{K}^*)$, we have $\beta = \lambda = 1$, if $R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$, we have $0 \leq \lambda \leq 1, 0 \leq \beta \leq 1$. The proof of these two cases are very similar, and we consider only the case $0 \leq \lambda \leq 1, 0 \leq \beta \leq 1$, i.e., we assume $R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$. The other case can be proved similarly.

Similar to Section 2.4.2.1, here also, we prove the desired identity

$$g(R_0^*) = f(R_0^*) \tag{2.75}$$

by contradiction. We first assume that

$$g(R_0^*) < f(R_0^*) \tag{2.76}$$

which implies that there exists a rate triple $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$ such that

$$\mu_p R_p^* + \mu_s R_s^* < \mu_p R_p^o + \mu_s R_s^o \tag{2.77}$$

where we define $R_s^* = R_s(\mathbf{K}^*)$. Since the sum rate $R_0 + R_p + R_s$ needs to be smaller than the legitimate user's single user capacity, we have

$$R_0^* + R_p^o + R_s^o \leq C_Y(\mathbf{S}) \tag{2.78}$$

On the other hand, we have the following

$$R_0^* + R_p^* + R_s^* = \min\{R_{0Y}(\mathbf{K}^*), R_{0Z}(\mathbf{K}^*)\} + R_p(\mathbf{K}^*) + R_s(\mathbf{K}^*) \tag{2.79}$$

$$= R_{0Y}(\mathbf{K}^*) + R_p(\mathbf{K}^*) + R_s(\mathbf{K}^*) \tag{2.80}$$

$$= C_Y(\mathbf{S}) \tag{2.81}$$

where (2.79) comes from (2.51), and (2.80) is due to our assumption that $R_0^* = R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$. Equations (2.78) and (2.81) imply that

$$R_p^o + R_s^o \leq R_p^* + R_s^* \tag{2.82}$$

In the rest of this section, we prove that we have $R_s^o \leq R_s^*$ for the given common message rate R_0^*, which, in conjunction with (2.82), will yield a contradiction with (2.77); proving (2.75). To this end, we first define a new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ as

follows

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \tag{2.83}$$

This new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ has some useful properties which are listed in the following lemma.

Lemma 2.4 *We have the following facts.*

- $\mathbf{0} \preceq \tilde{\mathbf{\Sigma}}_Y$
- $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y$
- $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$
- $(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}\tilde{\mathbf{\Sigma}}_Y = (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y$

The proof of this lemma is given in Appendix 2.7.4. Using this new covariance matrix, we define a random vector $\tilde{\mathbf{Y}}$ as

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y \tag{2.84}$$

where $\tilde{\mathbf{N}}_Y$ is a Gaussian random vector with covariance matrix $\tilde{\mathbf{\Sigma}}_Y$. Due to the first and second statements of Lemma 2.4, we have the following Markov chains

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y} \tag{2.85}$$

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Z} \tag{2.86}$$

We next study the following optimization problem

$$\begin{aligned}
&\max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad \mu_0 R_0 + (\mu_s - \mu_p\lambda)R_s \\
&= \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad \mu_0 \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} + (\mu_s - \mu_p\lambda)\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right]
\end{aligned} \tag{2.87}$$

where the equality follows from the fact that the maximum of $\mu_0 R_0 + \mu_s R_s$ is obtained by selecting both R_0 and R_s to be individually maximum, i.e., by setting $R_0 = \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\}$, $R_s = I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)$, since this is possible by simply setting $R_p = 0$.

Since we assume $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$, we have the following lower bound for (2.87)

$$\mu_0 R_0^* + (\mu_s - \mu_p\lambda)R_s^o \le \max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad \mu_0 R_0 + (\mu_s - \mu_p\lambda)R_s \tag{2.88}$$

Now we solve the optimization problem in (2.87) as follows

$$\max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad \mu_0 R_0 + (\mu_s - \mu_p\lambda)R_s$$

$$= \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad \mu_0 \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} + (\mu_s - \mu_p\lambda)\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right] \tag{2.89}$$

$$\leq \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad \mu_0\bar{\beta} I(U;\mathbf{Z}) + \mu_0\beta I(U;\mathbf{Y}) + (\mu_s - \mu_p\lambda)\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right] \tag{2.90}$$

$$\leq \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad \mu_0\bar{\beta} I(U;\mathbf{Z}) + \mu_0\beta I(U;\mathbf{Y}) + (\mu_s - \mu_p\lambda)\left[I(V;\tilde{\mathbf{Y}}|U) - I(V;\mathbf{Z}|U)\right] \tag{2.91}$$

$$\leq \max_{\substack{U\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad \mu_0\bar{\beta} I(U;\mathbf{Z}) + \mu_0\beta I(U;\mathbf{Y}) + (\mu_s - \mu_p\lambda)\left[I(\mathbf{X};\tilde{\mathbf{Y}}|U) - I(\mathbf{X};\mathbf{Z}|U)\right] \tag{2.92}$$

$$\begin{aligned} &\leq \frac{\mu_0\bar{\beta}}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_Z|} + \frac{\mu_0\beta}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Y|}{|\mathbf{K}^*+\mathbf{\Sigma}_Y|} \\ &\quad + \frac{\mu_s-\mu_p\lambda}{2}\left[\log\frac{|\mathbf{K}^*+\tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \end{aligned} \tag{2.93}$$

$$= \mu_0\bar{\beta}R_{0Z}(\mathbf{K}^*) + \mu_0\beta R_{0Y}(\mathbf{K}^*) + \frac{\mu_s-\mu_p\lambda}{2}\left[\log\frac{|\mathbf{K}^*+\tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|} - \log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \tag{2.94}$$

$$= \mu_0\bar{\beta}R_{0Z}(\mathbf{K}^*) + \mu_0\beta R_{0Y}(\mathbf{K}^*) + \frac{\mu_s-\mu_p\lambda}{2}\left[\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|} - \log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \tag{2.95}$$

$$= \mu_0\bar{\beta}R_{0Z}(\mathbf{K}^*) + \mu_0\beta R_{0Y}(\mathbf{K}^*) + (\mu_s-\mu_p\lambda)R_s(\mathbf{K}^*) \tag{2.96}$$

$$= \mu_0 R_0^* + (\mu_s-\mu_p\lambda)R_s^* \tag{2.97}$$

where (2.90) comes from the fact that $0 \leq \beta = 1 - \bar{\beta} \leq 1$, (2.91)-(2.92) are due to the Markov chains in (2.85)-(2.86), respectively, (2.93) can be obtained by using the analysis in [18, eqns (30)-(32)] which uses an extremal inequality from [5] to establish this result, (2.95) comes from the third part of Lemma 2.4, and (2.97) is due to our assumption that $R_0^* = R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$. Thus, (2.97) implies

$$\max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad \mu_0 R_0 + (\mu_s - \mu_p\lambda)R_s \leq \mu_0 R_0^* + (\mu_s - \mu_p\lambda)R_s^* \tag{2.98}$$

Comparing (2.88) and (2.98) yields

$$R_s^o \leq R_s^* \tag{2.99}$$

Using (2.82) and (2.99) and noting $\mu_s > \mu_p$, we can get

$$\mu_p R_p^o + \mu_s R_s^o \leq \mu_p R_p^* + \mu_s R_s^* \tag{2.100}$$

which contradicts with (2.77); proving (2.75). This completes the converse proof for this case.

Before providing the proof for the last case, we recap our proof for the case $R_0^* = R_{0Y}(\mathbf{K}^*) \leq R_{0Z}(\mathbf{K}^*)$. Similar to Section 2.4.2.1, here also, we prove the optimality of Gaussian signalling indirectly, i.e., we show the desired identity

$$g(R_0^*) = f(R_0^*) \tag{2.101}$$

indirectly. First, we show that for the given common message rate R_0^*, $R_s^*+R_p^*$ is sum rate optimal, i.e., (R_p^*, R_s^*) achieve the sum capacity of the public and confidential messages, by obtaining (2.82). Secondly, we show that $(R_0^*, 0, R_s^*)$ is also on the boundary of the capacity region $\mathcal{C}_p(\mathbf{S})$ by obtaining (2.98). These two findings give us the inequalities in (2.82) and (2.99). Finally, we use a time-sharing argument for these two inequalities in (2.82) and (2.99) to establish (2.101), which completes the proof.

2.4.2.3 $R_0^* = R_{0Z}(\mathbf{K}^*) < R_{0Y}(\mathbf{K}^*)$

In this case, we have $\lambda = \beta_Y = 0$, see (2.49)-(2.50). Hence, the KKT condition in (2.46) reduces to

$$\mu_s(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} = (\mu_s + \beta_Z)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{2.102}$$

We again prove the desired identity

$$g(R_0^*) = f(R_0^*) \tag{2.103}$$

by contradiction. We first assume that

$$g(R_0^*) < f(R_0^*) \tag{2.104}$$

which implies that there exists a rate triple $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$ such that

$$\mu_p R_p^* + \mu_s R_s^* < \mu_p R_p^o + \mu_s R_s^o \tag{2.105}$$

In the rest of the section, we show that

$$\mu_p R_p^* + \mu_s R_s^* \geq \mu_p R_p^o + \mu_s R_s^o \tag{2.106}$$

to reach a contradiction, and hence, prove (2.103). To this end, we define a new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ as follows

$$\mu_s(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = \mu_s(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \tag{2.107}$$

This new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ has some useful properties listed in the following lemma.

Lemma 2.5 *We have the following facts.*

- $\mathbf{0} \preceq \tilde{\mathbf{\Sigma}}_Y$
- $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y$
- $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$
- $(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}\tilde{\mathbf{\Sigma}}_Y = (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y$

The proof of this lemma is very similar to the proof Lemma 2.4, and hence is omitted. Using this new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$, we define a random vector $\tilde{\mathbf{Y}}$ as

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y \tag{2.108}$$

where $\tilde{\mathbf{N}}_Y$ is a Gaussian random vector with covariance matrix $\tilde{\mathbf{\Sigma}}_Y$. Due to the first and second statements of Lemma 2.5, we have the following Markov chains

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y} \tag{2.109}$$

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Z} \tag{2.110}$$

Next, we study the following optimization problem

$$\max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad (\mu_p+\beta_Z)R_0 + \mu_p R_p + \mu_s R_s \tag{2.111}$$

We note that since $(R_0^*, R_p^o, R_s^o) \in \mathcal{C}_p(\mathbf{S})$, we have the following lower bound for the optimization problem in (2.111)

$$(\mu_p+\beta_Z)R_0^* + \mu_p R_p^o + \mu_s R_s^o \leq \max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad (\mu_p+\beta_Z)R_0 + \mu_p R_p + \mu_s R_s \tag{2.112}$$

We next obtain the maximum for (2.111). To this end, we introduce the following lemma which provides an explicit form for this optimization problem.

Lemma 2.6 *For $\mu_s > \mu_p$, we have*

$$\begin{aligned}\max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad & (\mu_p+\beta_Z)R_0+\mu_pR_p+\mu_sR_s \\ = \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad & (\mu_p+\beta_Z)\min\{I(U;\mathbf{Y}),I(U;\mathbf{Z})\}+\mu_pI(V;\mathbf{Z}|U) \\ & +\mu_s\left[I(V;\mathbf{Y}|U)-I(V;\mathbf{Z}|U)\right] \end{aligned} \tag{2.113}$$

The proof of this lemma is given in Appendix 2.7.5.

Next we introduce the following extremal inequality from [5], which will be used subsequently in the solution of (2.113).

Lemma 2.7 ([5, Corollary 4]) *Let $(U,\mathbf{X})$ be an arbitrarily correlated random vector, where $\mathbf{X}$ has a covariance constraint $E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}$ and $\mathbf{S}\succ\mathbf{0}$. Let $\mathbf{N}_1,\mathbf{N}_2$ be Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_1,\mathbf{\Sigma}_2$, respectively. They are independent of $(U,\mathbf{X})$. Furthermore, $\mathbf{\Sigma}_1,\mathbf{\Sigma}_2$ satisfy $\mathbf{\Sigma}_1\preceq\mathbf{\Sigma}_2$. Assume that there exists a covariance matrix $\mathbf{K}^*$ such that $\mathbf{K}^*\preceq\mathbf{S}$ and*

$$\nu(\mathbf{K}^*+\mathbf{\Sigma}_1)^{-1}=\gamma(\mathbf{K}^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_S \tag{2.114}$$

where $\nu\geq 0,\gamma\geq 0$ and $\mathbf{M}_S$ is positive semi-definite matrix such that $(\mathbf{S}-\mathbf{K}^*)\mathbf{M}_S=\mathbf{0}$. Then, for any $(U,\mathbf{X})$, we have

$$\nu h(\mathbf{X}+\mathbf{N}_1|U)-\gamma h(\mathbf{X}+\mathbf{N}_2|U)\leq\frac{\nu}{2}\log|(2\pi e)(\mathbf{K}^*+\mathbf{\Sigma}_1)|-\frac{\gamma}{2}\log|(2\pi e)(\mathbf{K}^*+\mathbf{\Sigma}_2)| \tag{2.115}$$

Now we use Lemma 2.7. To this end, we note that using (2.107) in (2.102), we get

$$\mu_s(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mu_s + \beta_Z)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{2.116}$$

In view of (2.116) and the fact that $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$, Lemma 2.7 implies

$$\begin{aligned}\mu_s h(\tilde{\mathbf{Y}}|U) - (\mu_s + \beta_Z)h(\mathbf{Z}|U) \leq \frac{\mu_s}{2}\log|(2\pi e)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)| \\ - \frac{\mu_s + \beta_Z}{2}\log|(2\pi e)(\mathbf{K}^* + \mathbf{\Sigma}_Z)|\end{aligned} \tag{2.117}$$

We now consider the maximization in (2.113) as follows

$$\max_{(R_0,R_p,R_s)\in\mathcal{C}_p(\mathbf{S})} \quad (\mu_p + \beta_Z)R_0 + \mu_p R_p + \mu_s R_s$$

$$= \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad (\mu_p + \beta_Z)\min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} + \mu_p I(V;\mathbf{Z}|U)$$

$$+ \mu_s\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right] \tag{2.118}$$

$$\leq \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad (\mu_p + \beta_Z)I(U;\mathbf{Z}) + \mu_p I(V;\mathbf{Z}|U) + \mu_s\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right]$$

(2.119)

$$\leq \max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad (\mu_p + \beta_Z)I(U;\mathbf{Z}) + \mu_p I(\mathbf{X};\mathbf{Z}|U) + \mu_s\left[I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U)\right]$$

(2.120)

$$\leq \max_{\substack{U\to V\to \mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq \mathbf{S}}} \quad (\mu_p+\beta_Z)I(U;\mathbf{Z})+\mu_p I(\mathbf{X};\mathbf{Z}|U)+\mu_s\left[I(V;\tilde{\mathbf{Y}}|U)-I(V;\mathbf{Z}|U)\right] \tag{2.121}$$

$$\leq \max_{\substack{U\to \mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq \mathbf{S}}} \quad (\mu_p+\beta_Z)I(U;\mathbf{Z})+\mu_p I(\mathbf{X};\mathbf{Z}|U)+\mu_s\left[I(\mathbf{X};\tilde{\mathbf{Y}}|U)-I(\mathbf{X};\mathbf{Z}|U)\right] \tag{2.122}$$

$$\begin{aligned}
&= \max_{\substack{U\to \mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq \mathbf{S}}} \quad (\mu_p+\beta_Z)h(\mathbf{Z})+\mu_s h(\tilde{\mathbf{Y}}|U)-(\mu_s+\beta_Z)h(\mathbf{Z}|U) \\
&\qquad\qquad -\frac{\mu_s}{2}\log|(2\pi e)\tilde{\mathbf{\Sigma}}_Y|+\frac{\mu_s-\mu_p}{2}\log|(2\pi e)\mathbf{\Sigma}_Z| \qquad (2.123)\\
&\leq \frac{\mu_p+\beta_Z}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_Z)|+\max_{\substack{U\to \mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq \mathbf{S}}} \quad \mu_s h(\tilde{\mathbf{Y}}|U)-(\mu_s+\beta_Z)h(\mathbf{Z}|U) \\
&\quad -\frac{\mu_s}{2}\log|(2\pi e)\tilde{\mathbf{\Sigma}}_Y|+\frac{\mu_s-\mu_p}{2}\log|(2\pi e)\mathbf{\Sigma}_Z| \qquad (2.124)\\
&\leq \frac{\mu_p+\beta_Z}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_Z)|+\frac{\mu_s}{2}\log|(2\pi e)(\mathbf{K}^*+\tilde{\mathbf{\Sigma}}_Y)| \\
&\quad -\frac{\mu_s+\beta_Z}{2}\log|(2\pi e)(\mathbf{K}^*+\mathbf{\Sigma}_Z)|-\frac{\mu_s}{2}\log|(2\pi e)\tilde{\mathbf{\Sigma}}_Y|+\frac{\mu_s-\mu_p}{2}\log|(2\pi e)\mathbf{\Sigma}_Z| \qquad (2.125)\\
&= \frac{\mu_p+\beta_Z}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}+\frac{\mu_p}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \\
&\quad +\frac{\mu_s}{2}\left[\log\frac{|\mathbf{K}^*+\tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|}-\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \qquad (2.126)\\
&= (\mu_p+\beta_Z)R_{0Z}(\mathbf{K}^*)+\mu_p R_p(\mathbf{K}^*)+\frac{\mu_s}{2}\left[\log\frac{|\mathbf{K}^*+\tilde{\mathbf{\Sigma}}_Y|}{|\tilde{\mathbf{\Sigma}}_Y|}-\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \qquad (2.127)\\
&= (\mu_p+\beta_Z)R_{0Z}(\mathbf{K}^*)+\mu_p R_p(\mathbf{K}^*)+\frac{\mu_s}{2}\left[\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Y|}{|\mathbf{\Sigma}_Y|}-\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \qquad (2.128)\\
&= (\mu_p+\beta_Z)R_{0Z}(\mathbf{K}^*)+\mu_p R_p(\mathbf{K}^*)+\mu_s R_s(\mathbf{K}^*) \qquad (2.129)\\
&= (\mu_p+\beta_Z)R_0^*+\mu_p R_p^*+\mu_s R_s^* \qquad (2.130)
\end{aligned}$$

where (2.119) is due to $\min\{a, b\} \leq a$, (2.120) is due to the Markov chain in (2.110), (2.121)-(2.122) come from the Markov chains in (2.109)-(2.110), respectively, (2.124) is due to the maximum entropy theorem [22], (2.125) comes from (2.117), and (2.128) is due to the third part of Lemma 2.5. Comparing (2.130) and (2.112) yields

$$\mu_p R_p^o + \mu_s R_s^o \leq \mu_p R_p^* + \mu_s R_s^* \tag{2.131}$$

which contradicts with our assumption in (2.105); implying (2.103). This completes the converse proof for this case.

We note that contrary to Sections 2.4.2.1 and 2.4.2.2, here we prove the optimality of Gaussian signalling, i.e.,

$$g(R_0^*) = f(R_0^*) \tag{2.132}$$

directly. In other words, to show (2.132), we did not find any other points on the boundary of the capacity region $\mathcal{C}_p(\mathbf{S})$ and did not have to use a time-sharing argument between these points to reach (2.132). (This was our strategy in Sections 2.4.2.1 and 2.4.2.2.) Instead, we define a new optimization problem given in (2.113) whose solution yields (2.132).

2.5 Proof of Theorem 2.3 for the General Case

The achievability of the region given in Theorem 2.3 can be shown by computing the region in Theorem 2.1 with the following selection of $(U, V, \mathbf{X})$: $V = \mathbf{X}$,

$\mathbf{X} = \mathbf{U} + \mathbf{T}$ where $\mathbf{T}, \mathbf{U}$ are independent Gaussian random vectors with covariance matrices $\mathbf{K}, \mathbf{S} - \mathbf{K}$, respectively, $U = \mathbf{U}$. In the rest of this section, we consider the converse proof. We first note that following the approaches in Section V.B of [4] and Section 7.1 of [19], it can be shown that a new Gaussian MIMO wiretap channel can be constructed from any Gaussian MIMO wiretap channel described by (2.13)-(2.14) such that the new channel has the same capacity-equivocation region with the original one and in the new channel, both the legitimate user and the eavesdropper have the same number of antennas as the transmitter, i.e., $r_Y = r_Z = t$. Thus, without loss of generality, we assume that $r_Y = r_Z = t$. We next apply singular-value decomposition to the channel gain matrices $\mathbf{H}_Y, \mathbf{H}_Z$ as follows

$$\mathbf{H}_Y = \mathbf{U}_Y \mathbf{\Lambda}_Y \mathbf{V}_Y^\top \tag{2.133}$$

$$\mathbf{H}_Z = \mathbf{U}_Z \mathbf{\Lambda}_Z \mathbf{V}_Z^\top \tag{2.134}$$

where $\mathbf{U}_Y, \mathbf{U}_Z, \mathbf{V}_Y, \mathbf{V}_Z$ are $t \times t$ orthogonal matrices, and $\mathbf{\Lambda}_Y, \mathbf{\Lambda}_Z$ are diagonal matrices. We now define a new Gaussian MIMO wiretap channel as follows

$$\overline{\mathbf{Y}} = \overline{\mathbf{H}}_Y \mathbf{X} + \mathbf{N}_Y \tag{2.135}$$

$$\overline{\mathbf{Z}} = \overline{\mathbf{H}}_Z \mathbf{X} + \mathbf{N}_Z \tag{2.136}$$

where $\overline{\mathbf{H}}_Y, \overline{\mathbf{H}}_Z$ are defined as

$$\overline{\mathbf{H}}_Y = \mathbf{U}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})\mathbf{V}_Y^\top \tag{2.137}$$

$$\overline{\mathbf{H}}_Z = \mathbf{U}_Z(\mathbf{\Lambda}_Z + \alpha\mathbf{I})\mathbf{V}_Z^\top \tag{2.138}$$

for some $\alpha > 0$. We denote the capacity-equivocation region of the Gaussian MIMO wiretap channel defined in (2.135)-(2.136) by $\mathcal{C}_\alpha(\mathbf{S})$. Since $\overline{\mathbf{H}}_Y, \overline{\mathbf{H}}_Z$ are invertible, the capacity-equivocation region of the channel in (2.135)-(2.136) is equal to the capacity-equivocation region of the following aligned channel

$$\overline{\overline{\mathbf{Y}}} = \mathbf{X} + \overline{\mathbf{H}}_Y^{-1}\mathbf{N}_Y \tag{2.139}$$

$$\overline{\overline{\mathbf{Z}}} = \mathbf{X} + \overline{\mathbf{H}}_Z^{-1}\mathbf{N}_Z \tag{2.140}$$

Thus, using the capacity result for the aligned case, which was proved in the previous section, we obtain $\mathcal{C}_\alpha(\mathbf{S})$ as the union of rate triples (R_0, R_1, R_e) satisfying

$$0 \le R_e \le \frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Y\mathbf{K}\overline{\mathbf{H}}_Y^\top + \mathbf{\Sigma}_Y\right|}{|\mathbf{\Sigma}_Y|} - \frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Z\mathbf{K}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|} \tag{2.141}$$

$$\begin{aligned} R_0 + R_1 \le{}& \frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Y\mathbf{K}\overline{\mathbf{H}}_Y^\top + \mathbf{\Sigma}_Y\right|}{|\mathbf{\Sigma}_Y|} \\ &+ \min\left\{\frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Y\mathbf{S}\overline{\mathbf{H}}_Y^\top + \mathbf{\Sigma}_Y\right|}{\left|\overline{\mathbf{H}}_Y\mathbf{K}\overline{\mathbf{H}}_Y^\top + \mathbf{\Sigma}_Y\right|}, \frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Z\mathbf{S}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}{\left|\overline{\mathbf{H}}_Z\mathbf{K}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}\right\} \end{aligned} \tag{2.142}$$

$$R_0 \le \min\left\{\frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Y\mathbf{S}\overline{\mathbf{H}}_Y^\top + \mathbf{\Sigma}_Y\right|}{\left|\overline{\mathbf{H}}_Y\mathbf{K}\overline{\mathbf{H}}_Y^\top + \mathbf{\Sigma}_Y\right|}, \frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Z\mathbf{S}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}{\left|\overline{\mathbf{H}}_Z\mathbf{K}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}\right\} \tag{2.143}$$

for some positive semi-definite matrix $\mathbf{K}$ such that $\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}$.

We next obtain an outer bound for the capacity-equivocation region of the original Gaussian MIMO wiretap channel in (2.13)-(2.14) in terms of $\mathcal{C}_\alpha(\mathbf{S})$. To this end, we first note the following Markov chains

$$\mathbf{X} \to \overline{\mathbf{Y}} \to \mathbf{Y} \tag{2.144}$$

$$\mathbf{X} \to \overline{\mathbf{Z}} \to \mathbf{Z} \tag{2.145}$$

which imply that if the messages (W_0, W_1) with rates (R_0, R_1) are transmitted with a vanishingly small probability of error in the original Gaussian MIMO wiretap channel given by (2.13)-(2.14), they will be transmitted with a vanishingly small probability of error in the new Gaussian MIMO wiretap channel given by (2.135)-(2.136) as well. However, as opposed to the rates R_0, R_1, we cannot immediately conclude that if an equivocation rate R_e is achievable in the original Gaussian MIMO wiretap channel given in (2.13)-(2.14), it is also achievable in the new Gaussian MIMO wiretap channel in (2.135)-(2.136). The reason for this is that both the legitimate user's and the eavesdropper's channel gain matrices are enhanced in the new channel given by (2.135)-(2.136), see (2.137)-(2.138) and/or (2.144)-(2.145), and consequently, it is not clear what the overall effect of these two enhancements on the equivocation rate will be. However, in the sequel, we show that if $(R_0, R_1, R_e) \in \mathcal{C}(\mathbf{S})$, then we have $(R_0, R_1, R_e - \gamma) \in \mathcal{C}_\alpha(\mathbf{S})$. This will let us write down an outer bound for $\mathcal{C}(\mathbf{S})$ in terms of $\mathcal{C}_\alpha(\mathbf{S})$. To this end, we note that if $(R_0, R_1, R_e) \in \mathcal{C}(\mathbf{S})$, we need to have a random vector $(U, V, \mathbf{X})$ such that the inequalities given in Theorem 2.1 hold. Assume that we use the same random vector $(U, V, \mathbf{X})$ for

the new Gaussian MIMO wiretap channel in (2.135)-(2.136), and achieve the rate triple $(\overline{R}_0, \overline{R}_1, \overline{R}_e)$. Due to the Markov chains in (2.144)-(2.145), we already have $R_1 \leq \overline{R}_1, R_0 \leq \overline{R}_0$. Furthermore, following the analysis in Section 4 of [18], we can bound the gap between R_e and $\overline{R}_e$, i.e., γ, as follows

$$\gamma = R_e - \overline{R}_e \leq \frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Z\mathbf{S}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{2.146}$$

Thus, we have

$$\mathcal{C}(\mathbf{S}) \subseteq \mathcal{C}_\alpha(\mathbf{S}) + \mathcal{G}(\mathbf{S}) \tag{2.147}$$

where $\mathcal{G}(\mathbf{S})$ is

$$\mathcal{G}(\mathbf{S}) = \left\{(0,0,R_e) : 0 \leq R_e \leq \frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Z\mathbf{S}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right\} \tag{2.148}$$

Taking $\alpha \to 0$ in (2.147), we get

$$\mathcal{C}(\mathbf{S}) \subseteq \lim_{\alpha\to 0}\mathcal{C}_\alpha(\mathbf{S}) \tag{2.149}$$

where we use the fact that

$$\lim_{\alpha\to 0}\frac{1}{2}\log\frac{\left|\overline{\mathbf{H}}_Z\mathbf{S}\overline{\mathbf{H}}_Z^\top + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{H}_Z\mathbf{S}\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} = 0 \tag{2.150}$$

which follows from the continuity of $\log|\cdot|$ in positive semi-definite matrices, and the fact that $\lim_{\alpha\to 0}\overline{\mathbf{H}}_Z = \mathbf{H}_Z$. Finally, we note that

$$\lim_{\alpha\to 0}\mathcal{C}_\alpha(\mathbf{S}) \tag{2.151}$$

converges to the region given in Theorem 2.3 due to the continuity of $\log|\cdot|$ in positive semi-definite matrices and $\lim_{\alpha\to 0}\overline{\mathbf{H}}_Y = \mathbf{H}_Y, \lim_{\alpha\to 0}\overline{\mathbf{H}}_Z = \mathbf{H}_Z$; completing the proof.

2.6 Conclusions

In this chapter, we obtain the capacity-equivocation region of the Gaussian MIMO wiretap channel. In particular, we show that jointly Gaussian auxiliary random variables and channel input are sufficient to evaluate the existing single-letter description for the capacity-equivocation region of the Gaussian MIMO wiretap channel due to [3]. We prove this sufficiency by using channel enhancement [4] and an extremal inequality from [5].

2.7 Appendix

2.7.1 Proof of Lemma 2.1

The proof of this lemma for $R_0 = 0$ is outlined in [6, Problem 33-c], [7]. We extend their proof to the general case of interest here. We first note the inclusion $\mathcal{C}_p \subseteq \mathcal{C}$, which follows from the fact that if $(R_0, R_p, R_s) \in \mathcal{C}_p$, we can attain the rate triple

$(R_0, R_1 = R_s + R_p, R_e = R_s)$, i.e., $(R_0, R_s + R_p, R_s) \in \mathcal{C}$. To show the reverse inclusion, we use the achievability proof for Theorem 2.1 given in [3]. According to this achievable scheme, W_1 can be divided into two parts as $W_1 = (W_p, W_s)$ with rates $(R_1 - R_e, R_e)$, respectively, and we have

$$H(W_1|W_0, Z^n) = H(W_p, W_s|Z^n, W_0) \tag{2.152}$$

$$\geq H(W_s|Z^n, W_0) \tag{2.153}$$

$$\geq H(W_s) - n\gamma_n \tag{2.154}$$

for some γ_n which satisfies $\lim_{n\to\infty} \gamma_n = 0$. Hence, using this capacity achieving scheme for $\mathcal{C}$, we can attain the rate triple $(R_0, R_p = R_1 - R_e, R_s = R_e) \in \mathcal{C}_p$. This implies $\mathcal{C} \subseteq \mathcal{C}_p$; completing the proof of the lemma.

2.7.2 Proof of Lemma 2.2

Since the program in (2.44)-(2.45) is not necessarily convex, the KKT conditions are necessary but not sufficient. The Lagrangian for this optimization problem is given by

$$\begin{aligned}\mathcal{L} = {} & \mu_s R_s(\mathbf{K}) + \mu_p R_p + \lambda_Y \left[R_p(\mathbf{K}) + R_{0Y}(\mathbf{K}) - R_p - R_0^*\right] \\ & + \lambda_Z \left[R_p(\mathbf{K}) + R_{0Z}(\mathbf{K}) - R_p - R_0^*\right] + \beta_Y \left[R_{0Y}(\mathbf{K}) - R_0^*\right] + \beta_Z \left[R_{0Z}(\mathbf{K}) - R_0^*\right] \\ & + \mathrm{tr}(\mathbf{K}\mathbf{M}) + \mathrm{tr}((\mathbf{S} - \mathbf{K})\mathbf{M}_S)\end{aligned} \tag{2.155}$$

where $\mathbf{M}, \mathbf{M}_S$ are positive semi-definite matrices, and $\lambda_Y \geq 0, \lambda_Z \geq 0$, $\beta_Y \geq 0, \beta_Z \geq 0$.

The necessary KKT conditions that they need to satisfy are given as follows

$$\frac{\partial \mathcal{L}}{\partial R_p} \mid_{R_p = R_p^*} = 0 \tag{2.156}$$

$$\nabla_{\mathbf{K}} \mathcal{L} \mid_{\mathbf{K}=\mathbf{K}^*} = \mathbf{0} \tag{2.157}$$

$$\mathrm{tr}(\mathbf{K}^* \mathbf{M}) = 0 \tag{2.158}$$

$$\mathrm{tr}((\mathbf{S} - \mathbf{K}^*)\mathbf{M}_S) = 0 \tag{2.159}$$

$$\lambda_Y \left[R_p(\mathbf{K}^*) + R_{0Y}(\mathbf{K}^*) - R_p^* - R_0^* \right] = 0 \tag{2.160}$$

$$\lambda_Z \left[R_p(\mathbf{K}^*) + R_{0Z}(\mathbf{K}^*) - R_p^* - R_0^* \right] = 0 \tag{2.161}$$

$$\beta_Y (R_{0Y}(\mathbf{K}^*) - R_0^*) = 0 \tag{2.162}$$

$$\beta_Z (R_{0Z}(\mathbf{K}^*) - R_0^*) = 0 \tag{2.163}$$

The first KKT condition in (2.156) implies $\lambda_Y + \lambda_Z = \mu_p$. We define $\lambda_Y = \mu_p \lambda, \lambda_Z = \mu_p \bar{\lambda}$ and consequently, we have $0 \leq \bar{\lambda} = 1 - \lambda \leq 1$. The second KKT condition in (2.157) implies (2.46). Since $\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA})$ and $\mathrm{tr}(\mathbf{AB}) \geq 0$ for $\mathbf{A} \succeq \mathbf{0}, \mathbf{B} \succeq \mathbf{0}$, (2.158)-(2.159) imply (2.47)-(2.48). The KKT conditions in (2.160)-(2.161) imply (2.51). Furthermore, the KKT conditions in (2.160)-(2.161) state the conditions that if $R_{0Y}(\mathbf{K}^*) > R_{0Z}(\mathbf{K}^*)$, $\lambda = 0$, if $R_{0Y}(\mathbf{K}^*) < R_{0Z}(\mathbf{K}^*)$, $\lambda = 1$, and if $R_{0Y}(\mathbf{K}^*) = R_{0Z}(\mathbf{K}^*)$, λ is arbitrary, i.e., $0 \leq \lambda \leq 1$. Similarly, the KKT conditions in (2.162)-(2.163) imply (2.50).

2.7.3 Proof of Lemma 2.3

We note the following identities

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{2.164}$$

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \tag{2.165}$$

where (2.164) is due to (2.56), and (2.165) is obtained by plugging (2.164) into (2.52). Since $\mathbf{M} \succeq \mathbf{0}, \mathbf{M}_S \succeq \mathbf{0}$, (2.164)-(2.165) implies

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1} \succeq (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} \tag{2.166}$$

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1} \succeq (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} \tag{2.167}$$

Using the fact that for $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succ \mathbf{0}$, if $\mathbf{A} \preceq \mathbf{B}$, then $\mathbf{A}^{-1} \succeq \mathbf{B}^{-1}$ in (2.166)-(2.167), we can get the second and third parts of Lemma 2.3. Next, we prove the first part

of the lemma as follows

$$\tilde{\mathbf{\Sigma}}_Z = \left[(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{M} \right]^{-1} - \mathbf{K}^* \tag{2.168}$$

$$= \left[\mathbf{I} + \frac{1}{\mu_s - \mu_p \lambda} (\mathbf{K}^* + \mathbf{\Sigma}_Y) \mathbf{M} \right]^{-1} (\mathbf{K}^* + \mathbf{\Sigma}_Y) - \mathbf{K}^* \tag{2.169}$$

$$= \left[\mathbf{I} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{\Sigma}_Y \mathbf{M} \right]^{-1} (\mathbf{K}^* + \mathbf{\Sigma}_Y) - \mathbf{K}^* \tag{2.170}$$

$$= \left[\mathbf{\Sigma}_Y^{-1} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{M} \right]^{-1} \mathbf{\Sigma}_Y^{-1} (\mathbf{K}^* + \mathbf{\Sigma}_Y) - \mathbf{K}^* \tag{2.171}$$

$$= \left[\mathbf{\Sigma}_Y^{-1} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{M} \right]^{-1} \left[\mathbf{\Sigma}_Y^{-1} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{M} \right] \mathbf{K}^* + \left[\mathbf{\Sigma}_Y^{-1} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{M} \right]^{-1} - \mathbf{K}^* \tag{2.172}$$

$$= \mathbf{K}^* + \left[\mathbf{\Sigma}_Y^{-1} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{M} \right]^{-1} - \mathbf{K}^* \tag{2.173}$$

$$= \left[\mathbf{\Sigma}_Y^{-1} + \frac{1}{\mu_s - \mu_p \lambda} \mathbf{M} \right]^{-1} \tag{2.174}$$

$$\succeq \mathbf{0} \tag{2.175}$$

where (2.168) comes from (2.165), (2.170) and (2.172) follow from the KKT condition in (2.47).

Finally, we show the fourth part of Lemma 2.3 as follows

$$(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1}(\mathbf{S} + \tilde{\mathbf{\Sigma}}_Z) = (\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1}(\mathbf{S} + \mathbf{K}^* - \mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z) \tag{2.176}$$

$$= \mathbf{I} + (\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Z)^{-1}(\mathbf{S} - \mathbf{K}^*) \tag{2.177}$$

$$= \mathbf{I} + \left[(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \frac{1}{\mu_s - \mu_p\lambda}\mathbf{M}_S\right](\mathbf{S} - \mathbf{K}^*) \tag{2.178}$$

$$= \mathbf{I} + (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1}(\mathbf{S} - \mathbf{K}^*) \tag{2.179}$$

$$= (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1}(\mathbf{K}^* + \mathbf{\Sigma}_Z) + (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1}(\mathbf{S} - \mathbf{K}^*) \tag{2.180}$$

$$= (\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1}(\mathbf{S} + \mathbf{\Sigma}_Z) \tag{2.181}$$

where (2.178) is due to (2.164), and (2.179) comes from (2.48). The proof is complete.

2.7.4 Proof of Lemma 2.4

We note the following

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M} \tag{2.182}$$

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mu_s - \mu_p\lambda + \mu_0\bar{\beta})(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} + \mu_0\beta(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_S \tag{2.183}$$

where (2.182) is (2.83), and (2.183) comes from plugging (2.182) into (2.74). Since $\mathbf{M} \succeq \mathbf{0}$, (2.182) implies

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} \succeq (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} \tag{2.184}$$

Using the fact that for $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succ \mathbf{0}$, if $\mathbf{A} \preceq \mathbf{B}$, then $\mathbf{A}^{-1} \succeq \mathbf{B}^{-1}$ in (2.184) yields the second statement of the lemma. Since $0 \leq \beta = 1 - \bar{\beta} \leq 1$ and $\mathbf{M}_S \succeq \mathbf{0}$, (2.183) implies

$$(\mu_s - \mu_p\lambda)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} \succeq (\mu_s - \mu_p\lambda)(\mathbf{K}^* + \mathbf{\Sigma}_Z)^{-1} \tag{2.185}$$

Using the fact that for $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succ \mathbf{0}$, if $\mathbf{A} \preceq \mathbf{B}$, then $\mathbf{A}^{-1} \succeq \mathbf{B}^{-1}$ in (2.185) yields the first statement of the lemma. To prove the first statement of the lemma, we note that (2.182) implies

$$\tilde{\mathbf{\Sigma}}_Y = \left[(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \frac{1}{\mu_s - \mu_p\lambda}\mathbf{M}\right]^{-1} - \mathbf{K}^* \tag{2.186}$$

which is already shown to be positive semi-definite as done through (2.168)-(2.175) in Appendix 2.7.3.

Finally, we consider the fourth statement of this lemma as follows

$$(\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}\tilde{\mathbf{\Sigma}}_Y = (\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{K}^* - \mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y) \tag{2.187}$$

$$= \mathbf{I} - (\mathbf{K}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1}\mathbf{K}^* \tag{2.188}$$

$$= \mathbf{I} - \left[(\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1} + \frac{1}{\mu_s - \mu_p\lambda}\mathbf{M}\right]\mathbf{K}^* \tag{2.189}$$

$$= \mathbf{I} - (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}\mathbf{K}^* \tag{2.190}$$

$$= (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}(\mathbf{K}^* + \mathbf{\Sigma}_Y) - (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}\mathbf{K}^* \tag{2.191}$$

$$= (\mathbf{K}^* + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \tag{2.192}$$

where (2.189) is due to (2.182) and (2.190) comes from (2.47).

2.7.5 Proof of Lemma 2.6

The optimization problem in (2.113) can be written as

$$\max_{\substack{U\to V\to\mathbf{X}\to(\mathbf{Y},\mathbf{Z}) \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \quad \mu_s R_s + \mu_p R_p + (\mu_p + \beta_Z)R_0 \tag{2.193}$$

$$\text{s.t.} \begin{cases} 0 \le R_s & \le & I(V;\mathbf{Y}|U) - I(V;\mathbf{Z}|U) \\ R_s + R_p + R_0 & \le & I(V;\mathbf{Y}|U) + \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} \\ R_0 & \le & \min\{I(U;\mathbf{Y}), I(U;\mathbf{Z})\} \end{cases} \tag{2.194}$$

For a given $(U, V, \mathbf{X})$, we can rewrite the cost function in (2.193) as follows

$$\mu_s R_s + \mu_p R_p + (\mu_p + \beta_Z) R_0$$

$$\leq \mu_s R_s + \mu_p [I(V; \mathbf{Y}|U) + \min\{I(U; \mathbf{Y}), I(U; \mathbf{Z})\} - R_s - R_0] + (\mu_p + \beta_Z) R_0 \tag{2.195}$$

$$= (\mu_s - \mu_p) R_s + \mu_p [I(V; \mathbf{Y}|U) + \min\{I(U; \mathbf{Y}), I(U; \mathbf{Z})\}] + \beta_Z R_0 \tag{2.196}$$

$$\leq (\mu_s - \mu_p)[I(V; \mathbf{Y}|U) - I(V; \mathbf{Z}|U)] + \mu_p [I(V; \mathbf{Y}|U) + \min\{I(U; \mathbf{Y}), I(U; \mathbf{Z})\}]$$
$$+ \beta_Z R_0 \tag{2.197}$$

$$= \mu_s [I(V; \mathbf{Y}|U) - I(V; \mathbf{Z}|U)] + \mu_p [I(V; \mathbf{Z}|U) + \min\{I(U; \mathbf{Y}), I(U; \mathbf{Z})\}] + \beta_Z R_0 \tag{2.198}$$

$$\leq \mu_s [I(V; \mathbf{Y}|U) - I(V; \mathbf{Z}|U)] + \mu_p [I(V; \mathbf{Z}|U) + \min\{I(U; \mathbf{Y}), I(U; \mathbf{Z})\}]$$
$$+ \beta_Z \min\{I(U; \mathbf{Y}), I(U; \mathbf{Z})\} \tag{2.199}$$

$$= \mu_s [I(V; \mathbf{Y}|U) - I(V; \mathbf{Z}|U)] + \mu_p I(V; \mathbf{Z}|U) + (\mu_p + \beta_Z) \min\{I(U; \mathbf{Y}), I(U; \mathbf{Z})\} \tag{2.200}$$

where (2.195) comes from the second constraint in (2.194), (2.197) is due to the first constraint in (2.194) and the assumption $\mu_s > \mu_p$, and (2.199) comes from the third constraint in (2.194). The proof can be concluded by noting that the upper bound on the cost function given in (2.200) is attainable.

Chapter 3

Secure Broadcasting over Multi-receiver Wiretap Channels

3.1 Introduction

In this chapter, we consider the secure broadcasting problem, where one transmitter wants to have confidential communication with an arbitrary number of users in a broadcast channel, while this communication is being eavesdropped by an external entity (see Figure 3.1). In its most general form, the secure broadcasting problem subsumes the broadcast channel whose capacity region is still unknown, and is considered to be a hard problem. Hence, towards understanding the fundamental limits of secure broadcasting, the previous works consider some special cases of this problem [23, 24].

Reference [23] first considers an arbitrary wiretap channel with two legitimate receivers and one eavesdropper, and provides an inner bound for achievable rates when each user wishes to receive an independent message. Secondly, [23] focuses on the degraded wiretap channel with two receivers and one eavesdropper, where there is a degradedness order among the receivers, and the eavesdropper is degraded with respect to both users (see Figure 3.2 for a more general version of this problem that we study here). For this setting, [23] finds the secrecy capacity region. We obtain this result concurrently and independently, see Corollary 3.1.

Another relevant work on secure broadcasting is [24] which considers secure

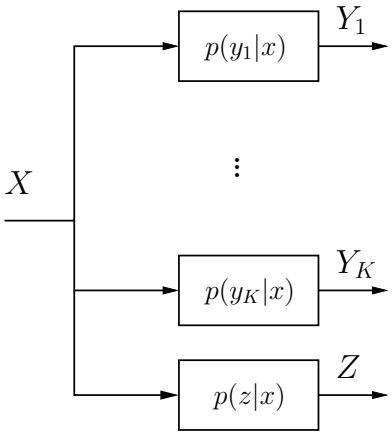

Figure 3.1: Secure broadcasting to many users in the presence of an eavesdropper.

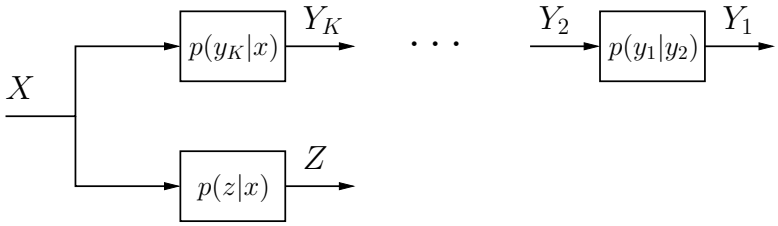

Figure 3.2: The degraded multi-receiver wiretap channel with a more noisy eavesdropper.

broadcasting to K users using M sub-channels (see Figure 3.3) for two different scenarios: In the first scenario, the transmitter wants to convey only a common confidential message to all users, and in the second scenario, the transmitter wants to send independent messages to all users. For both scenarios, [24] considers a sub-class of parallel multi-receiver wiretap channels, where in any given sub-channel there is a degradation order such that each receiver's observation (except the best one) is a degraded version of some other receiver's observation, and this degradation order is not necessarily the same for all sub-channels. For the first scenario, [24] finds the common message secrecy capacity for this sub-class. For the second scenario, where each user wishes to receive an independent message, [24] finds the sum secrecy

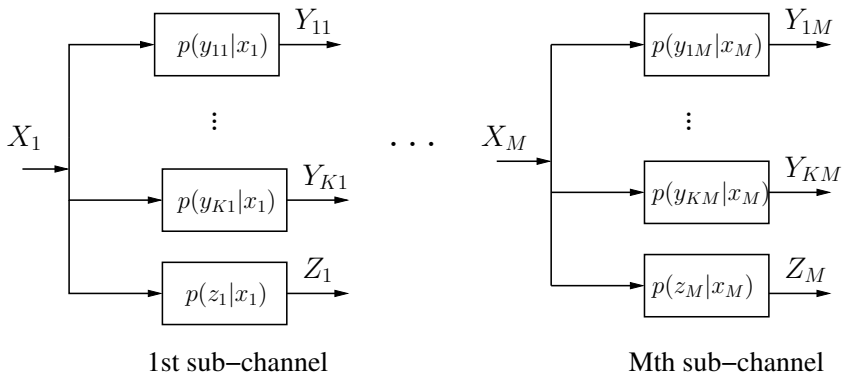

Figure 3.3: The parallel multi-receiver wiretap channel.

capacity for this sub-class of channels.

In this chapter, our approach will be two-fold: First, we will identify more general channel models than considered in [23, 24] and generalize the results in [23, 24] to those channel models, and secondly, we will consider somewhat more specialized channel models than in [24] and provide more comprehensive results. More precisely, our contributions in this chapter are:

1. We consider the degraded multi-receiver wiretap channel with an arbitrary number of users and one eavesdropper, where users are arranged according to a degradedness order, and each user has a less noisy channel with respect to the eavesdropper, see Figure 3.2. We find the secrecy capacity region when each user receives both an independent message and a common confidential message. Since degradedness implies less noisiness [3], this channel model contains the sub-class of channel models where in addition to the degradedness order users exhibit, the eavesdropper is degraded with respect to all users. Consequently, our result can be specialized to the degraded multi-receiver wiretap channel with an arbitrary number of users and a degraded eavesdropper, see

Corollary 3.1 and also [25]. The two-user version of the degraded multi-receiver wiretap channel was studied and the capacity region was found independently and concurrently in [23].

2. We then focus on a class of parallel multi-receiver wiretap channels with an arbitrary number of legitimate receivers and an eavesdropper, see Figure 3.3, where in each sub-channel, for any given user, either the user's channel is less noisy with respect to the eavesdropper's channel, or vice versa. We establish the common message secrecy capacity of this channel, which is a generalization of the corresponding capacity result in [24] to a broader class of channels. Secondly, we study the scenario where each legitimate receiver wishes to receive an independent message for another sub-class of parallel multi-receiver wiretap channels. For channels belonging to this sub-class, in each sub-channel, there is a less noisiness order which is not necessarily the same for all sub-channels. Consequently, this ordered class of channels is a subset of the class for which we establish the common message secrecy capacity. We find the sum secrecy capacity for this class, which is again a generalization of the corresponding result in [24] to a broader class of channels.

3. We also investigate a class of parallel multi-receiver wiretap channels with two sub-channels, two users and one eavesdropper, see Figure 3.4. For the channels in this class, there is a specific degradation order in each sub-channel such that in the first (resp. second) sub-channel the second (resp. first) user is degraded with respect to the first (resp. second) user, while the eavesdropper is

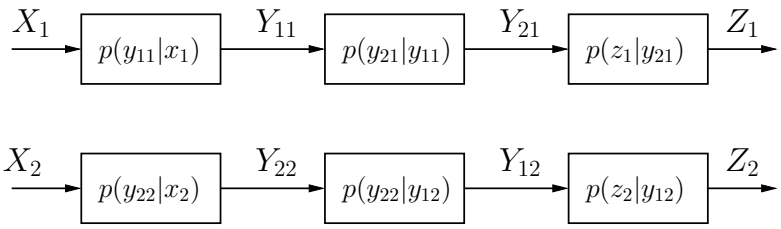

Figure 3.4: The parallel degraded multi-receiver wiretap channel.

degraded with respect to both users in both sub-channels. This is the model of [24] for $K = 2$ users and $M = 2$ sub-channels. This model is more restrictive compared to the one mentioned in the previous item. Our motivation to study this more special class is to provide a stronger and more comprehensive result. In particular, for this class, we determine the entire secrecy capacity region when each user receives both an independent message and a common message. In contrast, [24] gives the common message secrecy capacity (when only a common message is transmitted) and sum secrecy capacity (when only independent messages are transmitted) of this class. We discuss the generalization of this result to arbitrary numbers of users and sub-channels.

4. We finally consider a variant of the previous channel model. In this model, we again have a parallel multi-receiver wiretap channel with two sub-channels, two users and one eavesdropper, and the degradation order in each sub-channel is exactly the same as in the previous item. However, in this case, the input and output alphabets of one sub-channel are non-intersecting with the input and output alphabets of the other sub-channel. Moreover, we can use only one of these sub-channels at any time. We determine the secrecy capacity region

of this channel when the transmitter sends both an independent message to each receiver and a common message to both receivers.

3.2 Degraded Multi-receiver Wiretap Channels

We first consider the generalization of Wyner's degraded wiretap channel to the case with many legitimate receivers. In particular, the channel consists of a transmitter with an input alphabet $x \in \mathcal{X}$, K legitimate receivers with output alphabets $y_k \in \mathcal{Y}_k,\ k = 1, \ldots, K$, and an eavesdropper with output alphabet $z \in \mathcal{Z}$. The transmitter sends a confidential message to each user, say $w_k \in \mathcal{W}_k$ to the kth user, in addition to a common message, $w_0 \in \mathcal{W}_0$, which is to be delivered to all users. All messages are to be kept secret from the eavesdropper. The channel is assumed to be memoryless with a transition probability $p(y_1, y_2, \ldots, y_K, z|x)$.

In this section, we consider a special class of these channels, see Figure 3.2, where users exhibit a certain degradation order, i.e., their channel outputs satisfy the following Markov chain

$$X \to Y_K \to \ldots \to Y_1 \tag{3.1}$$

and each user has a less noisy channel with respect to the eavesdropper, i.e., we have

$$I(U; Y_k) > I(U; Z) \tag{3.2}$$

for every U such that $U \to X \to (Y_k, Z)$. In fact, since a degradation order exists among the users, it is sufficient to say that user 1 has a less noisy channel with respect to the eavesdropper to guarantee that all users do. Hereafter, we call this channel *the degraded multi-receiver wiretap channel with a more noisy eavesdropper*. We note that this channel model contains the degraded multi-receiver wiretap channel which is defined through the Markov chain

$$X \to Y_K \to \ldots \to Y_1 \to Z \tag{3.3}$$

because the Markov chain in (3.3) implies the less noisiness condition in (3.2).

A $(2^{nR_0}, 2^{nR_1}, \ldots, 2^{nR_K}, n)$ code for this channel consists of $K+1$ message sets, $\mathcal{W}_k = \{1, \ldots, 2^{nR_k}\}$, $k = 0, 1, \ldots, K$, an encoder $f : \mathcal{W}_0 \times \ldots \times \mathcal{W}_K \to \mathcal{X}^n$, K decoders, one at each legitimate receiver, $g_k : \mathcal{Y}_k \to \mathcal{W}_0 \times \mathcal{W}_k$, $k = 1, \ldots, K$. The probability of error is defined as $P_e^n = \max_{k=1,\ldots,K} \Pr\left[g_k(Y_k^n) \neq (W_0, W_k)\right]$. A rate tuple $(R_0, R_1, \ldots, R_K)$ is said to be achievable if there exists a code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z^n) \geq \sum_{k\in\mathcal{S}(W)} R_k, \quad \forall\, \mathcal{S}(W) \tag{3.4}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_0, W_1, \ldots, W_K\}$. Hence, we consider only perfect secrecy rates. The secrecy capacity region is defined as the closure of all achievable rate tuples.

The secrecy capacity region of the degraded multi-receiver wiretap channel

with a more noisy eavesdropper is given by the following theorem whose proof is provided in Appendix 3.7.1.

Theorem 3.1 *The secrecy capacity region of the degraded multi-receiver wiretap channel with a more noisy eavesdropper is given by the union of the rate tuples* $(R_0, R_1, \ldots, R_K)$ *satisfying*

$$R_0 + \sum_{k=1}^{\ell} R_k \leq \sum_{k=1}^{\ell} I(U_k; Y_k|U_{k-1}) - I(U_\ell; Z), \quad \ell = 1, \ldots, K \tag{3.5}$$

where $U_0 = \phi, U_K = X$*, and the union is over all probability distributions of the form*

$$p(u_1)p(u_2|u_1)\ldots p(u_{K-1}|u_{K-2})p(x|u_{K-1}) \tag{3.6}$$

Remark 3.1 *Theorem 3.1 implies that a modified version of superposition coding can achieve the boundary of the capacity region. The difference between the superposition coding scheme used to achieve (3.5) and the standard one in [22], that is used to achieve the capacity region of the degraded broadcast channel, is that the former uses stochastic encoding in each layer of the code to associate each message with many codewords. This controlled amount of redundancy prevents the eavesdropper from being able decode the message.*

As stated earlier, the degraded multi-receiver wiretap channel with a more noisy eavesdropper contains the degraded multi-receiver wiretap channel which requires the eavesdropper to be degraded with respect to all users as stated in (3.3).

Thus, we can specialize our result in Theorem 3.1 to the degraded multi-receiver wiretap channel as given in the following corollary.

Corollary 3.1 *The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of the rate tuples* $(R_0, R_1, \ldots, R_K)$ *satisfying*

$$R_0 + \sum_{k=1}^{\ell} R_k \leq \sum_{k=1}^{\ell} I(U_k; Y_k|U_{k-1}, Z), \quad \ell = 1, \ldots, K \tag{3.7}$$

where $U_0 = \phi, U_K = X$*, and the union is over all probability distributions of the form*

$$p(u_1)p(u_2|u_1)\ldots p(u_{K-1}|u_{K-2})p(x|u_{K-1}) \tag{3.8}$$

The proof of this corollary can be carried out from Theorem 3.1 by noting the following identity

$$I(U_\ell; Z) = \sum_{k=1}^{\ell} I(U_k; Z|U_{k-1}) \tag{3.9}$$

and the following Markov chains

$$U_{k-1} \to U_k \to Y_k \to Z, \quad k = 1, \ldots, K \tag{3.10}$$

We acknowledge an independent and concurrent work regarding the degraded multi-receiver wiretap channel. Reference [23] considers the two-user case and establishes the secrecy capacity region as well.

So far we have determined the entire secrecy capacity region of the degraded multi-receiver wiretap channel with a more noisy eavesdropper. This class of channels requires a certain degradation order among the legitimate receivers which may be viewed as being too restrictive from a practical point of view. Our goal is to consider progressively more general channel models. Towards that goal, in the next section, we consider channel models where the users are not ordered in a degradedness or noisiness order. However, the concepts of degradedness and noisiness are essential in proving capacity results. In the next section, we will consider multi-receiver broadcast channels which are composed of independent sub-channels. We will assume some noisiness properties in these sub-channels in order to derive certain capacity results. However, even though the sub-channels will have certain noisiness properties, the overall broadcast channel will not have any degradedness or noisiness properties.

3.3 Parallel Multi-receiver Wiretap Channels

Here, we investigate the parallel multi-receiver wiretap channel where the transmitter communicates with K legitimate receivers using M independent sub-channels in the presence of an eavesdropper, see Figure 3.3. The channel transition probability of a parallel multi-receiver wiretap channel is

$$p\left(\{y_{1m},\ldots,y_{Km},z_m\}_{m=1}^{M}\,|\,\{x_m\}_{m=1}^{M}\right)=\prod_{m=1}^{M}p\left(y_{1m},\ldots,y_{Km},z_m|x_m\right) \tag{3.11}$$

where $x_m \in \mathcal{X}_m$ is the input in the mth sub-channel where $\mathcal{X}_m$ is the corresponding channel input alphabet, $y_{km} \in \mathcal{Y}_{km}$ (resp. $z_m \in \mathcal{Z}_m$) is the output in the kth user's (resp. eavesdropper's) mth sub-channel where $\mathcal{Y}_{km}$ (resp. $\mathcal{Z}_m$) is the kth user's (resp. eavesdropper's) mth sub-channel output alphabet.

We note that the parallel multi-receiver wiretap channel can be regarded as an extension of the parallel wiretap channel [26, 27] to the case of multiple legitimate users. Though [26, 27] establish the secrecy capacity of the parallel wiretap channel for the most general case, for the parallel multi-receiver wiretap channel, obtaining the secrecy capacity region for the most general case seems to be intractable for now. Thus, in this section, we investigate special classes of parallel multi-receiver wiretap channels. These channel models contain the class of channel models studied in [24] as a special case. Similar to [24], our emphasis will be on the common message secrecy capacity and the sum secrecy capacity.

3.3.1 The Common Message Secrecy Capacity

We first consider the simplest possible scenario where the transmitter sends a common confidential message to all users. Despite its simplicity, the secrecy capacity of a common confidential message (hereafter will be called the common message secrecy capacity) in a general broadcast channel is unknown.

The common message secrecy capacity for a special class of parallel multi-receiver wiretap channels was studied in [24]. In this class of parallel multi-receiver wiretap channels [24], each sub-channel exhibits a certain degradation order which

is not necessarily the same for all sub-channels, i.e., the following Markov chain is satisfied

$$X_l \to Y_{\pi_l(1)} \to Y_{\pi_l(2)} \to \ldots \to Y_{\pi_l(K+1)} \tag{3.12}$$

in the lth sub-channel, where $(Y_{\pi_l(1)}, Y_{\pi_l(2)}, \ldots, Y_{\pi_l(K+1)})$ is a permutation of $(Y_{1l}, \ldots, Y_{Kl}, Z_l)$. Hereafter, we call this channel the parallel degraded multi-receiver wiretap channel[1]. Although [24] established the common message secrecy capacity for this class of channels, in fact, their result is valid for the broader class in which we have either

$$X_l \to Y_{kl} \to Z_l \tag{3.13}$$

or

$$X_l \to Z_l \to Y_{kl} \tag{3.14}$$

valid for every X_l and for any (k, l) pair where $k \in \{1, \ldots, K\}$, $l \in \{1, \ldots, M\}$. Thus, it is sufficient to have a degradedness order between each user and the eavesdropper in any sub-channel instead of the long Markov chain between all users and the eavesdropper as in (3.12).

Here, we focus on a broader class of channels where in each sub-channel, for any

[1]In [24], these channels are called *reversely degraded* parallel channels. Here, we call them parallel degraded multi-receiver wiretap channels to be consistent with the terminology used in the rest of the chapter.

given user, either the user's channel is less noisy than the eavesdropper's channel, or vice versa. More formally, we have either

$$I(U;Y_{kl}) > I(U;Z_l) \tag{3.15}$$

or

$$I(U;Y_{kl}) < I(U;Z_l) \tag{3.16}$$

for all $U \to X_l \to (Y_{kl}, Z)$ and any (k,l) pair where $k \in \{1,\ldots,K\}$, $l \in \{1,\ldots,M\}$. Hereafter, we call this channel *the parallel multi-receiver wiretap channel with a more noisy eavesdropper*. Since the Markov chain in (3.12) implies either (3.15) or (3.16), the parallel multi-receiver wiretap channel with a more noisy eavesdropper contains the parallel degraded multi-receiver wiretap channel studied in [24].

A $(2^{nR}, n)$ code for this channel consists of a message set, $\mathcal{W}_0 = \{1,\ldots,2^{nR}\}$, an encoder, $f : \mathcal{W}_0 \to \mathcal{X}_1^n \times \ldots \times \mathcal{X}_M^n$, K decoders, one at each legitimate receiver $g_k : \mathcal{Y}_{k1} \times \ldots \times \mathcal{Y}_{kM} \to \mathcal{W}_0, k = 1,\ldots,K$. The probability of error is defined as $P_e^n = \max_{k=1,\ldots,K} \Pr\left[\hat{W}_{k0} \neq W_0\right]$ where $\hat{W}_{k0}$ is the kth user's decoder output. The secrecy of the common message is measured through the equivocation rate which is defined as $\frac{1}{n}H(W_0|Z_1^n,\ldots,Z_M^n)$. A common message secrecy rate, R, is said to be achievable if there exists a code such that $\lim_{n\to\infty} P_e^n = 0$, and

$$\lim_{n\to\infty} \frac{1}{n} H(W_0|Z_1^n,\ldots,Z_M^n) \geq R \tag{3.17}$$

The common message secrecy capacity is the supremum of all achievable secrecy rates.

The common message secrecy capacity of the parallel multi-receiver wiretap channel with a more noisy eavesdropper is stated in the following theorem whose proof is given in Appendix 3.7.2.

Theorem 3.2 *The common message secrecy capacity, C_0, of the parallel multi-receiver wiretap channel with a more noisy eavesdropper is given by*

$$C_0 = \max \min_{k=1,\ldots,K} \sum_{l=1}^{M} \left[I(X_l; Y_{kl}) - I(X_l; Z_l) \right]^+ \tag{3.18}$$

where the maximization is over all distributions of the form $p(x_1, \ldots, x_M) = \prod_{l=1}^{M} p(x_l)$.

Remark 3.2 *Theorem 3.2 implies that we should not use the sub-channels in which there is no user that has a less noisy channel than the eavesdropper. Moreover, Theorem 3.2 shows that the use of independent inputs in each sub-channel is sufficient to achieve the capacity, i.e., inducing correlation between channel inputs of sub-channels cannot provide any improvement. This is similar to the results of [28, 29] in the sense that [28, 29] established the optimality of the use of independent inputs in each sub-channel for the product of two degraded broadcast channels.*

As stated earlier, the parallel multi-receiver wiretap channel with a more noisy eavesdropper encompasses the parallel degraded multi-receiver wiretap channel studied in [24]. Hence, we can specialize Theorem 3.2 to recover the common message secrecy capacity of the parallel degraded multi-receiver wiretap channel established

in [24]. This is stated in the following corollary whose proof can be carried out from Theorem 3.2 by noting the Markov chain $X_l \to Y_{kl} \to Z_l,\ \forall(k,l)$.

Corollary 3.2 *The common message secrecy capacity of the parallel degraded multi-receiver wiretap channel is given by*

$$C_0 = \max \min_{k=1,\ldots,K} \sum_{l=1}^{M} I(X_l; Y_{kl}|Z_l) \tag{3.19}$$

where the maximization is over all distributions of the form $p(x_1,\ldots,x_M) = \prod_{l=1}^{M} p(x_l)$.

3.3.2 The Sum Secrecy Capacity

We now consider the scenario where the transmitter sends an independent confidential message to each legitimate receiver, and focus on the sum secrecy capacity. We consider a class of parallel multi-receiver wiretap channels where the legitimate receivers and the eavesdropper exhibit a certain less noisiness order in each sub-channel. These less noisiness orders are not necessarily the same for all sub-channels. Therefore, the overall channel does not have a less noisiness order. In the lth sub-channel, for all $U \to X_l \to (Y_{1l},\ldots,Y_{Kl},Z_l)$, we have

$$I(U;Y_{\pi_l(1)}) > I(U;Y_{\pi_l(2)}) > \ldots > I(U;Y_{\pi_l(K+1)}) \tag{3.20}$$

where $(Y_{\pi_l(1)}, Y_{\pi_l(2)},\ldots,Y_{\pi_l(K+1)})$ is a permutation of $(Y_{1l},\ldots,Y_{Kl},Z_l)$. We call this channel *the parallel multi-receiver wiretap channel with a less noisiness order in each sub-channel*. We note that this class of channels is a subset of the paral-

lel multi-receiver wiretap channel with a more noisy eavesdropper studied in Section 3.3.1, because of the additional ordering imposed between users' sub-channels. We also note that the class of parallel degraded multi-receiver wiretap channels with a degradedness order in each sub-channel studied in [24] is not only a subset of parallel multi-receiver wiretap channels with a more noisy eavesdropper studied in Section 3.3.1 but also a subset of parallel multi-receiver wiretap channels with a less noisiness order in each sub-channel studied in this section.

A $(2^{nR_1}\ldots,2^{nR_K},n)$ code for this channel consists of K message sets, $\mathcal{W}_k = \{1,\ldots,2^{nR_k}\}, k=1,\ldots,K$, an encoder, $f:\mathcal{W}_1\times\ldots\times\mathcal{W}_K\rightarrow\mathcal{X}_1^n\times\ldots\times\mathcal{X}_M^n$, K decoders, one at each legitimate receiver $g_k:\mathcal{Y}_{k1}\times\ldots\times\mathcal{Y}_{kM}\rightarrow\mathcal{W}_k, k=1,\ldots,K$. The probability of error is defined as $P_e^n=\max_{k=1,\ldots,K}\Pr\left[\hat{W}_k\neq W_k\right]$ where $\hat{W}_k$ is the kth user's decoder output. The secrecy is measured through the equivocation rate which is defined as $\frac{1}{n}H(W_1,\ldots,W_K|Z_1^n,\ldots,Z_M^n)$. A sum secrecy rate, R_s, is said to be achievable if there exists a code such that $\lim_{n\rightarrow\infty}P_e^n=0$, and

$$\lim_{n\rightarrow\infty}\frac{1}{n}H(W_1,\ldots,W_K|Z_1^n,\ldots,Z_M^n)\geq R_s \tag{3.21}$$

The sum secrecy capacity is defined to be the supremum of all achievable sum secrecy rates.

The sum secrecy capacity for the class of parallel multi-receiver wiretap channels with a less noisiness order in each sub-channel studied in this section is stated in the following theorem whose proof is given in Appendix 3.7.3.

Theorem 3.3 *The sum secrecy capacity of the parallel multi-receiver wiretap chan-*

nel with a less noisiness order in each sub-channel is given by

$$\max \sum_{l=1}^{M} \left[I(X_l; Y_{\rho(l)l}) - I(X_l; Z_l) \right]^+ \tag{3.22}$$

where the maximization is over all input distributions of the form $p(x_1, \ldots, x_M) = \prod_{l=1}^{M} p(x_l)$ *and* $\rho(l)$ *denotes the index of the strongest user in the* l*th sub-channel in the sense that*

$$I(U; Y_{kl}) \leq I(U; Y_{\rho(l)l}) \tag{3.23}$$

for all $U \to X_l \to (Y_{1l}, \ldots, Y_{Kl}, Z_l)$ *and any* $k \in \{1, \ldots, K\}$.

Remark 3.3 *Theorem 3.3 implies that the sum secrecy capacity is achieved by sending information only to the strongest user in each sub-channel. As in Theorem 3.2, here also, the use of independent inputs for each sub-channel is capacity-achieving, which is again reminiscent of the result in [28, 29] about the optimality of the use of independent inputs in each sub-channel for the product of two degraded broadcast channels.*

As mentioned earlier, since the class of parallel multi-receiver wiretap channels with a less noisiness order in each sub-channel contains the class of parallel degraded multi-receiver wiretap channels studied in [24], Theorem 3.3 can be specialized to give the sum secrecy capacity of the latter class of channels as well. This result was originally obtained in [24]. This is stated in the following corollary. Since the proof of this corollary is similar to the proof of Corollary 3.2, we omit its proof.

Corollary 3.3 *The sum secrecy capacity of the parallel degraded multi-receiver wiretap channel is given by*

$$\max \sum_{l=1}^{M} I(X_l; Y_{\rho(l)l} | Z_l) \tag{3.24}$$

where the maximization is over all input distributions of the form $p(x_1, \ldots, x_M) = \prod_{l=1}^{M} p(x_l)$ *and* $\rho(l)$ *denotes the index of the strongest user in the* l*th sub-channel in the sense that*

$$X_l \to Y_{\rho(l)l} \to Y_{kl} \tag{3.25}$$

for all input distributions on X_l *and any* $k \in \{1, \ldots, K\}$.

So far, we have considered special classes of parallel multi-receiver wiretap channels for specific scenarios and obtained results similar to [24], only for broader classes of channels. In particular, in Section 3.3.1, we focused on the transmission of a common message, whereas in Section 3.3.2, we focused on the sum secrecy capacity when only independent messages are transmitted to all users. In the subsequent sections, we will specialize our channel model, but we will develop stronger and more comprehensive results. In particular, we will let the transmitter send both common and independent messages, and we will characterize the entire secrecy capacity region.

3.4 Parallel Degraded Multi-receiver Wiretap Channels

We consider a special class of parallel degraded multi-receiver wiretap channels with two sub-channels, two users and one eavesdropper. We consider the most general scenario where each user receives both an independent message and a common message. All messages are to be kept secret from the eavesdropper.

For the special class of parallel degraded multi-receiver wiretap channels in consideration, there is a specific degradation order in each sub-channel. In particular, we have the following Markov chain

$$X_1 \to Y_{11} \to Y_{21} \to Z_1 \tag{3.26}$$

in the first sub-channel, and the following Markov chain

$$X_2 \to Y_{22} \to Y_{12} \to Z_2 \tag{3.27}$$

in the second sub-channel. Consequently, although in each sub-channel, one user is degraded with respect to the other one, this does not hold for the overall channel, and the overall channel is not degraded for any user. The corresponding channel transition probability is

$$p(y_{11}|x_1)p(y_{21}|y_{11})p(z_1|y_{21})p(y_{22}|x_2)p(y_{12}|y_{22})p(z_2|y_{12}) \tag{3.28}$$

If we ignore the eavesdropper by setting $Z_1 = Z_2 = \phi$, this channel model reduces

to the broadcast channel that was studied in [28, 29].

A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for this channel consists of three message sets, $\mathcal{W}_0 = \{1, \ldots, 2^{nR_0}\}$, $\mathcal{W}_j = \{1, \ldots, 2^{nR_j}\}, j = 1, 2$, one encoder $f : \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}_1^n \times \mathcal{X}_2^n$, two decoders one at each legitimate receiver $g_j : \mathcal{Y}_{j1}^n \times \mathcal{Y}_{j2}^n \to \mathcal{W}_0 \times \mathcal{W}_j, j = 1, 2$. The probability of error is defined as $P_e^n = \max_{j=1,2} \Pr\left[g_j(Y_{j1}^n, Y_{j2}^n) \neq (W_0, W_j)\right]$. A rate tuple (R_0, R_1, R_2) is said to be achievable if there exists a code such that $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z_1^n, Z_2^n) \geq \sum_{k\in\mathcal{S}(W)} R_k, \quad \forall\ \mathcal{S}(W) \tag{3.29}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_0, W_1, W_2\}$. The secrecy capacity region is the closure of all achievable secrecy rate tuples.

The secrecy capacity region of this parallel degraded multi-receiver wiretap channel is characterized by the following theorem whose proof is given in Appendix 3.7.4.

Theorem 3.4 *The secrecy capacity region of the parallel degraded multi-receiver wiretap channel defined by (3.28) is the union of the rate tuples* (R_0, R_1, R_2) *satisfying*

$$R_0 \leq I(U_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) \tag{3.30}$$

$$R_0 \leq I(U_1; Y_{21}|Z_1) + I(U_2; Y_{22}|Z_2) \tag{3.31}$$

$$R_0 + R_1 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) \tag{3.32}$$

$$R_0 + R_2 \leq I(X_2; Y_{22}|Z_2) + I(U_1; Y_{21}|Z_1) \tag{3.33}$$

$$R_0 + R_1 + R_2 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) + I(X_2; Y_{22}|U_2, Z_2) \tag{3.34}$$

$$R_0 + R_1 + R_2 \leq I(X_2; Y_{22}|Z_2) + I(U_1; Y_{21}|Z_1) + I(X_1; Y_{11}|U_1, Z_1) \tag{3.35}$$

where the union is over all distributions of the form $p(u_1, u_2, x_1, x_2) = p(u_1, x_1)p(u_2, x_2)$.

Remark 3.4 *If we let the encoder use an arbitrary joint distribution* $p(u_1, x_1, u_2, x_2)$ *instead of the ones that satisfy* $p(u_1, x_1, u_2, x_2) = p(u_1, x_1)p(u_2, x_2)$*, this would not enlarge the region given in Theorem 3.4, because all rate expressions in Theorem 3.4 depend on either* $p(u_1, x_1)$ *or* $p(u_2, x_2)$ *but not on the joint distribution* $p(u_1, u_2, x_1, x_2)$.

Remark 3.5 *The capacity achieving scheme uses either superposition coding in both sub-channels or superposition coding in one of the sub-channels, and a dedicated transmission in the other one. We again note that this superposition coding is different from the standard one [22] in the sense that it associates each message with many codewords by using stochastic encoding at each layer of the code due to secrecy concerns.*

Remark 3.6 *If we set* $Z_1 = Z_2 = \phi$*, we recover the capacity region of the underlying broadcast channel [29].*

Remark 3.7 *If we disable one of the sub-channels, say the first one, by setting* $Y_{11} = Y_{21} = Z_1 = \phi$*, the parallel degraded multi-receiver wiretap channel of this section reduces to the degraded multi-receiver wiretap channel of Section 3.2. The*

corresponding secrecy capacity region is then given by the union of the rate tuples (R_0, R_1, R_2) *satisfying*

$$R_0 + R_1 \leq I(U_2; Y_{12}|Z_2) \tag{3.36}$$

$$R_0 + R_1 + R_2 \leq I(X_2; Y_{22}|U_2, Z_2) + I(U_2; Y_{12}|Z_2) \tag{3.37}$$

where the union is over all $p(u_2, x_2)$*. This region can be obtained through either Corollary 3.1 or Theorem 3.4 (by setting* $Y_{11} = Y_{21} = Z_1 = \phi$ *and eliminating redundant bounds) implying the consistency of the results.*

Next, we consider the scenario where the transmitter does not send a common message, and find the secrecy capacity region.

Corollary 3.4 *The secrecy capacity region of the parallel degraded multi-receiver wiretap channel defined through (3.28) with no common message is given by the union of the rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) \tag{3.38}$$

$$R_2 \leq I(X_2; Y_{22}|Z_2) + I(U_1; Y_{21}|Z_1) \tag{3.39}$$

$$R_1 + R_2 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) + I(X_2; Y_{22}|U_2, Z_2) \tag{3.40}$$

$$R_1 + R_2 \leq I(X_2; Y_{22}|Z_2) + I(U_1; Y_{21}|Z_1) + I(X_1; Y_{11}|U_1, Z_1) \tag{3.41}$$

where the union is over all distributions of the form $p(u_1)p(u_2)p(x_1|u_1)p(x_2|u_2)$*.*

Proof: Since the common message rate can be exchanged with any user's

independent message rate, we set $R_0 = \alpha + \beta, R_1' = R_1 + \alpha, R_2' = R_2 + \beta$ where $\alpha, \beta \geq 0$. Plugging these expressions into the rates in Theorem 3.4 and using Fourier-Moztkin elimination, we get the region given in the corollary. $\square$

Remark 3.8 *If we disable the eavesdropper by setting $Z_{11} = Z_{22} = \phi$, we recover the capacity region of the underlying broadcast channel without a common message, which was found originally in [28].*

At this point, one may ask whether the results of this section can be extended to arbitrary numbers of users and parallel sub-channels. Once we have Theorem 3.4, the extension of the results to an arbitrary number of parallel sub-channels is rather straightforward. Let us consider the parallel degraded multi-receiver wiretap channel with M sub-channels, and in each sub-channel, we have either the following Markov chain

$$X_l \to Y_{1l} \to Y_{2l} \to Z_l \tag{3.42}$$

or this Markov chain

$$X_l \to Y_{2l} \to Y_{1l} \to Z_l \tag{3.43}$$

for any $l \in \{1, \ldots, M\}$. We define the set of indices $\mathcal{S}_1$ (resp. $\mathcal{S}_2$) as those where for every $l \in \mathcal{S}_1$ (resp. $l \in \mathcal{S}_2$), the Markov chain in (3.42) (resp. in (3.43)) is satisfied. Then, using Theorem 3.4, we obtain the secrecy capacity region of the channel with two users and M sub-channels as given in the following theorem which is proved in

Appendix 3.7.5.

Theorem 3.5 *The secrecy capacity region of the parallel degraded multi-receiver wiretap channel with M sub-channels, where each sub-channel satisfies either (3.42) or (3.43) is given by the union of the rate tuples (R_0, R_1, R_2) satisfying*

$$R_0 \leq \sum_{l=1}^{M} I(U_l; Y_{1l}|Z_l) \tag{3.44}$$

$$R_0 \leq \sum_{l=1}^{M} I(U_l; Y_{2l}|Z_l) \tag{3.45}$$

$$R_0 + R_1 \leq \sum_{l\in\mathcal{S}_1} I(X_l; Y_{1l}|Z_l) + \sum_{l\in\mathcal{S}_2} I(U_l; Y_{1l}|Z_l) \tag{3.46}$$

$$R_0 + R_2 \leq \sum_{l\in\mathcal{S}_2} I(X_l; Y_{2l}|Z_l) + \sum_{l\in\mathcal{S}_1} I(U_l; Y_{2l}|Z_l) \tag{3.47}$$

$$R_0 + R_1 + R_2 \leq \sum_{l\in\mathcal{S}_1} I(X_l; Y_{1l}|Z_l) + \sum_{l\in\mathcal{S}_2} I(U_l; Y_{1l}|Z_l) + \sum_{l\in\mathcal{S}_2} I(X_l; Y_{2l}|U_l, Z_l) \tag{3.48}$$

$$R_0 + R_1 + R_2 \leq \sum_{l\in\mathcal{S}_2} I(X_l; Y_{2l}|Z_l) + \sum_{l\in\mathcal{S}_1} I(U_l; Y_{2l}|Z_l) + \sum_{l\in\mathcal{S}_1} I(X_l; Y_{1l}|U_l, Z_l) \tag{3.49}$$

where the union is over all distributions of the form $\prod_{l=1}^{M} p(u_l, x_l)$.

We are now left with the question whether these results can be generalized to an arbitrary number of users. If we consider the parallel degraded multi-receiver wiretap channel with more than two sub-channels and an arbitrary number of users, the secrecy capacity region for the scenario where each user receives a common message in addition to an independent message does not seem to be characterizable. Our intuition comes from the fact that, as of now, the capacity region of the corresponding broadcast channel without secrecy constraints is unknown [30]. However, if we consider the scenario where each user receives only an independent message,

i.e., there is no common message, then the secrecy capacity region may be found, because the capacity region of the corresponding broadcast channel without secrecy constraints can be established [30], although there is no explicit expression for it in the literature. We expect this particular generalization to be rather straightforward, and do not pursue it here.

3.5 Sum of Degraded Multi-receiver Wiretap Channels

We now consider a different multi-receiver wiretap channel which can be viewed as a sum of two degraded multi-receiver wiretap channels with two users and one eavesdropper. In this channel model, the transmitter has two non-intersecting input alphabets, i.e., $\mathcal{X}_1, \mathcal{X}_2$ with $\mathcal{X}_1 \cap \mathcal{X}_2 = \emptyset$, and each receiver has two non-intersecting alphabets, i.e., $\mathcal{Y}_{j1}, \mathcal{Y}_{j2}$ with $\mathcal{Y}_{j1} \cap \mathcal{Y}_{j2} = \emptyset$ for the jth user, $j = 1, 2$, and $\mathcal{Z}_1, \mathcal{Z}_2$ with $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$ for the eavesdropper. The channel is again memoryless with transition probability

$$p(y_1, y_2, z|x) = \begin{cases} p(y_{11}|x_1)p(y_{21}|y_{11})p(z_1|y_{21}) & \text{if } (x, y_1, y_2, z) \in \mathcal{X}_1 \times \mathcal{Y}_{11} \times \mathcal{Y}_{21} \times \mathcal{Z}_1 \\ p(y_{22}|x_2)p(y_{12}|y_{22})p(z_2|y_{12}) & \text{if } (x, y_1, y_2, z) \in \mathcal{X}_2 \times \mathcal{Y}_{21} \times \mathcal{Y}_{22} \times \mathcal{Z}_2 \\ 0 & \text{otherwise} \end{cases} \tag{3.50}$$

where $x \in \mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$, $y_j \in \mathcal{Y}_j = \mathcal{Y}_{j1} \cup \mathcal{Y}_{j2}, j = 1, 2$ and $z \in \mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2$. Thus, if the transmitter chooses to use its first alphabet, i.e., $\mathcal{X}_1$, the second user (resp. eavesdropper) receives a degraded version of user 1's (resp. user 2's) observation. However, if the transmitter uses its second alphabet, i.e., $\mathcal{X}_2$, the first

user (resp. eavesdropper) receives a degraded version of user 2's (resp. user 1's) observation. Consequently, the overall channel is not degraded from any user's perspective, however it is degraded from the eavesdropper's perspective.

A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for this channel consists of three message sets, $w_0 \in \mathcal{W}_0 = \{1, \ldots, 2^{nR_0}\}$, $w_j \in \mathcal{W}_j = \{1, \ldots, 2^{nR_j}\}, j = 1, 2$, one encoder $f : \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$ and two decoders, one at each legitimate receiver, $g_j : \mathcal{Y}_j^n \to \mathcal{W}_0 \times \mathcal{W}_j, j = 1, 2$. The probability of error is defined as $P_e^n = \max_{j=1,2} \Pr\left[g_j(Y_j^n) \neq (W_0, W_j)\right]$. A rate tuple (R_0, R_1, R_2) is said to be achievable if there exists a code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z^n) \geq \sum_{j \in \mathcal{S}(W)} R_j, \quad \forall\, \mathcal{S}(W) \tag{3.51}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_0, W_1, W_2\}$. The secrecy capacity region is the closure of all achievable secrecy rate tuples.

The secrecy capacity region of this channel is given in the following theorem which is proved in Appendix 3.7.6.

Theorem 3.6 *The secrecy capacity region of the sum of two degraded multi-receiver wiretap channels is given by the union of the rate tuples* (R_0, R_1, R_2) *satisfying*

$$R_0 \leq \alpha I(U_1; Y_{11}|Z_1) + \bar{\alpha} I(U_2; Y_{12}|Z_2) \tag{3.52}$$

$$R_0 \leq \alpha I(U_1; Y_{21}|Z_1) + \bar{\alpha} I(U_2; Y_{22}|Z_2) \tag{3.53}$$

$$R_0 + R_1 \leq \alpha I(X_1; Y_{11}|Z_1) + \bar{\alpha} I(U_2; Y_{12}|Z_2) \tag{3.54}$$

$$R_0 + R_2 \leq \alpha I(U_1; Y_{21}|Z_1) + \bar{\alpha} I(X_2; Y_{22}|Z_2) \tag{3.55}$$

$$R_0 + R_1 + R_2 \leq \alpha I(X_1; Y_{11}|Z_1) + \bar{\alpha} I(U_2; Y_{12}|Z_2) + \bar{\alpha} I(X_2; Y_{22}|U_2, Z_2) \tag{3.56}$$

$$R_0 + R_1 + R_2 \leq \alpha I(U_1; Y_{21}|Z_1) + \alpha I(X_1; Y_{11}|U_1, Z_1) + \bar{\alpha} I(X_2; Y_{22}|Z_2) \tag{3.57}$$

where the union is over all $\alpha \in [0, 1]$ *and distributions of the form* $p(u_1, u_2, x_1, x_2) = p(u_1, x_1)p(u_2, x_2)$.

Remark 3.9 *This channel model is similar to the parallel degraded multi-receiver wiretap channel of the previous section in the sense that it can be viewed to consist of two parallel sub-channels, however now the transmitter cannot use both sub-channels simultaneously. Instead, it should invoke a time-sharing approach between these two so-called parallel sub-channels (*α *reflects this concern). Moreover, superposition coding scheme again achieves the boundary of the secrecy capacity region, however it differs from the standard one [22] in the sense that it needs to be modified to incorporate secrecy constraints, i.e., it needs to use stochastic encoding to associate each message with multiple codewords.*

Remark 3.10 *An interesting point about the secrecy capacity region is that if we drop the secrecy constraints by setting* $Z_1 = Z_2 = \phi$*, we are unable to recover the capacity region of the corresponding broadcast channel that was found in [29]. After setting* $Z_1 = Z_2 = \phi$*, we note that each expression in Theorem 3.6 and its counterpart describing the capacity region [29] differ by exactly* $h(\alpha)$*. The reason for this is as follows. Here,* α *not only denotes the time-sharing variable but also carries*

an additional information, i.e., the change of the channel that is in use is part of the information transmission. However, since the eavesdropper can also decode these messages, the term $h(\alpha)$, which is the amount of information that can be transmitted via changes of the channel in use, disappears in the secrecy capacity region.

3.6 Conclusions

In this chapter, we study the secure broadcasting problem for degraded multi-receiver wiretap channels, parallel multi-receiver wiretap channels with a more noisy eavesdropper, parallel multi-receiver wiretap channels with less noisiness orderings in each sub-channel, and parallel degraded multi-receiver wiretap channels. Our motivation to focus on these specific channel models comes from the fact that although the broadcast channel problem is a largely open problem, its solution, i.e., the capacity region, is known for the specific cases listed above. Hence, by obtaining either a partial characterization of the secrecy capacity region or the entire secrecy capacity region for these specific instances of the secure broadcasting problem, we bring the literature of the secure broadcasting problem to the level of the literature on the broadcast channel problem.

3.7 Appendix

3.7.1 Proof of Theorem 3.1

First, we show achievability, then provide the converse.

3.7.1.1 Achievability

Fix the probability distribution as

$$p(u_1)p(u_2|u_1)\dots p(u_{K-1}|u_{K-2})p(x|u_{K-1}) \tag{3.58}$$

Codebook generation:

- Generate $2^{n(R_0+R_1+\tilde{R}_1)}$ length-n sequences $\mathbf{u}_1$ through $p(\mathbf{u}_1)=\prod_{i=1}^{n}p(u_{1,i})$ and index them as $\mathbf{u}_1(w_0,w_1,\tilde{w}_1)$ where $w_0\in\left\{1,\dots,2^{nR_0}\right\}$, $w_1\in\left\{1,\dots,2^{nR_1}\right\}$ and $\tilde{w}_1\in\left\{1,\dots,2^{n\tilde{R}_1}\right\}$.

- For each $\mathbf{u}_{j-1}$, where $j=2,\dots,K-1$, generate $2^{n(R_j+\tilde{R}_j)}$ length-n sequences $\mathbf{u}_j$ through $p(\mathbf{u}_j|\mathbf{u}_{j-1})=\prod_{i=1}^{n}p(u_{j,i}|u_{j-1,i})$ and index them as $\mathbf{u}_j(w_0,w_1,\dots,w_j,\tilde{w}_1,\dots,\tilde{w}_j)$ where $w_j\in\left\{1,\dots,2^{nR_j}\right\}$ and $\tilde{w}_j\in\left\{1,\dots,2^{n\tilde{R}_j}\right\}$.

- Finally, for each $\mathbf{u}_{K-1}$, generate $2^{n(R_K+\tilde{R}_K)}$ length-n sequences $\mathbf{x}$ through $p(\mathbf{x}|\mathbf{u}_{K-1})=\prod_{i=1}^{n}p(x_i|u_{K,i})$ and index them as $\mathbf{x}(w_0,w_1,\dots,w_K,\tilde{w}_1,\dots,\tilde{w}_K)$ where $w_K\in\left\{1,\dots,2^{nR_K}\right\}$ and $\tilde{w}_K\in\left\{1,\dots,2^{n\tilde{R}_K}\right\}$.

- Furthermore, we set

$$\tilde{R}_i=I(U_i;Z|U_{i-1}),\quad i=1,\dots,K \tag{3.59}$$

  where $U_0=\phi$ and $U_K=X$.

Encoding:

Assume the messages to be transmitted are $(w_0, w_1, \ldots, w_K)$. Then, the encoder randomly picks a set $(\tilde{w}_1, \ldots, \tilde{w}_K)$ and sends $\mathbf{x}(w_0, w_1, \ldots, w_K, \tilde{w}_1, \ldots, \tilde{w}_K)$.

Decoding:

It is straightforward to see that if the following conditions are satisfied,

$$R_0 + R_1 + \tilde{R}_1 \leq I(U_1; Y_1) \tag{3.60}$$

$$R_j + \tilde{R}_j \leq I(U_j; Y_j|U_{j-1}), \quad j = 2, \ldots, K-1 \tag{3.61}$$

$$R_K + \tilde{R}_K \leq I(X; Y_K|U_{K-1}) \tag{3.62}$$

then all users can decode both the common message and the independent message directed to itself with vanishingly small error probability. Moreover, since the channel is degraded, each user, say the jth one, can decode all of the independent messages intended for the users whose channels are degraded with respect to the jth user's channel. Thus, these degraded users' rates can be exploited to increase the jth user's rate which leads to the following achievable region

$$R_0 + \sum_{j=1}^{\ell} R_j + \sum_{j=1}^{\ell} \tilde{R}_j \leq \sum_{j=1}^{\ell} I(U_j; Y_j|U_{j-1}), \quad \ell = 1, \ldots, K \tag{3.63}$$

where $U_0 = \phi$ and $U_K = X$. Moreover, after eliminating $\left\{\tilde{R}_j\right\}_{j=1}^{K}$, (3.63) can be expressed as

$$R_0 + \sum_{j=1}^{\ell} R_j \leq \sum_{j=1}^{\ell} I(U_j; Y_j|U_{j-1}) - I(U_\ell; Z), \quad \ell = 1, \ldots, K \tag{3.64}$$

where we used the fact that

$$\sum_{j=1}^{\ell} \tilde{R}_j = \sum_{j=1}^{\ell} I(U_j; Z|U_{j-1}) = I(U_1, \ldots, U_\ell; Z) = I(U_\ell; Z) \tag{3.65}$$

where the second and the third equalities are due to the following Markov chain

$$U_1 \to \ldots \to U_{K-1} \to X \to Z \tag{3.66}$$

Equivocation computation:

We now calculate the equivocation of the code described above. To that end, we first introduce the following lemma which states that a code satisfying the sum rate secrecy constraint fulfills all other secrecy constraints.

Lemma 3.1 *If the sum rate secrecy constraint is satisfied, i.e.,*

$$\frac{1}{n} H(W_0, W_1, \ldots, W_K|Z^n) \geq \sum_{j=0}^{K} R_j - \epsilon_n \tag{3.67}$$

then all other secrecy constraints are satisfied as well, i.e.,

$$\frac{1}{n} H(\mathcal{S}(W)|Z^n) \geq \sum_{j \in \mathcal{S}(W)} R_j - \epsilon_n \tag{3.68}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_0, W_1, \ldots, W_K\}$.

Proof: The proof of this lemma is as follows.

$$\frac{1}{n}H(\mathcal{S}(W)|Z^n) = \frac{1}{n}H(\mathcal{S}(W), \mathcal{S}^c(W)|Z^n) - \frac{1}{n}H(\mathcal{S}^c(W)|\mathcal{S}(W), Z^n) \tag{3.69}$$

$$\geq \sum_{j=0}^{K} R_j - \epsilon_n - \frac{1}{n}H(\mathcal{S}^c(W)|\mathcal{S}(W), Z^n) \tag{3.70}$$

$$= \sum_{j\in\mathcal{S}(W)} R_j - \epsilon_n + \sum_{j\in\mathcal{S}^c(W)} R_j - \frac{1}{n}H(\mathcal{S}^c(W)|\mathcal{S}(W), Z^n) \tag{3.71}$$

$$= \sum_{j\in\mathcal{S}(W)} R_j - \epsilon_n + \frac{1}{n}H(\mathcal{S}^c(W)) - \frac{1}{n}H(\mathcal{S}^c(W)|\mathcal{S}(W), Z^n) \tag{3.72}$$

$$\geq \sum_{j\in\mathcal{S}(W)} R_j - \epsilon_n \tag{3.73}$$

where (3.70) is due to the fact that we assumed that sum rate secrecy constraint (3.67) is satisfied and (3.72) follows from

$$\sum_{j\in\mathcal{S}^c(W)} R_j = \frac{1}{n}H(\mathcal{S}^c(W)) \tag{3.74}$$

which is a consequence of the fact that message sets are uniformly and independently distributed. □

Hence, it is sufficient to check whether coding scheme presented satisfies the

sum rate secrecy constraint.

$$H(W_0, W_1, \ldots, W_K|Z^n) = H(W_0, W_1, \ldots, W_K, Z^n) - H(Z^n) \tag{3.75}$$

$$= H(U_1^n, \ldots, U_{K-1}^n, X^n, W_0, W_1, \ldots, W_K, Z^n) - H(Z^n)$$

$$- H(U_1^n, \ldots, U_{K-1}^n, X^n|W_0, W_1, \ldots, W_K, Z^n) \tag{3.76}$$

$$= H(U_1^n, \ldots, U_{K-1}^n, X^n) + H(W_0, W_1, \ldots, W_K, Z^n|U_1^n, \ldots, U_{K-1}^n, X^n) - H(Z^n)$$

$$- H(U_1^n, \ldots, U_{K-1}^n, X^n|W_0, W_1, \ldots, W_K, Z^n) \tag{3.77}$$

$$\geq H(U_1^n, \ldots, U_{K-1}^n, X^n) - I(U_1^n, \ldots, U_{K-1}^n, X^n; Z^n)$$

$$- H(U_1^n, \ldots, U_{K-1}^n, X^n|W_0, W_1, \ldots, W_K, Z^n) \tag{3.78}$$

where each term will be treated separately. Since given $U_k^n = u_k^n$, U_{k+1}^n can take $2^{n(R_{k+1}+\tilde{R}_{k+1})}$ values uniformly, the first term is

$$H(U_1^n, \ldots, U_{K-1}^n, X^n) = H(U_1^n) + \sum_{k=2}^{K-1} H(U_k^n|U_{k-1}^n) + H(X^n|U_{K-1}^n) \tag{3.79}$$

$$= nR_0 + n\sum_{k=1}^{K} R_k + n\sum_{k=1}^{K} \tilde{R}_k \tag{3.80}$$

where the first equality follows from the following Markov chain

$$U_1^n \to U_2^n \to \ldots \to U_{K-1}^n \to X^n \tag{3.81}$$

The second term in (3.78) is

$$I(U_1^n, \ldots, U_{K-1}^n, X^n; Z^n) = I(X^n; Z^n) + I(U_1^n, U_2^n, \ldots, U_{K-1}^n; Z^n | X^n) \tag{3.82}$$

$$= I(X^n; Z^n) \tag{3.83}$$

$$\leq nI(X; Z) + \gamma_n \tag{3.84}$$

where (3.83) follows from the Markov chain in (3.81) and (3.84) can be shown by following the approach devised in [2]. We now bound the third term in (3.78). To that end, assume that the eavesdropper tries to decode $\left(U_1^n, \ldots, U_{K-1}^n, X^n\right)$ using the side information $(W_0, W_1, \ldots, W_K)$ which is equivalent to decoding $\left(\tilde{W}_1, \ldots, \tilde{W}_K\right)$. Since $\tilde{R}_j$s are selected to ensure that the eavesdropper can decode them successively, see (3.59), then using Fano's lemma, we have

$$H(U_1^n, \ldots, U_{K-1}^n, X^n | W_0, W_1, \ldots, W_K, Z^n) \leq \epsilon_n \tag{3.85}$$

Thus, using (3.80), (3.84) and (3.85) in (3.78), we get

$$H(W_0, W_1, \ldots, W_K | Z^n) \geq n \sum_{j=0}^{K} R_j + n \sum_{j=1}^{K} \tilde{R}_j - nI(X; Z) - \epsilon_n \tag{3.86}$$

$$= n \sum_{j=0}^{K} R_j - \epsilon_n - \gamma_n \tag{3.87}$$

where (3.87) follows from the following, see (3.59) and (3.65),

$$\sum_{j=1}^{K} \tilde{R}_j = I(X;Z) \tag{3.88}$$

3.7.1.2 Converse

First let us define the following auxiliary random variables,

$$U_{k,i} = W_0 W_1 \dots W_k Y_{k+1}^{i-1} Z_{i+1}^n, \quad k = 1, \dots, K-1 \tag{3.89}$$

which satisfy the following Markov chain

$$U_{1,i} \to U_{2,i} \to \dots \to U_{K-1,i} \to X_i \to (Z_i, Y_{K,i}, \dots, Y_{1,i}) \tag{3.90}$$

To provide a converse, we will show

$$\frac{1}{n} H(W_0, W_1, \dots, W_\ell | Z^n) \leq \sum_{k=1}^{\ell} I(U_k; Y_k | U_{k-1}) - I(U_\ell; Z), \quad \ell = 1, \dots, K \tag{3.91}$$

where $U_0 = \phi$, $U_K = X$. We show this in three steps. First, let us write down

$$H(W_0, W_1, \dots, W_\ell | Z^n) = H(W_0, W_1 | Z^n) + \sum_{k=2}^{\ell} H(W_k | W_0, W_1, \dots, W_{k-1}, Z^n) \tag{3.92}$$

The first term on the right hand side of (3.92) is bounded as follows,

$$H(W_0, W_1|Z^n) \leq I(W_0, W_1; Y_1^n) - I(W_0, W_1; Z^n) + \epsilon_n \tag{3.93}$$

$$\leq \sum_{i=1}^{n} I(W_0, W_1; Y_{1,i}|Y_1^{i-1}, Z_{i+1}^n) - I(W_0, W_1; Z_i|Y_1^{i-1}, Z_{i+1}^n) + \epsilon_n \tag{3.94}$$

$$\leq \sum_{i=1}^{n} I(W_0, W_1; Y_{1,i}|Y_1^{i-1}, Z_{i+1}^n) - I(W_0, W_1; Z_i|Y_1^{i-1}, Z_{i+1}^n)$$

$$+ I(Y_1^{i-1}, Z_{i+1}^n; Y_{1,i}) - I(Y_1^{i-1}, Z_{i+1}^n; Z_i) + \epsilon_n \tag{3.95}$$

$$= \sum_{i=1}^{n} I(W_0, W_1, Y_1^{i-1}, Z_{i+1}^n; Y_{1,i}) - I(W_0, W_1, Y_1^{i-1}, Z_{i+1}^n; Z_i) + \epsilon_n \tag{3.96}$$

$$\leq \sum_{i=1}^{n} I(W_0, W_1, Y_1^{i-1}, Z_{i+1}^n; Y_{1,i}) - I(W_0, W_1, Y_1^{i-1}, Z_{i+1}^n; Z_i)$$

$$+ I(Y_2^{i-1}; Y_{1,i}|W_0, W_1, Y_1^{i-1}, Z_{i+1}^n) - I(Y_2^{i-1}; Z_i|W_0, W_1, Y_1^{i-1}, Z_{i+1}^n) + \epsilon_n \tag{3.97}$$

$$= \sum_{i=1}^{n} I(W_0, W_1, Y_1^{i-1}, Z_{i+1}^n, Y_2^{i-1}; Y_{1,i}) - I(W_0, W_1, Y_1^{i-1}, Z_{i+1}^n, Y_2^{i-1}; Z_i) + \epsilon_n$$

$$\tag{3.98}$$

$$= \sum_{i=1}^{n} I(W_0, W_1, Z_{i+1}^n, Y_2^{i-1}; Y_{1,i}) - I(W_0, W_1, Z_{i+1}^n, Y_2^{i-1}; Z_i) \tag{3.99}$$

$$+ I(Y_1^{i-1}; Y_{1,i}|W_0, W_1, Z_{i+1}^n, Y_2^{i-1}) - I(Y_1^{i-1}; Z_i|W_0, W_1, Z_{i+1}^n, Y_2^{i-1}) + \epsilon_n \tag{3.100}$$

$$= \sum_{i=1}^{n} I(W_0, W_1, Z_{i+1}^n, Y_2^{i-1}; Y_{1,i}) - I(W_0, W_1, Z_{i+1}^n, Y_2^{i-1}; Z_i) + \epsilon_n \tag{3.101}$$

$$= \sum_{i=1}^{n} I(U_{1,i}; Y_{1,i}) - I(U_{1,i}; Z_i) + \epsilon_n \tag{3.102}$$

where (3.93) follows from Fano's lemma, (3.94) is obtained using Csiszar-Korner identity (see Lemma 7 of [3]), (3.95) is due to the fact that

$$I(Y_1^{i-1}, Z_{i+1}^n; Y_{1,i}) - I(Y_1^{i-1}, Z_{i+1}^n; Z_i) > 0 \tag{3.103}$$

which follows from the fact that each user's channel is less noisy with respect to the eavesdropper. Similarly, (3.97) follows from the fact that

$$I(Y_2^{i-1}; Y_{1,i}|W_0, W_1, Y_1^{i-1}, Z_{i+1}^n) - I(Y_2^{i-1}; Z_i|W_0, W_1, Y_1^{i-1}, Z_{i+1}^n) > 0 \tag{3.104}$$

which is a consequence of the fact that each user's channel is less noisy with respect to the eavesdropper's channel. Finally, (3.101) is due to the following Markov chain

$$Y_1^{i-1} \to Y_2^{i-1} \to \left(W_0, W_1, Z_{i+1}^n, Y_{1,i}, Z_i\right) \tag{3.105}$$

which is a consequence of the fact that the legitimate receivers exhibit a degradation order.

We now bound the terms of the summation in (3.92) for $2 \leq k \leq K-1$. Let us use the shorthand notation, $\tilde{W}_{k-1} = (W_0, W_1, \ldots, W_{k-1})$, then

$$H(W_k|\tilde{W}_{k-1}, Z^n) \leq I(W_k; Y_k^n|\tilde{W}_{k-1}) - I(W_k; Z^n|\tilde{W}_{k-1}) + \epsilon_n \tag{3.106}$$

$$\leq \sum_{i=1}^{n} I(W_k; Y_{k,i}|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n) - I(W_k; Z_i|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n) + \epsilon_n \tag{3.107}$$

$$\leq \sum_{i=1}^{n} I(W_k; Y_{k,i}|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n) - I(W_k; Z_i|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n)$$

$$+ I(Y_{k+1}^{i-1}; Y_{k,i}|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n, W_k) - I(Y_{k+1}^{i-1}; Z_i|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n, W_k) + \epsilon_n \tag{3.108}$$

$$= \sum_{i=1}^{n} I(W_k, Y_{k+1}^{i-1}; Y_{k,i}|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n) - I(W_k, Y_{k+1}^{i-1}; Z_i|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n) + \epsilon_n \tag{3.109}$$

$$= \sum_{i=1}^{n} I(U_{k,i}; Y_{k,i}|U_{k-1,i}) - I(U_{k,i}; Z_i|U_{k-1,i}) + \epsilon_n \tag{3.110}$$

where (3.106) follows from Fano's lemma, (3.107) is obtained through Csiszar-Korner identity, and (3.108) is a consequence of the fact that

$$I(Y_{k+1}^{i-1}; Y_{k,i}|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n, W_k) - I(Y_{k+1}^{i-1}; Z_i|\tilde{W}_{k-1}, Y_k^{i-1}, Z_{i+1}^n, W_k) > 0 \tag{3.111}$$

which follows from the fact that each user's channel is less noisy with respect to the eavesdropper's channel. Finally, we bound the following term where we again use the shorthand notation $\tilde{W}_{K-1} = (W_0, W_1, \ldots, W_{K-1})$,

$$H(W_K|\tilde{W}_{K-1}, Z^n) \leq I(W_K; Y_K^n|\tilde{W}_{K-1}) - I(W_K; Z^n|\tilde{W}_{K-1}) + \epsilon_n \tag{3.112}$$

$$\leq \sum_{i=1}^{n} I(W_K; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) - I(W_K; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) + \epsilon_n \tag{3.113}$$

$$\leq \sum_{i=1}^{n} I(W_K; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) - I(W_K; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n)$$

$$+ I(X_i; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n, W_K) - I(X_i; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n, W_K) + \epsilon_n \tag{3.114}$$

$$= \sum_{i=1}^{n} I(W_K, X_i; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) - I(W_K, X_i; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) + \epsilon_n \tag{3.115}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) + I(W_K; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n, X_i)$$

$$- I(X_i; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) - I(W_K; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n, X_i) + \epsilon_n \tag{3.116}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) - I(X_i; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n) + \epsilon_n \tag{3.117}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{K,i}|U_{K-1,i}) - I(X_i; Z_i|U_{K-1,i}) + \epsilon_n \tag{3.118}$$

where (3.112) follows from Fano's lemma, (3.113) is obtained by using Csiszar-Korner identity, and (3.114) follows from the fact that

$$I(X_i; Y_{K,i}|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n, W_K) - I(X_i; Z_i|\tilde{W}_{K-1}, Y_K^{i-1}, Z_{i+1}^n, W_K) > 0 \tag{3.119}$$

which is due to the fact that each user's channel is less noisy with respect to the eavesdropper and (3.117) is due to the Markov chain

$$(Y_{K,i}, Z_i) \rightarrow X_i \rightarrow \left(W_0, W_1, \ldots, W_K, Y_K^{i-1}, Z_{i+1}^n\right) \tag{3.120}$$

which follows from the fact that the channel is memoryless. Finally, plugging (3.102), (3.110) and (3.118) into (3.92), we get

$$H(W_0, W_1, \ldots, W_\ell|Z^n) \leq n \sum_{k=1}^{\ell} I(U_k; Y_k|U_{k-1}) - nI(U_\ell; Z), \quad \ell = 1, \ldots, K \tag{3.121}$$

where $U_0 = \phi$ and $U_K = X$, and this concludes the converse.

3.7.2 Proof of Theorem 3.2

Achievability of these rates follows from Proposition 2 of [24]. We provide the converse. First let us define the following random variables,

$$Z^n = (Z_1^n, \ldots, Z_M^n) \tag{3.122}$$

$$Y_k^n = (Y_{k1}^n, \ldots, Y_{kM}^n) \tag{3.123}$$

$$Z_{i+1}^n = \left(Z_{1,i+1}^n, \ldots, Z_{M,i+1}^n\right) \tag{3.124}$$

$$Y_k^{i-1} = \left(Y_{k1}^{i-1} \ldots, Y_{kM}^{i-1}\right) \tag{3.125}$$

$$Y_k(i) = (Y_{k1}(i), \ldots, Y_{kM}(i)) \tag{3.126}$$

$$Z(i) = (Z_1(i), \ldots, Z_M(i)) \tag{3.127}$$

where $Y_{kl}^{i-1} = (Y_{kl}(1), \ldots, Y_{kl}(i-1))$, $Z_{l,i+1}^n = (Z_l(i+1), \ldots, Z_l(n))$. Start with the definition,

$$H(W_0|Z^n) = H(W_0) - I(W_0; Z^n) \tag{3.128}$$

$$\leq I(W_0; Y_k^n) - I(W_0; Z^n) + \epsilon_n \tag{3.129}$$

$$= \sum_{i=1}^{n} I(W_0; Y_k(i)|Y_k^{i-1}) - I(W_0; Z(i)|Z_{i+1}^n) + \epsilon_n \tag{3.130}$$

$$= \sum_{i=1}^{n} I(W_0, Z_{i+1}^n; Y_k(i)|Y_k^{i-1}) - I(Z_{i+1}^n; Y_k(i)|Y_k^{i-1}, W_0)$$

$$- I(W_0, Y_k^{i-1}; Z(i)|Z_{i+1}^n) + I(Y_k^{i-1}; Z(i)|Z_{i+1}^n, W_0) + \epsilon_n \tag{3.131}$$

$$= \sum_{i=1}^{n} I(W_0, Z_{i+1}^n; Y_k(i)|Y_k^{i-1}) - I(W_0, Y_k^{i-1}; Z(i)|Z_{i+1}^n) + \epsilon_n \tag{3.132}$$

$$= \sum_{i=1}^{n} I(W_0; Y_k(i)|Y_k^{i-1}, Z_{i+1}^n) + I(Z_{i+1}^n; Y_k(i)|Y_k^{i-1})$$

$$- I(W_0; Z(i)|Z_{i+1}^n, Y_k^{i-1}) - I(Y_k^{i-1}; Z(i)|Z_{i+1}^n) + \epsilon_n \tag{3.133}$$

$$= \sum_{i=1}^{n} I(W_0; Y_k(i)|Y_k^{i-1}, Z_{i+1}^n) - I(W_0; Z(i)|Z_{i+1}^n, Y_k^{i-1}) + \epsilon_n \tag{3.134}$$

where (3.132) and (3.134) are due the following identities

$$\sum_{i=1}^{n} I(Z_{i+1}^n; Y_k(i)|Y_k^{i-1}, W_0) = \sum_{i=1}^{n} I(Y_k^{i-1}; Z(i)|Z_{i+1}^n, W_0) \tag{3.135}$$

$$\sum_{i=1}^{n} I(Z_{i+1}^n; Y_k(i)|Y_k^{i-1}) = \sum_{i=1}^{n} I(Y_k^{i-1}; Z(i)|Z_{i+1}^n) \tag{3.136}$$

respectively, which are due to Lemma 7 of [3]. Now, we will bound each summand in (3.134) separately. First, define the following variables.

$$U_{k,i} = \left(Z_{i+1}^n, Y_k^{i-1}\right) \tag{3.137}$$

$$\tilde{Y}_k^{l-1}(i) = \left(Y_{k1}(i), \ldots, Y_{k(l-1)}(i)\right) \tag{3.138}$$

$$\tilde{Z}_{l+1}^M(i) = \left(Z_{l+1}(i), \ldots, Z_M(i)\right) \tag{3.139}$$

Hence, the summand in (3.134) can be written as follows,

$$I(W_0; Y_k(i)|Y_k^{i-1}, Z_{i+1}^n) - I(W_0; Z(i)|Z_{i+1}^n, Y_k^{i-1}) \tag{3.140}$$

$$= I(W_0; Y_k(i)|U_{k,i}) - I(W_0; Z(i)|U_{k,i}) \tag{3.141}$$

$$= I(W_0; Y_{k1}(i), \ldots, Y_{kM}(i)|U_{k,i}) - I(W_0; Z_1(i), \ldots, Z_M(i)|U_{k,i}) \tag{3.142}$$

$$= \sum_{l=1}^{M} I(W_0; Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i)) - I(W_0; Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i)) \tag{3.143}$$

$$= \sum_{l=1}^{M} I(W_0, \tilde{Z}_{l+1}^{M}(i); Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i)) - I(\tilde{Z}_{l+1}^{M}(i); Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i), W_0)$$

$$- I(W_0, \tilde{Y}_k^{l-1}(i); Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i)) + I(\tilde{Y}_k^{l-1}(i); Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i), W_0) \tag{3.144}$$

$$= \sum_{l=1}^{M} I(W_0, \tilde{Z}_{l+1}^{M}(i); Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i)) - I(W_0, \tilde{Y}_k^{l-1}(i); Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i))$$

$$\tag{3.145}$$

$$= \sum_{l=1}^{M} I(\tilde{Z}_{l+1}^{M}(i); Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i)) + I(W_0; Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^{M}(i))$$

$$- I(\tilde{Y}_k^{l-1}(i); Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i)) - I(W_0; Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i), \tilde{Y}_k^{l-1}(i)) \tag{3.146}$$

$$= \sum_{l=1}^{M} I(W_0; Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^{M}(i)) - I(W_0; Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i), \tilde{Y}_k^{l-1}(i))$$

$$\tag{3.147}$$

where (3.145) and (3.147) follow from the following identities

$$\sum_{l=1}^{M} I(\tilde{Z}_{l+1}^{M}(i); Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i), W_0) = \sum_{l=1}^{M} I(\tilde{Y}_k^{l-1}(i); Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i), W_0)$$

$$\tag{3.148}$$

$$\sum_{l=1}^{M} I(\tilde{Z}_{l+1}^{M}(i); Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i)) = \sum_{l=1}^{M} I(\tilde{Y}_k^{l-1}(i); Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^{M}(i)) \tag{3.149}$$

respectively, which are again due to Lemma 7 of [3]. Now, define the set of sub-channels, say $\mathcal{S}(k)$, in which the kth user is less noisy with respect to the eavesdropper. Thus, the summands in (3.147) for $l \notin \mathcal{S}(k)$ are negative and by dropping

them, we can bound (3.147) as follows,

$$I(W_0; Y_k(i)|Y_k^{i-1}, Z_{i+1}^n) - I(W_0; Z(i)|Z_{i+1}^n, Y_k^{i-1})$$
$$\leq \sum_{l\in\mathcal{S}(k)} I(W_0; Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^M(i)) - I(W_0; Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^M(i), \tilde{Y}_k^{l-1}(i)) \tag{3.150}$$

Moreover, for $l \in \mathcal{S}(k)$, we have

$$I(U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^M(i); Y_{kl}(i)) - I(U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^M(i); Z_l(i)) \geq 0 \tag{3.151}$$

$$I(X_l(i); Y_{kl}(i)|U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^M(i), W_0) - I(X_l(i); Z_l(i)|U_{k,i}, \tilde{Z}_{l+1}^M(i), \tilde{Y}_k^{l-1}(i), W_0) \geq 0 \tag{3.152}$$

where both are due to the fact that for $l \in \mathcal{S}(k)$, in this sub-channel the kth user is less noisy with respect to the eavesdropper. Therefore, adding (3.151) and (3.152) to each summand in (3.150), we get the following bound,

$$\begin{aligned} &I(W_0; Y_k(i)|Y_k^{i-1}, Z_{i+1}^n) - I(W_0; Z(i)|Z_{i+1}^n, Y_k^{i-1}) \\ &\quad\leq \sum_{l\in\mathcal{S}(k)} I(X_l(i), W_0, U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^M(i); Y_{kl}(i)) \\ &\quad- \quad I(X_l(i), W_0, U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^M(i); Z_l(i)) \qquad (3.153) \\ &\quad= \sum_{l\in\mathcal{S}(k)} I(X_l(i); Y_{kl}(i)) - I(X_l(i); Z_l(i)) \qquad (3.154) \end{aligned}$$

where the equality follows from the following Markov chain

$$\left(W_0, U_{k,i}, \tilde{Y}_k^{l-1}(i), \tilde{Z}_{l+1}^{M}(i)\right) \rightarrow X_l(i) \rightarrow (Y_{kl}(i), Z_l(i)) \tag{3.155}$$

which is a consequence of the facts that channel is memoryless and sub-channels are independent. Finally, using (3.154) in (3.134), we get

$$H(W_0|Z^n) \leq \sum_{i=1}^{n} \sum_{l \in \mathcal{S}(k)} I(X_l(i); Y_{kl}(i)) - I(X_l(i); Z_l(i)) + \epsilon_n \tag{3.156}$$

$$\leq n \sum_{l \in \mathcal{S}(k)} I(X_l; Y_{kl}) - I(X_l; Z_l) + \epsilon_n \tag{3.157}$$

$$= n \sum_{l=1}^{M} \left[I(X_l; Y_{kl}) - I(X_l; Z_l)\right]^+ + \epsilon_n \tag{3.158}$$

which completes the proof.

3.7.3 Proof of Theorem 3.3

Achievability of Theorem 3.3 is a consequence of the achievability result for wiretap channels in [3]. We provide the converse proof here. We first define the function $\rho(l)$ which denotes the index of the strongest user in the lth subchannel in the sense that

$$I(U; Y_{kl}) \leq I(U; Y_{\rho(l)l}) \tag{3.159}$$

for all $U \to X_l \to (Y_{1l}, \ldots, Y_{Kl}, Z_l)$ and any $k \in \{1, \ldots, K\}$. Moreover, we define the following shorthand notations

$$\tilde{Y}_l^n = Y_{\rho(l)l}^n, \qquad l = 1, \ldots, M \tag{3.160}$$

$$\tilde{Y}^n = (\tilde{Y}_1^n, \ldots, \tilde{Y}_M^n) \tag{3.161}$$

$$Y_k^n = (Y_{k1}^n, \ldots, Y_{kM}^n), \qquad k = 1, \ldots, K \tag{3.162}$$

$$Z^n = (Z_1^n, \ldots, Z_M^n) \tag{3.163}$$

$$Y_k^{i-1} = (Y_{k1}^{i-1}, \ldots, Y_{kM}^{i-1}), \qquad k = 1, \ldots, K \tag{3.164}$$

$$Z^{i-1} = (Z_1^{i-1}, \ldots, Z_M^{i-1}) \tag{3.165}$$

$$\tilde{Y}_{i+1}^n = (\tilde{Y}_{1,i+1}^n, \ldots, \tilde{Y}_{M,i+1}^n) \tag{3.166}$$

$$Y_k^{l-1}(i) = (Y_{k1}(i), \ldots, Y_{k,l-1}(i)), \qquad l = 1, \ldots, M \tag{3.167}$$

$$Z^{l-1}(i) = (Z_1(i), \ldots, Z_{l-1}(i)), \qquad l = 1, \ldots, M \tag{3.168}$$

$$\tilde{Y}_{l+1}^M(i) = (\tilde{Y}_{l+1}(i), \ldots, \tilde{Y}_M(i)), \qquad l = 1, \ldots, M \tag{3.169}$$

We first introduce the following lemma.

Lemma 3.2 *For the parallel multi-receiver wiretap channel with less noisiness order, we have*

$$I(W_k; Y_k^n) \leq I(W_k; \tilde{Y}^n), \quad k = 1, \ldots, K \tag{3.170}$$

Proof: Consecutive uses of Csiszar-Korner identity [3], as in Appendix 3.7.2, yield

$$I(W_k;Y_k^n) - I(W_k;\tilde{Y}^n) = \sum_{i=1}^{n}\sum_{l=1}^{M}\Big[I(W_k;Y_{kl}(i)|Y_k^{i-1},\tilde{Y}_{i+1}^n,Y_k^{l-1}(i),\tilde{Y}_{l+1}^M(i)) - I(W_k;\tilde{Y}_l(i)|Y_k^{i-1},\tilde{Y}_{i+1}^n,Y_k^{l-1}(i),\tilde{Y}_{l+1}^M(i))\Big] \quad (3.171)$$

where each of the summand is negative, i.e., we have

$$I(W_k;Y_{kl}(i)|Y_k^{i-1},\tilde{Y}_{i+1}^n,Y_k^{l-1}(i),\tilde{Y}_{l+1}^M(i)) - I(W_k;\tilde{Y}_l(i)|Y_k^{i-1},\tilde{Y}_{i+1}^n,Y_k^{l-1}(i),\tilde{Y}_{l+1}^M(i)) \leq 0 \quad (3.172)$$

because $\tilde{Y}_l(i)$ is the observation of the strongest user in the lth sub-channel, i.e., its channel is less noisy with respect to all other users in the lth sub-channel. This concludes the proof of the lemma. □

This lemma implies that

$$H(W_k|\tilde{Y}^n) \leq H(W_k|Y_k^n) \leq \epsilon_n \quad (3.173)$$

where the second inequality is due to Fano's lemma. Using (3.173), we get

$$H(W_1,\ldots,W_K|\tilde{Y}^n) \leq \sum_{k=1}^{K} H(W_k|\tilde{Y}^n) \leq K\epsilon_n \quad (3.174)$$

where the first inequality follows from the fact that conditioning cannot increase entropy.

We now start the converse proof.

$$H(W_1,\ldots,W_K|Z^n) \leq I(W_1,\ldots,W_K;\tilde{Y}^n) - I(W_1,\ldots,W_K;Z^n) + K\epsilon_n \quad (3.175)$$

$$= \sum_{i=1}^{n}\sum_{l=1}^{M}\Big[I(W_1,\ldots,W_K;\tilde{Y}_l(i)|Z^{i-1},\tilde{Y}_{i+1}^n,Z^{l-1}(i),\tilde{Y}_{l+1}^M(i)) - I(W_1,\ldots,W_K;Z_l(i)|Z^{i-1},\tilde{Y}_{i+1}^n,Z^{l-1}(i),\tilde{Y}_{l+1}^M(i))\Big] + K\epsilon_n \quad (3.176)$$

where (3.175) is a consequence of (3.174) and (3.176) is obtained via consecutive uses of the Csiszar-Korner identity [3] as we did in Appendix 3.7.2. We define the set of indices $\mathcal{S}$ such that for all $l \in \mathcal{S}$, the strongest user in the lth sub-channel has a less noisy channel with respect to the eavesdropper, i.e., we have

$$I(U;\tilde{Y}_l(i)) \geq I(U;Z_l(i)) \quad (3.177)$$

for all $U \to X_l(i) \to (\tilde{Y}_l(i), Z_l(i))$ and any $l \in \mathcal{S}$. Thus, we can further bound (3.176) as follows,

$$H(W_1,\ldots,W_K|Z^n)$$

$$\leq \sum_{i=1}^{n}\sum_{l\in\mathcal{S}}\Big[I(W_1,\ldots,W_K;\tilde{Y}_l(i)|Z^{i-1},\tilde{Y}_{i+1}^n,Z^{l-1}(i),\tilde{Y}_{l+1}^M(i)) - I(W_1,\ldots,W_K;Z_l(i)|Z^{i-1},\tilde{Y}_{i+1}^n,Z^{l-1}(i),\tilde{Y}_{l+1}^M(i))\Big] + K\epsilon_n \quad (3.178)$$

$$\leq \sum_{i=1}^{n}\sum_{l\in\mathcal{S}}\Big[I(W_1,\ldots,W_K,Z^{i-1},\tilde{Y}_{i+1}^n,Z^{l-1}(i),\tilde{Y}_{l+1}^M(i);\tilde{Y}_l(i)) - I(W_1,\ldots,W_K,Z^{i-1},\tilde{Y}_{i+1}^n,Z^{l-1}(i),\tilde{Y}_{l+1}^M(i);Z_l(i))\Big] + K\epsilon_n \quad (3.179)$$

$$\leq \sum_{i=1}^{n} \sum_{l \in \mathcal{S}} \Big[I(X_l(i), W_1, \ldots, W_K, Z^{i-1}, \tilde{Y}_{i+1}^n, Z^{l-1}(i), \tilde{Y}_{l+1}^M(i); \tilde{Y}_l(i))$$

$$- I(X_l(i), W_1, \ldots, W_K, Z^{i-1}, \tilde{Y}_{i+1}^n, Z^{l-1}(i), \tilde{Y}_{l+1}^M(i); Z_l(i)) \Big] + K\epsilon_n \tag{3.180}$$

$$= \sum_{i=1}^{n} \sum_{l \in \mathcal{S}} \Big[I(X_l(i); \tilde{Y}_l(i)) - I(X_l(i); Z_l(i)) \Big] + K\epsilon_n \tag{3.181}$$

where (3.178) is obtained by dropping the negative terms, (3.179)-(3.180) are due to the following inequalities

$$I(Z^{i-1}, \tilde{Y}_{i+1}^n, Z^{l-1}(i), \tilde{Y}_{l+1}^M(i); \tilde{Y}_l(i)) \geq I(Z^{i-1}, \tilde{Y}_{i+1}^n, Z^{l-1}(i), \tilde{Y}_{l+1}^M(i); Z_l(i)) \tag{3.182}$$

$$I(X_l(i); \tilde{Y}_l(i) | W_1, \ldots, W_K, Z^{i-1}, \tilde{Y}_{i+1}^n, Z^{l-1}(i), \tilde{Y}_{l+1}^M(i)) \geq$$

$$I(X_l(i); Z_l(i) | W_1, \ldots, W_K, Z^{i-1}, \tilde{Y}_{i+1}^n, Z^{l-1}(i), \tilde{Y}_{l+1}^M(i)) \tag{3.183}$$

which come from the fact that for any $l \in \mathcal{S}$, the strongest user in the lth sub-channel has a less noisy channel with respect to the eavesdropper. Finally, we get (3.181) using the following Markov chain

$$(W_1, \ldots, W_K, Z^{i-1}, \tilde{Y}_{i+1}^n, Z^{l-1}(i), \tilde{Y}_{l+1}^M(i)) \rightarrow X_l(i) \rightarrow (\tilde{Y}_l, Z_l(i)) \tag{3.184}$$

which is a consequence of the facts that channel is memoryless, and the sub-channels are independent.

3.7.4 Proof of Theorem 3.4

We prove Theorem 3.4 in two parts, first achievability and then converse. Throughout the proof, we use the shorthand notations $Y_1^n = (Y_{11}^n, Y_{12}^n)$, $Y_2^n = (Y_{21}^n, Y_{22}^n)$, $Z_1^n = (Z_1^n, Z_2^n)$.

3.7.4.1 Achievability

To show the achievability of the region given by (3.30)-(3.35), first we need to note that the boundary of this region can be decomposed into three surfaces as follows [29].

- First surface:

$$R_0 \leq I(U_2; Y_{12}|Z_2) \tag{3.185}$$

$$R_2 \leq I(X_2; Y_{22}|U_2, Z_2) \tag{3.186}$$

$$R_0 + R_1 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2), \quad U_1 = \phi \tag{3.187}$$

- Second surface:

$$R_0 \leq I(U_1; Y_{21}|Z_1) \tag{3.188}$$

$$R_1 \leq I(X_1; Y_{11}|U_1, Z_1) \tag{3.189}$$

$$R_0 + R_2 \leq I(X_2; Y_{22}|Z_2) + I(U_1; Y_{21}|Z_1), \quad U_2 = \phi \tag{3.190}$$

- Third surface:

$$R_0 \leq I(U_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) \tag{3.191}$$

$$R_0 \leq I(U_1; Y_{21}|Z_1) + I(U_2; Y_{22}|Z_2) \tag{3.192}$$

$$R_1 \leq I(X_1; Y_{11}|U_1, Z_1) \tag{3.193}$$

$$R_2 \leq I(X_2; Y_{22}|U_2, Z_2) \tag{3.194}$$

We now show the achievability of these regions separately. Start with the first region.

Proposition 3.1 *The region defined by (3.185)-(3.187) is achievable.*

Proof: Fix the probability distribution

$$p(x_1)p(u_2)p(x_2|u_2)p(y_1, y_2, z|x) \tag{3.195}$$

Codebook generation:

- Split the private message rate of user 1 as $R_1 = R_{11} + R_{12}$.
- Generate $2^{n(R_{11}+\tilde{R}_{11})}$ length-n sequences $\mathbf{x}_1$ through $p(\mathbf{x}_1) = \prod_{i=1}^{n} p(x_{1,i})$ and index them as $\mathbf{x}_1(w_{11}, \tilde{w}_{11})$ where $w_{11} \in \left\{1, \ldots, 2^{nR_{11}}\right\}$ and $\tilde{w}_{11} \in \left\{1, \ldots, 2^{n\tilde{R}_{11}}\right\}$.
- Generate $2^{n(R_0+R_{12}+\tilde{R}_{12})}$ length-n sequences $\mathbf{u}_2$ through $p(\mathbf{u}_2) = \prod_{i=1}^{n} p(u_{2,i})$ and index them as $\mathbf{u}_2(w_0, w_{12}, \tilde{w}_{12})$ where $w_0 \in \left\{1, \ldots, 2^{nR_0}\right\}$, $w_{12} \in \left\{1, \ldots, 2^{nR_{12}}\right\}$ and $\tilde{w}_{12} \in \left\{1, \ldots, 2^{n\tilde{R}_{12}}\right\}$.

- For each $\mathbf{u}_2$, generate $2^{n(R_2+\tilde{R}_2)}$ length-n sequences $\mathbf{x}_2$ through $p(\mathbf{x}_2|\mathbf{u}_2) = \prod_{i=1}^{n} p(x_{2,i}|u_{2,i})$ and index them as $\mathbf{x}_2(w_2, \tilde{w}_2, w_0, w_{12}, \tilde{w}_{12})$ where $w_2 \in \left\{1, \ldots, 2^{nR_2}\right\}$, $\tilde{w}_2 \in \left\{1, \ldots, 2^{n\tilde{R}_2}\right\}$.

- Furthermore, set the confusion message rates as follows.

$$\tilde{R}_{11} = I(X_1; Z_1) \tag{3.196}$$

$$\tilde{R}_{12} = I(U_2; Z_2) \tag{3.197}$$

$$\tilde{R}_2 = I(X_2; Z_2|U_2) \tag{3.198}$$

Encoding:

If $(w_0, w_{11}, w_{12}, w_2)$ is the message to be transmitted, then the receiver randomly picks $(\tilde{w}_{11}, \tilde{w}_{12}, \tilde{w}_2)$ and sends the corresponding codewords through each channel.

Decoding:

It is straightforward to see that if the following conditions are satisfied, then both users can decode the messages directed to themselves with vanishingly small

error probability.

$$R_0 + \tilde{R}_{12} + R_{12} \leq I(U_2; Y_{12}) \tag{3.199}$$

$$R_{11} + \tilde{R}_{11} \leq I(X_1; Y_{11}) \tag{3.200}$$

$$R_2 + \tilde{R}_2 \leq I(X_2; Y_{22}|U_2) \tag{3.201}$$

After eliminating R_{11} and R_{12} and plugging the values of $\tilde{R}_{11}, \tilde{R}_{12}, \tilde{R}_2$, we can reach the following conditions,

$$R_0 \leq I(U_2; Y_{12}|Z_2) \tag{3.202}$$

$$R_2 \leq I(X_2; Y_{22}|U_2, Z_2) \tag{3.203}$$

$$R_0 + R_1 \leq I(X_1; Y_{11}|Z_1) + I(U_2; Y_{12}|Z_2) \tag{3.204}$$

where we used the degradedness of the channel. Thus, we only need to show that this coding scheme satisfies the secrecy constraints.

Equivocation computation:

As shown previously in Lemma 3.1 of Appendix 3.7.1, checking the sum rate secrecy condition is sufficient.

$$\begin{aligned} H(W_0, W_1, W_2|Z^n) &= H(W_0, W_1, W_2, Z^n) - H(Z^n) \\ &= H(W_0, W_1, W_2, U_2^n, X_2^n, X_1^n, Z^n) - H(U_2^n, X_2^n, X_1^n|W_0, W_1, W_2, Z^n) - H(Z^n) \end{aligned} \tag{3.205}$$

$$= H(U_2^n, X_2^n, X_1^n) + H(W_0, W_1, W_2, Z^n | U_2^n, X_2^n, X_1^n) - H(Z^n)$$

$$- H(U_2^n, X_2^n, X_1^n | W_0, W_1, W_2, Z^n) \tag{3.206}$$

$$\geq H(U_2^n, X_2^n, X_1^n) + H(Z^n | U_2^n, X_2^n, X_1^n) - H(Z^n) - H(U_2^n, X_2^n, X_1^n | W_0, W_1, W_2, Z^n) \tag{3.207}$$

We treat each term in (3.207) separately. The first term in (3.207) is

$$H(U_2^n, X_2^n, X_1^n) = H(U_2^n, X_2^n) + H(X_1^n) \tag{3.208}$$

$$= n(R_0 + R_{11} + R_2 + R_{12} + \tilde{R}_{11} + \tilde{R}_{12} + \tilde{R}_2) \tag{3.209}$$

where the first equality is due to the independence of (U_2^n, X_2^n) and X_1^n, and the second equality is due the fact that both messages and confusion codewords are uniformly distributed. The second and the third terms in (3.207) are

$$H(Z^n) - H(Z^n | U_2^n, X_2^n, X_1^n) = H(Z_1^n, Z_2^n) - H(Z^n | U_2^n, X_2^n, X_1^n) \tag{3.210}$$

$$\leq H(Z_1^n) + H(Z_2^n) - H(Z_1^n, Z_2^n | U_2^n, X_2^n, X_1^n) \tag{3.211}$$

$$= H(Z_1^n) + H(Z_2^n) - H(Z_1^n, Z_2^n | X_2^n, X_1^n) \tag{3.212}$$

$$= H(Z_1^n) + H(Z_2^n) - H(Z_1^n | X_1^n) - H(Z_2^n | X_2^n) \tag{3.213}$$

$$= I(X_1^n; Z_1^n) + I(X_2^n; Z_2^n) \tag{3.214}$$

$$\leq nI(X_1; Z_1) + nI(X_2; Z_2) + \gamma_{1,n} + \gamma_{2,n} \tag{3.215}$$

where the equalities in (3.212) and (3.213) are due to the following Markov chains

$$U_2^n \to X_2^n \to (X_1^n, Z_1^n, Z_2^n) \tag{3.216}$$

$$Z_2^n \to X_2^n \to X_1^n \to Z_1^n \tag{3.217}$$

respectively, and the last inequality in (3.215) can be shown using the technique devised in [2]. To bound the last term in (3.207), assume that the eavesdropper tries to decode (U_2^n, X_2^n, X_1^n) using the side information W_0, W_1, W_2 and its observation. Since the rates of the confusion codewords are selected such that the eavesdropper can decode them given $W_0 = w_0, W_1 = w_1, W_2 = w_2$ (see (3.196)-(3.198)), using Fano's lemma, we get

$$H(U_2^n, X_2^n, X_1^n | W_0, W_1, W_2, Z^n) \leq \epsilon_n \tag{3.218}$$

for the third term in (3.207). Plugging (3.209), (3.215) and (3.218) into (3.207), we get

$$H(W_0, W_1, W_2 | Z^n) \geq n(R_0 + R_1 + R_2) - \epsilon_n - \gamma_{1,n} - \gamma_{2,n} \tag{3.219}$$

which completes the proof. □

Achievability of the region defined by (3.188)-(3.190) follows due to symmetry. We now show the achievability of the region defined by (3.191)-(3.194).

Proposition 3.2 *The region described by (3.191)-(3.194) is achievable.*

Proof: Fix the probability distribution as follows,

$$p(u_1)p(x_1|u_1)p(u_2)p(x_2|u_2)p(y_1, y_2, z|x) \tag{3.220}$$

Codebook generation:

- Generate $2^{n(R_0+\tilde{R}_{01})}$ length-n sequences $\mathbf{u}_1$ through $p(\mathbf{u}_1) = \prod_{i=1}^{n} p(u_{1,i})$ and index them as $\mathbf{u}_1(w_0, \tilde{w}_{01})$ where $w_0 \in \left\{1, \ldots, 2^{nR_0}\right\}$, $\tilde{w}_{01} \in \left\{1, \ldots, 2^{n\tilde{R}_{01}}\right\}$.

- For each $\mathbf{u}_1$, generate $2^{n(R_1+\tilde{R}_1)}$ $\mathbf{x}_1(w_0, \tilde{w}_{01}, w_1, \tilde{w}_1)$ length-n sequences $\mathbf{x}_1$ through $p(\mathbf{x}_1) = \prod_{i=1}^{n} p(x_{1,i}|u_{1,i})$ where $w_1 \in \left\{1, \ldots, 2^{nR_1}\right\}$, $\tilde{w}_1 \in \left\{1, \ldots, 2^{n\tilde{R}_1}\right\}$.

- Generate $2^{n(R_0+\tilde{R}_{02})}$ length-n sequences $\mathbf{u}_2$ through $p(\mathbf{u}_2) = \prod_{i=1}^{n} p(u_{2,i})$ and index them as $\mathbf{u}_2(w_0, \tilde{w}_{02})$ where $w_0 \in \left\{1, \ldots, 2^{nR_0}\right\}$, $\tilde{w}_{02} \in \left\{1, \ldots, 2^{n\tilde{R}_{02}}\right\}$.

- For each $\mathbf{u}_2$, generate $2^{n(R_2+\tilde{R}_2)}$ $\mathbf{x}_2(w_0, \tilde{w}_{02}, w_2, \tilde{w}_2)$ length-n sequences $\mathbf{x}_2$ through $p(\mathbf{x}_2) = \prod_{i=1}^{n} p(x_{2,i}|u_{2,i})$ where $w_2 \in \left\{1, \ldots, 2^{nR_2}\right\}$, $\tilde{w}_2 \in \left\{1, \ldots, 2^{n\tilde{R}_2}\right\}$.

- Moreover, set the rates of confusion messages as follows,

$$\tilde{R}_{01} = I(U_1; Z_1) \tag{3.221}$$

$$\tilde{R}_{02} = I(U_2; Z_2) \tag{3.222}$$

$$\tilde{R}_1 = I(X_1; Z_1|U_1) \tag{3.223}$$

$$\tilde{R}_2 = I(X_2; Z_2|U_2) \tag{3.224}$$

Encoding:

Assume that the messages to be transmitted are (w_0, w_1, w_2). Then, after randomly picking the tuple $(\tilde{w}_{01}, \tilde{w}_{02}, \tilde{w}_1, \tilde{w}_2)$, corresponding codewords are sent.

Decoding:

Users decode w_0 using their both observations. If w_0 is the only message that satisfies

$$E_{i1}^{w_0} = \{\exists \tilde{w}_{01} : (\mathbf{u}_1(w_0, \tilde{w}_{01}), \mathbf{y}_{i1}) \in A_\epsilon^n\} \tag{3.225}$$

$$E_{i2}^{w_0} = \{\exists \tilde{w}_{02} : (\mathbf{u}_2(w_0, \tilde{w}_{02}), \mathbf{y}_{i2}) \in A_\epsilon^n\} \tag{3.226}$$

simultaneously for user i, w_0 is declared to be transmitted. Assume $w_0 = 1$ is transmitted. The error probability for user i can be bounded as

$$\Pr(E_i) \leq \Pr\left(\left(E_{i1}^1, E_{i2}^1\right)^c\right) + \sum_{j=2}^{2^{nR_0}} \Pr\left(E_{i1}^j, E_{i2}^j\right) \tag{3.227}$$

using the union bound. Let us consider the following

$$\Pr\left(E_{i1}^j\right) = \Pr\left(\exists \tilde{w}_{01} : (\mathbf{u}_1(j, \tilde{w}_{01}), \mathbf{y}_{i1}) \in A_\epsilon^n\right) \tag{3.228}$$

$$\leq \sum_{\forall \tilde{w}_{01}} \Pr\left((\mathbf{u}_1(j, \tilde{w}_{01}), \mathbf{y}_{i1}) \in A_\epsilon^n\right) \tag{3.229}$$

$$\leq 2^{n\tilde{R}_{01}} 2^{-n(I(U_1;Y_{i1})-\epsilon_n)} \tag{3.230}$$

$$= 2^{n(\tilde{R}_{01}-I(U_1;Y_{i1})+\epsilon_n)} \tag{3.231}$$

Similarly, we have

$$\Pr\left(E_{i2}^{j}\right) \leq 2^{n(\tilde{R}_{02}-I(U_2;Y_{i2})+\epsilon_n)} \tag{3.232}$$

Thus, the probability of declaring that the jth message was transmitted can be bounded as

$$\Pr\left(E_{i1}^{j}, E_{i2}^{j}\right) = \Pr\left(E_{i1}^{j}\right) \times \Pr\left(E_{i2}^{j}\right) \tag{3.233}$$

$$\leq 2^{n(\tilde{R}_{01}-I(U_1;Y_{i1})+\epsilon_n)} \times 2^{n(\tilde{R}_{02}-I(U_2;Y_{i2})+\epsilon_n)} \tag{3.234}$$

$$= 2^{n(\tilde{R}_{01}-I(U_1;Y_{i1})+\tilde{R}_{02}-I(U_2;Y_{i2})+2\epsilon_n)} \tag{3.235}$$

where the first equality is due to the independence of sub-channels and codebooks used for each channel. Therefore, error probability can be bounded as

$$\Pr\left(E_i\right) \leq \epsilon_n + \sum_{j=2}^{2^{nR_0}} 2^{n(\tilde{R}_{01}-I(U_1;Y_{i1})+\tilde{R}_{02}-I(U_2;Y_{i2})+2\epsilon_n)} \tag{3.236}$$

$$= \epsilon_n + 2^{n(R_0+\tilde{R}_{01}-I(U_1;Y_{i1})+\tilde{R}_{02}-I(U_2;Y_{i2})+2\epsilon_n)} \tag{3.237}$$

which vanishes if the following are satisfied,

$$R_0 + \tilde{R}_{01} + \tilde{R}_{02} \leq I(U_1;Y_{i1}) + I(U_2;Y_{i2}), \quad i = 1,2 \tag{3.238}$$

After decoding the common message, both users decode their private messages if the rates satisfy

$$R_1 + \tilde{R}_1 \leq I(X_1; Y_{11}|U_1) \tag{3.239}$$

$$R_2 + \tilde{R}_2 \leq I(X_2; Y_{22}|U_2) \tag{3.240}$$

After plugging the values of $\tilde{R}_{01}, \tilde{R}_{02}, \tilde{R}_1, \tilde{R}_2$ given by (3.221)-(3.224) into (3.238)-(3.240), one can recover the region described by (3.191)-(3.194) using the degradedness of the channel.

Equivocation calculation:

It is sufficient to check the sum rate constraint,

$$H(W_0, W_1, W_2|Z^n) = H(W_0, W_1, W_2, Z^n) - H(Z^n) \tag{3.241}$$

$$= H(U_1^n, U_2^n, X_1^n, X_2^n, W_0, W_1, W_2, Z^n) - H(U_1^n, U_2^n, X_1^n, X_2^n|W_0, W_1, W_2, Z^n)$$
$$- H(Z^n) \tag{3.242}$$

$$= H(U_1^n, U_2^n, X_1^n, X_2^n) + H(W_0, W_1, W_2, Z^n|U_1^n, U_2^n, X_1^n, X_2^n) - H(Z^n)$$
$$- H(U_1^n, U_2^n, X_1^n, X_2^n|W_0, W_1, W_2, Z^n) \tag{3.243}$$

$$\geq H(U_1^n, U_2^n, X_1^n, X_2^n) + H(Z^n|U_1^n, U_2^n, X_1^n, X_2^n) - H(Z^n)$$
$$- H(U_1^n, U_2^n, X_1^n, X_2^n|W_0, W_1, W_2, Z^n) \tag{3.244}$$

where each term will be treated separately. The first term is

$$H(U_1^n, U_2^n, X_1^n, X_2^n) = H(U_1^n, U_2^n) + H(X_1^n|U_1^n, U_2^n) + H(X_1^n|U_1^n, U_2^n) \quad (3.245)$$

$$= n(R_0 + R_1 + R_2 + \tilde{R}_{01} + \tilde{R}_{02} + \tilde{R}_1 + \tilde{R}_2) \quad (3.246)$$

where we first use the fact that X_1^n and X_2^n are independent given (U_1^n, U_2^n) and secondly, we use the fact that messages are uniformly distributed. The second and third term of (3.244) are

$$H(Z^n) - H(Z^n|U_1^n, U_2^n, X_1^n, X_2^n) = H(Z_1^n, Z_2^n) - H(Z_1^n|X_1^n) - H(Z_1^n|X_2^n) \quad (3.247)$$

$$\leq H(Z_1^n) + H(Z_2^n) - H(Z_1^n|X_1^n) - H(Z_1^n|X_2^n) \quad (3.248)$$

$$= I(X_1^n; Z_1^n) + I(X_2^n; Z_2^n) \quad (3.249)$$

$$\leq nI(X_1; Z_1) + nI(X_2; Z_2) + \gamma_{1,n} + \gamma_{2,n} \quad (3.250)$$

where the first equality is due to the independence of the sub-channels. We now consider the last term of (3.244) for which assume that eavesdropper tries to decode $(U_1^n, U_2^n, X_1^n, X_2^n)$ using the side information (W_0, W_1, W_2) and its observation. Since the rates of the confusion messages are selected to ensure that the eavesdropper can decode $(U_1^n, U_2^n, X_1^n, X_2^n)$ given $(W_0 = w_0, W_1 = w_1, W_2 = w_2)$ (see (3.221)-(3.224)), using Fano's lemma we have

$$H(U_1^n, U_2^n, X_1^n, X_2^n|W_0, W_1, W_2, Z^n) \leq \epsilon_n \quad (3.251)$$

Plugging (3.246), (3.250) and (3.251) into (3.244), we have

$$H(W_0, W_1, W_2|Z^n) \geq n(R_0 + R_1 + R_2) - \epsilon_n - \gamma_{1,n} - \gamma_{2,n} \tag{3.252}$$

which concludes the proof. □

3.7.4.2 Converse

First let us define the following auxiliary random variables,

$$U_{1,i} = W_0 W_2 Y_{12}^n Y_{11}^{i-1} Z_{1,i+1}^n \tag{3.253}$$

$$U_{2,i} = W_0 W_1 Y_{21}^n Y_{22}^{i-1} Z_{2,i+1}^n \tag{3.254}$$

which satisfy the following Markov chains

$$U_{1,i} \to X_{1,i} \to (Y_{11,i}, Y_{21,i}, Z_{1,i}) \tag{3.255}$$

$$U_{2,i} \to X_{2,i} \to (Y_{12,i}, Y_{22,i}, Z_{2,i}) \tag{3.256}$$

We remark that although $U_{1,i}$ and $U_{2,i}$ are correlated, at the end of the proof, it will turn out that selection of them as independent will yield the same region. We start with the common message rate,

$$H(W_0|Z^n) = H(W_0) - I(W_0; Z^n) \tag{3.257}$$

$$\leq I(W_0; Y_1^n) - I(W_0; Z^n) + \epsilon_n \tag{3.258}$$

$$= I(W_0; Y_1^n | Z^n) + \epsilon_n \tag{3.259}$$

$$= I(W_0; Y_{12}^n | Z^n) + I(W_0; Y_{11}^n | Y_{12}^n, Z^n) + \epsilon_n \tag{3.260}$$

$$\leq I(W_0, W_1; Y_{12}^n | Z^n) + I(W_0, W_2; Y_{11}^n | Y_{12}^n, Z^n) + \epsilon_n \tag{3.261}$$

where (3.258) is due to Fano's lemma, equality in (3.259) is due to the fact that the eavesdropper's channel is degraded with respect to the first user's channel. We bound each term in (3.261) separately. First term is

$$I(W_0, W_1; Y_{12}^n | Z^n) = \sum_{i=1}^{n} I(W_0, W_1; Y_{12,i} | Y_{12}^{i-1}, Z_1^n, Z_2^n) \tag{3.262}$$

$$= \sum_{i=1}^{n} H(Y_{12,i} | Y_{12}^{i-1}, Z_1^n, Z_2^n) - H(Y_{12,i} | Y_{12}^{i-1}, Z_1^n, Z_2^n, W_0, W_1) \tag{3.263}$$

$$\leq \sum_{i=1}^{n} H(Y_{12,i} | Z_{2,i}) - H(Y_{12,i} | Y_{12}^{i-1}, Z_1^n, Z_2^n, W_0, W_1, Y_{21}^n, Y_{22}^{i-1}) \tag{3.264}$$

$$= \sum_{i=1}^{n} H(Y_{12,i} | Z_{2,i}) - H(Y_{12,i} | W_0, W_1, Y_{21}^n, Y_{22}^{i-1}, Z_{2,i+1}^n, Z_{2,i}) \tag{3.265}$$

$$= \sum_{i=1}^{n} I(U_{2,i}; Y_{12,i} | Z_{2,i}) \tag{3.266}$$

where (3.264) follows from the fact that conditioning cannot increase entropy and the equality in (3.265) is due to the following Markov chains

$$Z_1^n \to Y_{21}^n \to (W_0, W_1, Y_{22}^n, Z_2^n, Y_{12}^n) \tag{3.267}$$

$$Y_{12}^{i-1} Z_2^{i-1} \to Y_{22}^{i-1} \to \left(W_0, W_1, Y_{21}^n, Y_{12,i}, Z_{2,i}^n, Z_1^n\right) \tag{3.268}$$

both of which are due to the fact that sub-channels are independent, memoryless and degraded. We now consider the second term in (3.261),

$$I(W_0, W_2; Y_{11}^n | Y_{12}^n, Z^n) = \sum_{i=1}^{n} I(W_0, W_2; Y_{11,i} | Y_{12}^n, Z_1^n, Z_2^n, Y_{11}^{i-1}) \tag{3.269}$$

$$= \sum_{i=1}^{n} I(W_0, W_2; Y_{11,i} | Y_{12}^n, Y_{11}^{i-1}, Z_{1,i+1}^n, Z_{1,i}) \tag{3.270}$$

$$\leq \sum_{i=1}^{n} I(W_0, W_2, Y_{12}^n, Y_{11}^{i-1}, Z_{1,i+1}^n; Y_{11,i} | Z_{1,i}) \tag{3.271}$$

$$= \sum_{i=1}^{n} I(U_{1,i}; Y_{11,i} | Z_{1,i}) \tag{3.272}$$

where (3.270) follows from the following Markov chains

$$Z_2^n \to Y_{12}^n \to \left(W_0, W_2, Y_{11}^{i-1}, Z_1^n, Y_{11,i}\right) \tag{3.273}$$

$$Z_1^{i-1} \to Y_{11}^{i-1} \to (W_0, W_2, Y_{12}^n, Z_{1,i+1}^n, Z_{1,i}, Y_{11,i}) \tag{3.274}$$

both of which are due to the fact that sub-channels are independent, memoryless and degraded. Plugging (3.266) and (3.272) into (3.261), we get the following outer bound on the common rate.

$$H(W_0|Z^n) \leq \sum_{i=1}^{n} I(U_{2,i}; Y_{12,i} | Z_{2,i}) + \sum_{i=1}^{n} I(U_{1,i}; Y_{11,i} | Z_{1,i}) + \epsilon_n \tag{3.275}$$

Using the same analysis on the second user, we can obtain the following outer bound on the common rate as well.

$$H(W_0|Z^n) \leq \sum_{i=1}^{n} I(U_{2,i}; Y_{22,i}|Z_{2,i}) + \sum_{i=1}^{n} I(U_{1,i}; Y_{21,i}|Z_{1,i}) + \epsilon_n \tag{3.276}$$

We now bound the sum of independent and common message rates for each user,

$$\begin{aligned} H(W_0, W_1|Z^n) &\leq I(W_0, W_1; Y_1^n) - I(W_0, W_1; Z^n) + \epsilon_n && (3.277)\\ &= I(W_0, W_1; Y_1^n|Z^n) + \epsilon_n && (3.278)\\ &= I(W_0, W_1; Y_{11}^n, Y_{12}^n|Z^n) + \epsilon_n && (3.279)\\ &= I(W_0, W_1; Y_{12}^n|Z^n) + I(W_0, W_1; Y_{11}^n|Y_{12}^n, Z^n) + \epsilon_n && (3.280) \end{aligned}$$

where (3.277) is due to Fano's lemma, (3.278) is due to the fact that the eavesdropper's channel is degraded with respect to the first user's channel. Using (3.266), the first term in (3.280) can be bounded as

$$I(W_0, W_1; Y_{12}^n|Z^n) \leq \sum_{i=1}^{n} I(U_{2,i}; Y_{12,i}|Z_{2,i}) \tag{3.281}$$

Thus, we only need to bound the second term of (3.280),

$$\begin{aligned} I(W_0, W_1; Y_{11}^n|Y_{12}^n, Z^n) &= H(Y_{11}^n|Y_{12}^n, Z_1^n, Z_2^n) - H(Y_{11}^n|Y_{12}^n, Z_1^n, Z_2^n, W_0, W_1) && (3.282)\\ &\leq H(Y_{11}^n|Z_1^n) - H(Y_{11}^n|Y_{12}^n, Z_1^n, Z_2^n, W_0, W_1, X_1^n) && (3.283)\\ &= H(Y_{11}^n|Z_1^n) - H(Y_{11}^n|Z_1^n, X_1^n) && (3.284) \end{aligned}$$

$$= I(X_1^n; Y_{11}^n | Z_1^n) \tag{3.285}$$

$$\leq \sum_{i=1}^{n} H(Y_{11,i}|Z_{1,i}) - H(Y_{11,i}|Z_1^n, X_1^n, Y_{11}^{i-1}) \tag{3.286}$$

$$= \sum_{i=1}^{n} H(Y_{11,i}|Z_{1,i}) - H(Y_{11,i}|Z_{1,i}, X_{1,i}) \tag{3.287}$$

$$= \sum_{i=1}^{n} I(X_{1,i}; Y_{11,i}|Z_{1,i}) \tag{3.288}$$

where (3.283) is due to the fact that conditioning cannot increase entropy, (3.284) is due to the following Markov chain

$$(Y_{11}^n, Z_1^n) \rightarrow X_1^n \rightarrow (Y_{12}^n, Z_2^n, W_0, W_1) \tag{3.289}$$

and (3.286) follows from the fact that conditioning cannot increase entropy. Finally, (3.287) is due to the fact that each sub-channel is memoryless. Hence, plugging (3.281) and (3.288) into (3.280), we get the following outer bound.

$$H(W_0, W_1|Z^n) \leq \sum_{i=1}^{n} I(X_{1,i}; Y_{11,i}|Z_{1,i}) + \sum_{i=1}^{n} I(U_{2,i}; Y_{12,i}|Z_{2,i}) + \epsilon_n \tag{3.290}$$

Similarly, for the second user, we can get the following outer bound,

$$H(W_0, W_2|Z^n) \leq \sum_{i=1}^{n} I(X_{2,i}; Y_{22,i}|Z_{2,i}) + \sum_{i=1}^{n} I(U_{1,i}; Y_{21,i}|Z_{1,i}) + \epsilon_n \tag{3.291}$$

We now bound the sum rates to conclude the converse,

$$H(W_0, W_1, W_2|Z^n) = H(W_0, W_1, W_2) - I(W_0, W_1, W_2; Z^n) \tag{3.292}$$

$$\leq I(W_0, W_1; Y_1^n) + I(W_2; Y_2^n|W_0, W_1) - I(W_0, W_1, W_2; Z^n) + \epsilon_n \tag{3.293}$$

$$= I(W_0, W_1; Y_1^n|Z^n) + I(W_2; Y_2^n|W_0, W_1, Z^n) + \epsilon_n \tag{3.294}$$

$$= I(W_0, W_1; Y_{12}^n|Z^n) + I(W_0, W_1; Y_{11}^n|Z^n, Y_{12}^n) + I(W_2; Y_{21}^n|W_0, W_1, Z^n)$$
$$+ I(W_2; Y_{22}^n|W_0, W_1, Z^n, Y_{21}^n) + \epsilon_n \tag{3.295}$$

$$= I(W_0, W_1, Y_{21}^n; Y_{12}^n|Z^n) - I(Y_{21}^n; Y_{12}^n|W_0, W_1, Z^n) + I(W_0, W_1; Y_{11}^n|Z^n, Y_{12}^n)$$
$$+ I(W_2; Y_{21}^n|W_0, W_1, Z^n) + I(W_2; Y_{22}^n|W_0, W_1, Z^n, Y_{21}^n) + \epsilon_n \tag{3.296}$$

$$= \mathrm{S}_1 - \mathrm{S}_2 + \mathrm{S}_3 + \mathrm{S}_4 + \mathrm{S}_5 \tag{3.297}$$

where (3.293) follows from Fano's lemma, (3.294) is due to the fact that the eavesdropper's channel is degraded with respect to both users' channels, (3.296) is obtained by adding and subtracting S_2 from the first term of (3.295). Now, we proceed as follows.

$$\mathrm{S}_4 - \mathrm{S}_2 = I(W_2; Y_{21}^n|W_0, W_1, Z^n) - I(Y_{21}^n; Y_{12}^n|W_0, W_1, Z^n) \tag{3.298}$$

$$\leq I(W_2, Y_{12}^n; Y_{21}^n|W_0, W_1, Z^n) - I(Y_{21}^n; Y_{12}^n|W_0, W_1, Z^n) \tag{3.299}$$

$$= I(W_2; Y_{21}^n|W_0, W_1, Z^n, Y_{12}^n) \tag{3.300}$$

Adding S_3 to (3.300), we get

$$\mathrm{S}_3 + \mathrm{S}_4 - \mathrm{S}_2 \leq I(W_0, W_1; Y_{11}^n | Z^n, Y_{12}^n) + I(W_2; Y_{21}^n | W_0, W_1, Z^n, Y_{12}^n) \tag{3.301}$$

$$\leq I(W_0, W_1; Y_{11}^n | Z^n, Y_{12}^n) + I(W_2; Y_{11}^n, Y_{21}^n | W_0, W_1, Z^n, Y_{12}^n) \tag{3.302}$$

$$= I(W_0, W_1; Y_{11}^n | Z^n, Y_{12}^n) + I(W_2; Y_{11}^n | W_0, W_1, Z^n, Y_{12}^n)$$

$$+ I(W_2; Y_{21}^n | W_0, W_1, Z^n, Y_{12}^n, Y_{11}^n) \tag{3.303}$$

$$= I(W_0, W_1, W_2; Y_{11}^n | Z^n, Y_{12}^n) + I(W_2; Y_{21}^n | W_0, W_1, Z^n, Y_{12}^n, Y_{11}^n) \tag{3.304}$$

where the second term is zero as we show next,

$$I(W_2; Y_{21}^n | W_0, W_1, Z^n, Y_{12}^n, Y_{11}^n)$$

$$= H(W_2 | W_0, W_1, Z_1^n, Z_2^n, Y_{12}^n, Y_{11}^n) - H(W_2 | W_0, W_1, Z_1^n, Z_2^n, Y_{12}^n, Y_{11}^n, Y_{21}^n) \tag{3.305}$$

$$= H(W_2 | W_0, W_1, Y_{12}^n, Y_{11}^n) - H(W_2 | W_0, W_1, Y_{12}^n, Y_{11}^n) = 0 \tag{3.306}$$

where we used the following Markov chain

$$(W_0, W_1, W_2) \to (Y_{11}^n, Y_{12}^n) \to (Y_{21}^n, Z_1^n, Z_2^n) \tag{3.307}$$

which is a consequence of the degradation orders that sub-channels exhibit. Thus, (3.304) can be expressed as

$$\begin{aligned} \mathrm{S}_3 + \mathrm{S}_4 - \mathrm{S}_2 &\leq I(W_0, W_1, W_2; Y_{11}^n | Z^n, Y_{12}^n) && (3.308) \\ &= I(W_0, W_1, W_2; Y_{11}^n | Z_1^n, Y_{12}^n) && (3.309) \\ &\leq I(X_1^n, W_0, W_1, W_2; Y_{11}^n | Z_1^n, Y_{12}^n) && (3.310) \\ &= I(X_1^n; Y_{11}^n | Z_1^n, Y_{12}^n) + I(W_0, W_1, W_2; Y_{11}^n | Z_1^n, Y_{12}^n, X_1^n) && (3.311) \end{aligned}$$

where (3.309) follows from the following Markov chain

$$Z_2^n \to Y_{12}^n \to (W_0, W_1, W_2, Y_{11}^n, Z_1^n) \tag{3.312}$$

which is due to the degradedness of the channel. Moreover, the second term in (3.311) is zero as we show next,

$$\begin{aligned} &I(W_0, W_1, W_2; Y_{11}^n | Z_1^n, Y_{12}^n, X_1^n) \\ &= H(W_0, W_1, W_2 | Z_1^n, Y_{12}^n, X_1^n) - H(W_0, W_1, W_2 | Z_1^n, Y_{12}^n, X_1^n, Y_{11}^n) && (3.313) \\ &= H(W_0, W_1, W_2 | Y_{12}^n, X_1^n) - H(W_0, W_1, W_2 | Y_{12}^n, X_1^n) = 0 && (3.314) \end{aligned}$$

where (3.314) follows from the following Markov chain

$$(Y_{11}^n, Z_1^n) \to X_1^n \to (W_0, W_1, W_2, Y_{12}^n) \tag{3.315}$$

Thus, (3.311) turns out to be

$$\mathrm{S}_3 + \mathrm{S}_4 - \mathrm{S}_2 \leq I(X_1^n; Y_{11}^n | Z_1^n, Y_{12}^n) \tag{3.316}$$

which can be further bounded as follows,

$$\begin{aligned}
\mathrm{S}_3 + \mathrm{S}_4 - \mathrm{S}_2 &\leq H(Y_{11}^n | Z_1^n, Y_{12}^n) - H(Y_{11}^n | Z_1^n, Y_{12}^n, X_1^n) && (3.317)\\
&\leq H(Y_{11}^n | Z_1^n) - H(Y_{11}^n | Z_1^n, Y_{12}^n, X_1^n) && (3.318)\\
&= H(Y_{11}^n | Z_1^n) - H(Y_{11}^n | Z_1^n, X_1^n) && (3.319)\\
&\leq \sum_{i=1}^{n} I(X_{1,i}; Y_{11,i} | Z_{1,i}) && (3.320)
\end{aligned}$$

where (3.318) is due to the fact that conditioning cannot increase entropy, (3.319) is due to the following Markov chain

$$(Y_{11}^n, Z_1^n) \to X_1^n \to Y_{12}^n \tag{3.321}$$

Finally, (3.320) is due to our previous result in (3.288). We keep bounding terms in (3.297),

$$\begin{aligned}
\mathrm{S}_5 &= I(W_2; Y_{22}^n | W_0, W_1, Y_{21}^n, Z_1^n, Z_2^n) && (3.322)\\
&= I(W_2; Y_{22}^n | W_0, W_1, Y_{21}^n, Z_2^n) && (3.323)\\
&= \sum_{i=1}^{n} I(W_2; Y_{22,i} | W_0, W_1, Y_{21}^n, Z_2^n, Y_{22}^{i-1}) && (3.324)\\
&= \sum_{i=1}^{n} I(W_2; Y_{22,i} | W_0, W_1, Y_{21}^n, Z_{2,i+1}^n, Y_{22}^{i-1}, Z_{2,i}) && (3.325)\\
&= \sum_{i=1}^{n} I(W_2; Y_{22,i} | U_{2,i}, Z_{2,i}) && (3.326)\\
&\leq \sum_{i=1}^{n} H(Y_{22,i} | U_{2,i}, Z_{2,i}) - H(Y_{22,i} | U_{2,i}, Z_{2,i}, W_2, X_{2,i}) && (3.327)\\
&\leq \sum_{i=1}^{n} I(X_{2,i}; Y_{22,i} | U_{2,i}, Z_{2,i}) && (3.328)
\end{aligned}$$

where (3.323) and (3.325) are due to the following Markov chains

$$Z_1^n \to Y_{21}^n \to (W_0, W_1, W_2, Y_{22}^n, Z_2^n) \tag{3.329}$$

$$Z_2^{i-1} \to Y_{22}^{i-1} \to \left(W_0, W_1, W_2, Y_{21}^n, Z_{2,i}^n, Y_{22,i}\right) \tag{3.330}$$

respectively, (3.327) follows from that conditioning cannot increase entropy and (3.328) is due to the following Markov chain

$$(Y_{22,i}, Z_{2,i}) \to X_{2,i} \to (W_2, U_{2,i}) \tag{3.331}$$

which is a consequence of the fact that each sub-channel is memoryless. Thus, we only need to bound S_1 in (3.297) to reach the outer bound for the sum secrecy rate,

$$\begin{aligned}
\mathrm{S}_1 &= I(W_0, W_1, Y_{21}^n; Y_{12}^n | Z^n) && (3.332)\\
&= \sum_{i=1}^{n} I(W_0, W_1, Y_{21}^n; Y_{12,i} | Z_1^n, Z_2^n, Y_{12}^{i-1}) && (3.333)\\
&\leq \sum_{i=1}^{n} H(Y_{12,i}|Z_{2,i}) - H(Y_{12,i}|Z_1^n, Z_2^n, Y_{12}^{i-1}, W_0, W_1, Y_{21}^n, Y_{22}^{i-1}) && (3.334)\\
&= \sum_{i=1}^{n} H(Y_{12,i}|Z_{2,i}) - H(Y_{12,i}|Z_2^n, Y_{12}^{i-1}, W_0, W_1, Y_{21}^n, Y_{22}^{i-1}) && (3.335)\\
&= \sum_{i=1}^{n} H(Y_{12,i}|Z_{2,i}) - H(Y_{12,i}|W_0, W_1, Y_{21}^n, Y_{22}^{i-1}, Z_{2,i+1}^n, Z_{2,i}) && (3.336)\\
&= \sum_{i=1}^{n} I(U_{2,i}; Y_{12,i}|Z_{2,i}) && (3.337)
\end{aligned}$$

where (3.334) is due to the fact that conditioning cannot increase entropy, (3.335) and (3.336) follow from the following Markov chains

$$Z_1^n \to Y_{21}^n \to \left(W_0, W_1, Y_{22}^{i-1}, Y_{12}^n, Z_2^n\right) \tag{3.338}$$

$$\left(Y_{12}^{i-1}, Z_2^{i-1}\right) \to Y_{22}^{i-1} \to \left(W_0, W_1, W_2, Y_{21}^n, Z_{2,i}^n, Y_{12,i}\right) \tag{3.339}$$

respectively. Thus, plugging (3.320), (3.328) and (3.337) into (3.297), we get the following outer bound on the sum secrecy rate.

$$\begin{aligned}
H(W_0, W_1, W_2|Z^n) \leq \sum_{i=1}^{n} & I(X_{1,i}; Y_{11,i}|Z_{1,i}) + I(X_{2,i}; Y_{22,i}|U_{2,i}, Z_{2,i}) \\
& + I(U_{2,i}; Y_{12,i}|Z_{2,i}) + \epsilon_n
\end{aligned} \tag{3.340}$$

Following similar steps, we can also get the following one

$$H(W_0, W_1, W_2|Z^n) \leq \sum_{i=1}^{n} I(X_{2,i}; Y_{22,i}|Z_{2,i}) + I(X_{1,i}; Y_{11,i}|U_{1,i}, Z_{1,i}) + I(U_{1,i}; Y_{21,i}|Z_{1,i}) + \epsilon_n \tag{3.341}$$

So far, we derived outer bounds, (3.275), (3.276), (3.290), (3.291), (3.340), (3.341), on the capacity region which match the achievable region provided. The only difference can be on the joint distribution that they need to satisfy. However, the outer bounds depend on either $p(u_1, x_1)$ or $p(u_2, x_2)$ but not on the joint distribution $p(u_1, u_2, x_1, x_2)$. Hence, for the outer bound, it is sufficient to consider the joint distributions having the form $p(u_1, u_2, x_1, x_2) = p(u_1, x_1)p(u_2, x_2)$. Thus, the outer bounds derived and the achievable region coincide yielding the capacity region.

3.7.5 Proof of Theorem 3.5

3.7.5.1 Achievability

To show the achievability of the region given in Theorem 3.5, we use Theorem 3.4. First, we group sub-channels into two sets $\mathcal{S}_j, j = 1, 2$, where $\mathcal{S}_j, j = 1, 2$, contains the sub-channels in which user j has the best observation. In other words, we have the Markov chain

$$X_l \to Y_{1l} \to Y_{2l} \to Z_l \tag{3.342}$$

for $l \in \mathcal{S}_1$, and we have this Markov chain

$$X_l \to Y_{2l} \to Y_{1l} \to Z_l \tag{3.343}$$

for $l \in \mathcal{S}_2$.

We replace U_j with $\{U_l\}_{l\in\mathcal{S}_j}$, X_j with $\{X_l\}_{l\in\mathcal{S}_j}$, Y_{j1} with $\{Y_{jl}\}_{l\in\mathcal{S}_1}$, Y_{j2} with $\{Y_{jl}\}_{l\in\mathcal{S}_2}$, and Z_j with $\{Z_l\}_{l\in\mathcal{S}_j}, j = 1, 2$, in Theorem 3.4. Moreover, if we select the pairs $\{(U_l, X_l)\}_{l=1}^M$ to be mutually independent, we get the following joint distribution

$$p\left(\{u_l, x_l, y_{1l}, y_{2l}, z_l\}_{l=1}^M\right) = \prod_{l=1}^M p(u_l, x_l)p(y_{1l}, y_{2l}, z_l|x_l) \tag{3.344}$$

which implies that random variable tuples $\{(u_l, x_l, y_{1l}, y_{2l}, z_l)\}_{l=1}^M$ are mutually independent. Using this fact, one can reach the expressions given in Theorem 3.5.

3.7.5.2 Converse

For the converse part, we again use the proof of Theorem 3.4. First, without loss of generality, we assume $\mathcal{S}_1 = \{1, \ldots, L_1\}$, and $\mathcal{S}_2 = \{L_1 + 1, \ldots, M\}$. We define the following auxiliary random variables

$$U_{1,i} = W_0 W_2 Y_{1[L_1+1:M]}^n Y_{1[1:L_1]}^{i-1} Z_{[1:L_1],i+1}^n \tag{3.345}$$

$$U_{2,i} = W_0 W_1 Y_{2[1:L_1]}^n Y_{2[L_1+1:M]}^{i-1} Z_{[L_1+1:M],i+1}^n \tag{3.346}$$

which satisfy the Markov chains

$$U_{1,i} \to X_{l,i} \to (Y_{1l,i}, Y_{2l,i}, Z_{l,i}), \quad l = 1, \ldots, L_1 \tag{3.347}$$

$$U_{2,i} \to X_{l,i} \to (Y_{1l,i}, Y_{2l,i}, Z_{l,i}), \quad l = L_1 + 1, \ldots, M \tag{3.348}$$

Using the analysis carried out for the proof of Theorem 3.4, we get

$$nR_0 \leq \sum_{i=1}^{n} I(U_{1,i}; Y_{1[1:L_1],i} | Z_{[1:L_1],i}) + \sum_{i=1}^{n} I(U_{2,i}; Y_{1[L_1+1:M],i} | Z_{[L_1+1:M],i}) + \epsilon_n \tag{3.349}$$

where each term will be treated separately. The first term can be bounded as follows

$$I(U_{1,i}; Y_{1[1:L_1],i} | Z_{[1:L_1],i}) = \sum_{l=1}^{L_1} I(U_{1,i}; Y_{1l,i} | Y_{1[1:l-1],i}, Z_{[1:L_1],i}) \tag{3.350}$$

$$= \sum_{l=1}^{L_1} I(U_{1,i}; Y_{1l,i} | Y_{1[1:l-1],i}, Z_{[l:L_1],i}) \tag{3.351}$$

$$\leq \sum_{l=1}^{L_1} I(U_{1,i}, Y_{1[1:l-1],i}, Z_{[l+1:L_1],i}; Y_{1l,i} | Z_{l,i}) \tag{3.352}$$

where (3.351) follows from the Markov chain

$$Z_{[1:l-1],i} \to Y_{1[1:l-1],i} \to (U_{1,i}, Y_{1l,i}, Z_{[l:L_1],i}) \tag{3.353}$$

which is due to the degradedness of the sub-channels. To this end, we define the following auxiliary random variables

$$V_{l,i} = Y_{1[1:l-1],i} Z_{[l+1:L_1],i} U_{1,i}, \quad l = 1, \ldots, L_1 \tag{3.354}$$

which satisfy the Markov chains

$$V_{l,i} \to X_{l,i} \to (Y_{1l,i}, Y_{2l,i}, Z_{l,i}), \quad l = 1, \ldots, L_1 \tag{3.355}$$

Thus, using these new auxiliary random variables in (3.352), we get

$$I(U_{1,i}; Y_{1[1:L_1],i}|Z_{[1:L_1],i}) \leq \sum_{l=1}^{L_1} I(V_{l,i}; Y_{1l,i}|Z_{l,i}) \tag{3.356}$$

We now bound the second term in (3.349) as follows,

$$\begin{aligned}
&I(U_{2,i}; Y_{1[L_1+1:M],i}|Z_{[L_1+1:M],i}) \\
&= \sum_{l=L_1+1}^{M} I(U_{2,i}; Y_{1l,i}|Z_{[L_1+1:M],i}, Y_{1[L_1+1:l-1],i}) && (3.357)\\
&= \sum_{l=L_1+1}^{M} I(U_{2,i}; Y_{1l,i}|Z_{[l:M],i}, Y_{1[L_1+1:l-1],i}) && (3.358)\\
&\leq \sum_{l=L_1+1}^{M} H(Y_{1l,i}|Z_{l,i}) - H(Y_{1l,i}|Z_{[l:M],i}, Y_{1[L_1+1:l-1],i}, U_{2,i}) && (3.359)\\
&\leq \sum_{l=L_1+1}^{M} H(Y_{1l,i}|Z_{l,i}) - H(Y_{1l,i}|Z_{[l:M],i}, Y_{1[L_1+1:l-1],i}, U_{2,i}, Y_{2[L_1+1:l-1],i}) && (3.360)\\
&= \sum_{l=L_1+1}^{M} H(Y_{1l,i}|Z_{l,i}) - H(Y_{1l,i}|Z_{[l:M],i}, U_{2,i}, Y_{2[L_1+1:l-1],i}) && (3.361)\\
&= \sum_{l=L_1+1}^{M} I(Z_{[l+1:M],i}, U_{2,i}, Y_{2[L_1+1:l-1],i}; Y_{1l,i}|Z_{l,i}) && (3.362)
\end{aligned}$$

where (3.358) follows from the Markov chain

$$Z_{[L_1+1:l-1],i} \to Y_{1[L_1+1:l-1],i} \to (U_{2,i}, Z_{[l:M],i}, Y_{1l,i}) \tag{3.363}$$

which is a consequence of the degradedness of the sub-channels, (3.359) and (3.360) follow from the fact that conditioning cannot increase entropy, and (3.361) is due to the Markov chain

$$Y_{1[L_1+1:l-1],i} \rightarrow Y_{2[L_1+1:l-1],i} \rightarrow (U_{2,i}, Z_{[l:M],i}, Y_{1l,i}) \tag{3.364}$$

which is again a consequence of the degradedness of the sub-channels. To this end, we define the following auxiliary random variables

$$V_{l,i} = Y_{2[L_1+1:l-1],i} Z_{[l+1:M],i} U_{2,i}, \quad l = L_1 + 1, \ldots, M \tag{3.365}$$

which satisfy the Markov chains

$$V_{l,i} \rightarrow X_{l,i} \rightarrow (Y_{1l,i}, Y_{2l,i}, Z_{l,i}), \quad l = L_1 + 1, \ldots, M \tag{3.366}$$

Thus, using these new auxiliary random variables in (3.362), we get

$$I(U_{2,i}; Y_{1[L_1+1:M],i} | Z_{[L_1+1:M],i}) \leq \sum_{l=L_1+1}^{M} I(V_{l,i}; Y_{1l,i} | Z_{l,i}) \tag{3.367}$$

Finally, using (3.356) and (3.367) in (3.349), we obtain

$$nR_0 \leq \sum_{i=1}^{n} \sum_{l=1}^{M} I(V_{l,i}; Y_{1l,i} | Z_{l,i}) + \epsilon_n \tag{3.368}$$

Due to symmetry, we also have

$$nR_0 \leq \sum_{i=1}^{n} \sum_{l=1}^{M} I(V_{l,i}; Y_{2l,i}|Z_{l,i}) + \epsilon_n \tag{3.369}$$

We now bound the sum of common and independent message rates. Using the converse proof of Theorem 3.4, we get

$$n(R_0 + R_1) \leq \sum_{i=1}^{n} I(X_{[1:L_1],i}; Y_{1[1:L_1],i}|Z_{[1:L_1],i}) + \sum_{i=1}^{n} I(U_{2,i}; Y_{1[L_1+1:M],i}|Z_{[L_1+M],i}) + \epsilon_n \tag{3.370}$$

where, for the second term we already obtained an outer bound given in (3.367). We now bound the first term,

$$\begin{aligned} I(X_{[1:L_1],i}; Y_{1[1:L_1],i}|Z_{[1:L_1],i}) &= \sum_{l=1}^{L_1} I(X_{[1:L_1],i}; Y_{1l,i}|Z_{[1:L_1],i}, Y_{1[1:l-1],i}) && (3.371) \\ &\leq \sum_{l=1}^{L_1} H(Y_{1l,i}|Z_{l,i}) - H(Y_{1l,i}|Z_{[1:L_1],i}, Y_{1[1:l-1],i}, X_{[1:L_1],i}) && (3.372) \\ &= \sum_{l=1}^{L_1} H(Y_{1l,i}|Z_{l,i}) - H(Y_{1l,i}|Z_{l,i}, X_{l,i}) && (3.373) \\ &= \sum_{l=1}^{L_1} I(X_{l,i}; Y_{1l,i}|Z_{l,i}) && (3.374) \end{aligned}$$

where (3.372) follows from the fact that conditioning cannot increase entropy, and

(3.373) is due to the following Markov chain

$$(Y_{1l,i}, Z_{l,i}) \rightarrow X_{l,i} \rightarrow (X_{[1:l-1],i}, X_{[l+1:L_1],i}, Y_{1[1:l-1],i} Z_{[1:l-1],i}, Z_{[l+1:L_1],i}) \tag{3.375}$$

which follows from the facts that channel is memoryless and sub-channels are independent. Thus, plugging (3.367) and (3.374) into (3.370), we obtain

$$n(R_0 + R_1) \leq \sum_{i=1}^{n} \sum_{l \in \mathcal{S}_1} I(X_{l,i}; Y_{1l,i} | Z_{l,i}) + \sum_{i=1}^{n} \sum_{l \in \mathcal{S}_2} I(V_{l,i}; Y_{1l,i} | Z_{l,i}) + \epsilon_n \tag{3.376}$$

Due to symmetry, we also have

$$n(R_0 + R_1) \leq \sum_{i=1}^{n} \sum_{l \in \mathcal{S}_2} I(X_{l,i}; Y_{2l,i} | Z_{l,i}) + \sum_{i=1}^{n} \sum_{l \in \mathcal{S}_1} I(V_{l,i}; Y_{2l,i} | Z_{l,i}) + \epsilon_n \tag{3.377}$$

We now bound the sum secrecy rate. We first borrow the following outer bound from the converse proof of Theorem 3.4,

$$n(R_0 + R_1 + R_2) \leq \sum_{i=1}^{n} I(X_{[1:L_1],i}; Y_{1[1:L_1],i} | Z_{[1:L_1],i}) \tag{3.378}$$

$$+ \sum_{i=1}^{n} I(X_{[L_1+1:M],i}; Y_{2[L_1+1:M],i} | U_{2,i}, Z_{[L_1+1:M],i}) + \sum_{i=1}^{n} I(U_{2,i}; Y_{1[L_1+1:M],i} | Z_{[L_1+1:M],i}) \tag{3.379}$$

where, for the first and third terms we already obtained outer bounds given in

(3.374) and (3.367), respectively. We now bound the second term as follows,

$$
\begin{aligned}
&I(X_{[L_1+1:M],i}; Y_{2[L_1+1:M],i}|U_{2,i}, Z_{[L_1+1:M],i}) \\
&\qquad = \sum_{l=L_1+1}^{M} I(X_{[L_1+1:M],i}; Y_{2l,i}|U_{2,i}, Z_{[L_1+1:M],i}, Y_{2[L_1+1:l-1],i}) && (3.380)\\
&\qquad = \sum_{l=L_1+1}^{M} I(X_{[L_1+1:M],i}; Y_{2l,i}|U_{2,i}, Z_{[l:M],i}, Y_{2[L_1+1:l-1],i}) && (3.381)\\
&\qquad = \sum_{l=L_1+1}^{M} I(X_{[L_1+1:M],i}; Y_{2l,i}|V_{l,i}, Z_{l,i}) && (3.382)\\
&\qquad = \sum_{l=L_1+1}^{M} H(Y_{2l,i}|V_{l,i}, Z_{l,i}) - H(Y_{2l,i}|V_{l,i}, Z_{l,i}, X_{[L_1+1:M],i}) && (3.383)\\
&\qquad = \sum_{l=L_1+1}^{M} H(Y_{2l,i}|V_{l,i}, Z_{l,i}) - H(Y_{2l,i}|V_{l,i}, Z_{l,i}, X_{l,i}) && (3.384)\\
&\qquad = \sum_{l=L_1+1}^{M} I(X_{l,i}; Y_{2l,i}|V_{l,i}, Z_{l,i}) && (3.385)
\end{aligned}
$$

where (3.381) follows from the Markov chain

$$Z_{[L_1+1:l-1],i} \to Y_{2[L_1+1:l-1],i} \to U_{2,i}, Z_{[l:M],i}, X_{[L_1+1:M],i}, Y_{2l,i} \tag{3.386}$$

which is a consequence of the degradedness of the sub-channels, (3.382) is obtained via using the definition of $V_{2,i}$ given in (3.365), and (3.384) follows from the Markov chain

$$(Z_{l,i}, Y_{2l,i}) \to X_{l,i} \to (V_{l,i}, X_{[L_1+1:l-1],i}, X_{[l+1:M]}) \tag{3.387}$$

which is due to the facts that channel is memoryless and sub-channels are indepen-

dent. Thus, plugging (3.367), (3.374) and (3.385) into (3.379), we get

$$n(R_0+R_1+R_2) \leq \sum_{i=1}^{n}\sum_{l\in\mathcal{S}_1} I(X_{l,i};Y_{1l,i}|Z_{l,i}) + \sum_{i=1}^{n}\sum_{l\in\mathcal{S}_2} I(X_{l,i};Y_{2l,i}|V_{l,i},Z_{l,i}) + \sum_{i=1}^{n}\sum_{l\in\mathcal{S}_2} I(V_{l,i};Y_{1l,i}|Z_{l,i}) + \epsilon_n \tag{3.388}$$

Due to symmetry, we also have

$$n(R_0+R_1+R_2) \leq \sum_{i=1}^{n}\sum_{l\in\mathcal{S}_2} I(X_{l,i};Y_{2l,i}|Z_{l,i}) + \sum_{i=1}^{n}\sum_{l\in\mathcal{S}_1} I(X_{l,i};Y_{1l,i}|V_{l,i},Z_{l,i}) + \sum_{i=1}^{n}\sum_{l\in\mathcal{S}_1} I(V_{l,i};Y_{2l,i}|Z_{l,i}) + \epsilon_n \tag{3.389}$$

Finally, we note that all outer bounds depend on the distributions

$$p(v_{l,i},x_{l,i},y_{1l,i},y_{2l,i},z_{l,i}) = p(v_{l,i},x_{l,i})p(y_{1l,i},y_{2l,i},z_{l,i}|x_{l,i}) \tag{3.390}$$

but not on any joint distributions of the tuples $(v_{l,i},x_{l,i},y_{1l,i},y_{2l,i},z_{l,i})$ implying that selection of the pairs $(v_{l,i},x_{l,i})$ to be mutually independent is optimum.

3.7.6 Proof of Theorem 3.6

We prove Theorem 3.6 in two parts; first, we show achievability, and then we prove the converse.

3.7.6.1 Achievability

Similar to what we have done to show the achievability of Theorem 3.4, we first note that boundary of the capacity region can be decomposed into three surfaces [29].

- First surface:

$$R_0 \leq \bar{\alpha} I(U_2; Y_{12}|Z_2) \tag{3.391}$$

$$R_2 \leq \bar{\alpha} I(X_2; Y_{22}|U_2, Z_2) \tag{3.392}$$

$$R_0 + R_1 \leq \alpha I(X_1; Y_{11}|Z_1) + \bar{\alpha} I(U_2; Y_{12}|Z_2), \quad U_1 = \phi \tag{3.393}$$

- Second surface:

$$R_0 \leq \alpha I(U_1; Y_{21}|Z_1) \tag{3.394}$$

$$R_1 \leq \alpha I(X_1; Y_{11}|U_1, Z_1) \tag{3.395}$$

$$R_0 + R_2 \leq \alpha I(U_1; Y_{21}|Z_1) + \bar{\alpha} I(X_2; Y_{22}|Z_2), \quad U_2 = \phi \tag{3.396}$$

- Third surface:

$$R_1 \leq \alpha I(X_1; Y_{11}|U_1, Z_1) \tag{3.397}$$

$$R_2 \leq \bar{\alpha} I(X_2; Y_{22}|U_2, Z_2) \tag{3.398}$$

$$R_0 \leq \alpha I(U_1; Y_{11}|Z_1) + \bar{\alpha} I(U_2; Y_{12}|Z_2) \tag{3.399}$$

$$R_0 \leq \alpha I(U_1; Y_{21}|Z_1) + \bar{\alpha} I(U_2; Y_{22}|Z_2) \tag{3.400}$$

To show the achievability of each surface, we first introduce a codebook structure.

Codebook generation:

Fix the probability distribution as,

$$p(u_1, x_1)p(u_2, x_2)p(y_1, y_2, z|x) \tag{3.401}$$

- Generate $2^{n(R_{01}+R_{11}+\tilde{R}_{11})}$ length-n_1 sequences $\mathbf{u}_1$ through $p(\mathbf{u}_1) = \prod_{i=1}^{n_1} p(u_{1,i})$ and index them as $\mathbf{u}_1(w_{01}, w_{11}, \tilde{w}_{11})$ where $w_{01} \in \{1, \ldots, 2^{nR_{01}}\}$, $w_{11} \in \{1, \ldots, 2^{nR_{11}}\}$ and $\tilde{w}_{11} \in \{1, \ldots, 2^{n\tilde{R}_{11}}\}$.

- For each $\mathbf{u}_1$, generate $2^{n(R_{12}+\tilde{R}_{12})}$ length-n_1 sequences $\mathbf{x}_1$ through $p(\mathbf{x}_1) = \prod_{i=1}^{n_1} p(x_{1,i}|u_{1,i})$ and index them as $\mathbf{x}_1(w_{01}, w_{11}, \tilde{w}_{11}, w_{12}, \tilde{w}_{12})$ where $w_{12} \in \{1, \ldots, 2^{nR_{12}}\}$, $\tilde{w}_{12} \in \{1, \ldots, 2^{n\tilde{R}_{12}}\}$.

- Generate $2^{n(R_{02}+R_{21}+\tilde{R}_{21})}$ length-$(n - n_1)$ sequences $\mathbf{u}_2$ through $p(\mathbf{u}_2) = \prod_{i=1}^{n-n_1} p(u_{2,i})$ and index them as $\mathbf{u}_2(w_{02}, w_{21}, \tilde{w}_{21})$ where $w_{02} \in \{1, \ldots, 2^{nR_{02}}\}$, $w_{21} \in \{1, \ldots, 2^{nR_{21}}\}$ and $\tilde{w}_{21} \in \{1, \ldots, 2^{n\tilde{R}_{21}}\}$.

- For each $\mathbf{u}_2$, generate $2^{n(R_{22}+\tilde{R}_{22})}$ length-$(n-n_1)$ sequences $\mathbf{x}_2$ through $p(\mathbf{x}_2) = \prod_{i=1}^{n-n_1} p(x_{2,i}|u_{2,i})$ and index them as $\mathbf{x}_2(w_{02}, w_{21}, \tilde{w}_{21}, w_{22}, \tilde{w}_{22})$ where $w_{22} \in \{1, \ldots, 2^{nR_{22}}\}$, $\tilde{w}_{22} \in \{1, \ldots, 2^{n\tilde{R}_{22}}\}$.

- We remark that this codebook uses first channel n_1 times and the other one

$(n - n_1)$ times. We define

$$\alpha = \frac{n_1}{n} \tag{3.402}$$

and $\bar{\alpha} = 1 - \alpha$.

- Furthermore, we set

$$\tilde{R}_{11} = \alpha I(U_1; Z_1) \tag{3.403}$$

$$\tilde{R}_{12} = \alpha I(X_1; Z_1|U_1) \tag{3.404}$$

$$\tilde{R}_{21} = \bar{\alpha} I(U_2; Z_2) \tag{3.405}$$

$$\tilde{R}_{22} = \bar{\alpha} I(X_2; Z_2|U_2) \tag{3.406}$$

$$R_1 = R_{11} + R_{12} \tag{3.407}$$

$$R_2 = R_{21} + R_{22} \tag{3.408}$$

Encoding:

When the transmitted messages are $(w_{01}, w_{02}, w_{11}, w_{12}, w_{21}, w_{22})$, we randomly pick $(\tilde{w}_{11}, \tilde{w}_{12}, \tilde{w}_{21}, \tilde{w}_{22})$ and send corresponding codewords.

Decoding:

Using this codebook structure, we can show that all three surfaces which determine the boundary of the capacity region are achievable. For example, if we set $U_1 = \phi$ (that implies $R_{01} = R_{11} = \tilde{R}_{11} = 0$) and $R_{21} = 0$, then we achieve the

following rates with vanishingly small error probability.

$$R_1 \leq \alpha I(X_1; Y_{11}|Z_1) \tag{3.409}$$

$$R_0 \leq \bar{\alpha} I(U_2; Y_{12}|Z_2) \tag{3.410}$$

$$R_2 \leq \bar{\alpha} I(X_2; Y_{22}|U_2, Z_2) \tag{3.411}$$

Exchanging common message rate with user 1's independent message rate, one can obtain the first surface. Second surface follows from symmetry. For the third surface, we first set $R_{11} = R_{21} = 0$. Moreover, we send common message in its entirety, i.e., we do not use a rate splitting for the common message, hence we set $R_{01} = R_{02} = R_0$, $w_{01} = w_{02} = w_0$. In this case, each user, say the jth one, decodes the common message by looking for a unique w_0 which satisfies

$$E_{j1}^{w_0} = \{\exists \tilde{w}_{01} : (\mathbf{u}_1(w_0, \tilde{w}_{01}), \mathbf{y}_{j1}) \in A_\epsilon^n\} \tag{3.412}$$

$$E_{j2}^{w_0} = \{\exists \tilde{w}_{02} : (\mathbf{u}_2(w_0, \tilde{w}_{02}), \mathbf{y}_{j2}) \in A_\epsilon^n\} \tag{3.413}$$

Following the analysis carried out in (3.227)-(3.238), the sufficient conditions for the common message to be decodable by both users can be found as

$$R_0 \leq \alpha I(U_1; Y_{j1}|Z_1) + \bar{\alpha} I(U_2; Y_{j2}|Z_2), \quad j = 1, 2 \tag{3.414}$$

After decoding the common message, each user can decode its independent message if

$$R_1 \leq \alpha I(X_1; Y_{11}|U_1, Z_1) \tag{3.415}$$

$$R_2 \leq \bar{\alpha} I(X_2; Y_{22}|U_2, Z_2) \tag{3.416}$$

Thus, the third surface can be achieved with vanishingly small error probability. As of now, we showed that all rates in the so-called capacity region are achievable with vanishingly small error probability, however we did not claim anything about the secrecy conditions which will be considered next.

Equivocation computation:

To complete the achievability part of the proof, we need to show that this codebook structure also satisfies the secrecy conditions. For that purpose, it is sufficient to consider the sum rate secrecy condition.

$$H(W_0, W_1, W_2|Z_1^{n_1}, Z_2^{n-n_1}) = H(W_0, W_1, W_2, Z_1^{n_1}, Z_2^{n-n_1}) - H(Z_1^{n_1}, Z_2^{n-n_1}) \tag{3.417}$$

$$= H(W_0, W_1, W_2, U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}, Z_1^{n_1}, Z_2^{n-n_1}) - H(Z_1^{n_1}, Z_2^{n-n_1})$$
$$- H(U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}|W_0, W_1, W_2, Z_1^{n_1}, Z_2^{n-n_1}) \tag{3.418}$$

$$= H(U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}) + H(W_0, W_1, W_2, Z_1^{n_1}, Z_2^{n-n_1}|U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1})$$
$$- H(Z_1^{n_1}, Z_2^{n-n_1}) - H(U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}|W_0, W_1, W_2, Z_1^{n_1}, Z_2^{n-n_1}) \tag{3.419}$$

$$\geq H(U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}) + H(Z_1^{n_1}, Z_2^{n-n_1}|U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1})$$
$$- H(Z_1^{n_1}, Z_2^{n-n_1}) - H(U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}|W_0, W_1, W_2, Z_1^{n_1}, Z_2^{n-n_1}) \tag{3.420}$$

where each term will be treated separately. The first term is

$$
\begin{aligned}
&H(U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}) \\
&= H(U_1^{n_1}, U_2^{n-n_1}) + H(X_1^{n_1}|U_1^{n_1}) + H(X_2^{n-n_1}|U_2^{n-n_1}) && (3.421)\\
&= n(R_0 + R_{11} + \tilde{R}_{11} + R_{21} + \tilde{R}_{21}) + n(R_{12} + \tilde{R}_{12}) + n(R_{22} + \tilde{R}_{22}) && (3.422)\\
&= n(R_0 + R_1 + R_2) + n_1 I(X_1; Z_1) + (n - n_1) I(X_2; Z_2) && (3.423)
\end{aligned}
$$

where the first equality is due to the Markov chain

$$X_1^{n_1} \to U_1^{n_1} \to U_2^{n-n_1} \to X_2^{n-n_1} \tag{3.424}$$

The equality in (3.422) is due to the fact that $(U_1^{n_1}, U_2^{n-n_1})$ can take $2^{n(R_0+R_{11}+\tilde{R}_{11}+R_{21}+\tilde{R}_{21})}$ values uniformly, and given $U_1^{n_1}$ (resp. $U_2^{n-n_1}$), $X_1^{n_1}$ (resp. $X_2^{n-n_1}$) can take $2^{n(R_{12}+\tilde{R}_{12})}$ (resp. $2^{n(R_{22}+\tilde{R}_{22})}$) values with equal probability. To reach (3.423), we use the definitions in (3.403)-(3.408). We consider the second and third terms in (3.420).

$$
\begin{aligned}
&H(Z_1^{n_1}, Z_2^{n-n_1}) - H(Z_1^{n_1}, Z_2^{n-n_1}|U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}) \\
&\leq H(Z_1^{n_1}) + H(Z_2^{n-n_1}) - H(Z_1^{n_1}, Z_2^{n-n_1}|U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1}) && (3.425)\\
&= H(Z_1^{n_1}) + H(Z_2^{n-n_1}) - H(Z_1^{n_1}|X_1^{n_1}) + H(Z_2^{n-n_1}|X_2^{n-n_1}) && (3.426)\\
&= I(X_1^{n_1}; Z_1^{n_1}) + I(X_2^{n-n_1}; Z_2^{n-n_1}) && (3.427)\\
&\leq n_1 I(X_1; Z_1) + (n - n_1) I(X_2; Z_2) + \gamma_{1,n} + \gamma_{2,n} && (3.428)
\end{aligned}
$$

where (3.425) is due to the fact that conditioning cannot increase entropy, (3.426) follows from the Markov chain

$$Z_1^{n_1} \to X_1^{n_1} \to U_1^{n_1} \to U_2^{n-n_1} \to X_2^{n-n_1} \to Z_2^{n-n_1} \tag{3.429}$$

and (3.428) can be shown using the technique devised in [2]. We bound the fourth term of (3.420). To this end, we assume that, given the side information ($W_0 = w_0, W_1 = w_1, W_2 = w_2$), the eavesdropper tries to decode

$$(U_1^{n_1}, X_1^{n_1}, U_2^{n-n_1}, X_2^{n-n_1}) \tag{3.430}$$

Since the confusion message rates are selected to ensure that (see (3.403)-(3.406)) the eavesdropper can decode them as long as side information is available. Consequently, use of Fano's lemma yields

$$H(U_1^{n_1}, U_2^{n-n_1}, X_1^{n_1}, X_2^{n-n_1} | W_0, W_1, W_2, Z_1^{n_1}, Z_2^{n-n_1}) < \epsilon_n \tag{3.431}$$

Finally, plugging (3.423),(3.428) and (3.431) into (3.420), we get

$$H(W_0, W_1, W_2 | Z_1^{n_1}, Z_2^{n-n_1}) \geq n(R_0 + R_1 + R_2) - \epsilon_n - \gamma_{1,n} - \gamma_{2,n} \tag{3.432}$$

which completes the achievability part of the proof.

3.7.6.2 Converse

First, let us define the following auxiliary random variables,

$$U_{1,i} = W_0 W_2 Y_{12}^{n-n_1} Y_{11}^{i-1} Z_{1,i+1}^{n_1}, \quad i = 1, \ldots, n_1 \tag{3.433}$$

$$U_{2,i} = W_0 W_1 Y_{21}^{n_1} Y_{22}^{i-1} Z_{2,i+1}^{n-n_1}, \qquad i = 1, \ldots, n - n_1 \tag{3.434}$$

where we assume that first channel is used n_1 times. We again define

$$\alpha = \frac{n_1}{n} \tag{3.435}$$

We note that auxiliary random variables, $U_{1,i}, U_{2,i}$ satisfy the Markov chains

$$U_{1,i} \to X_{1,i} \to (Y_{11,i}, Y_{21,i}, Z_{1,i}) \tag{3.436}$$

$$U_{2,i} \to X_{2,i} \to (Y_{21,i}, Y_{22,i}, Z_{2,i}) \tag{3.437}$$

Similar to the converse of Theorem 3.4, here again, $U_{1,i}$ and $U_{2,i}$ can be arbitrarily correlated. However, at the end of converse, it will be clear that selection of them

as independent would yield the same region. Start with the common message rate,

$$H(W_0|Z_1^{n_1}, Z_2^{n-n_1}) \tag{3.438}$$

$$\leq I(W_0; Y_{11}^{n_1}, Y_{12}^{n-n_1}) - I(W_0; Z_1^{n_1}, Z_2^{n-n_1}) + \epsilon_n \tag{3.439}$$

$$= I(W_0; Y_{11}^{n_1}, Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) + \epsilon_n \tag{3.440}$$

$$= I(W_0; Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) + I(W_0; Y_{11}^{n_1}|Z_1^{n_1}, Z_2^{n-n_1}, Y_{12}^{n-n_1}) + \epsilon_n \tag{3.441}$$

$$\leq I(W_0, W_1; Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) + I(W_0, W_2; Y_{11}^{n_1}|Z_1^{n_1}, Z_2^{n-n_1}, Y_{12}^{n-n_1}) + \epsilon_n \tag{3.442}$$

where (3.439) is due to Fano's lemma, (3.440) is due to the fact that the eavesdropper's channel is degraded with respect to the first user's channel. Once we obtain (3.442), using the analysis carried out in the proof of Theorem 3.4, we can obtain the following bounds.

$$I(W_0, W_1; Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) \leq \sum_{i=1}^{n-n_1} I(U_{2,i}; Y_{12,i}|Z_{2,i}) \tag{3.443}$$

$$I(W_0, W_2; Y_{11}^{n_1}|Z_1^{n_1}, Z_2^{n-n_1}, Y_{12}^{n-n_1}) \leq \sum_{i=1}^{n_1} I(U_{1,i}; Y_{11,i}|Z_{1,i}) \tag{3.444}$$

where (3.443) (resp. (3.444)) can be derived following the lines from (3.262) (resp. (3.269)) to (3.266) (resp. (3.272)). Thus, we have

$$H(W_0|Z_1^{n_1}, Z_2^{n-n_1}) \leq \sum_{i=1}^{n-n_1} I(U_{2,i}; Y_{12,i}|Z_{2,i}) + \sum_{i=1}^{n_1} I(U_{1,i}; Y_{11,i}|Z_{1,i}) + \epsilon_n \tag{3.445}$$

and similarly, we can get

$$H(W_0|Z_1^{n_1}, Z_2^{n-n_1}) \leq \sum_{i=1}^{n-n_1} I(U_{2,i}; Y_{22,i}|Z_{2,i}) + \sum_{i=1}^{n_1} I(U_{1,i}; Y_{21,i}|Z_{1,i}) + \epsilon_n \tag{3.446}$$

We now consider the sum of common and independent message rates,

$$\begin{aligned}
&H(W_0, W_1|Z_1^{n_1}, Z_2^{n-n_1}) \\
&\leq I(W_0, W_1; Y_{11}^{n_1}, Y_{12}^{n-n_1}) - I(W_0, W_1; Z_1^{n_1}, Z_2^{n-n_1}) + \epsilon_n && (3.447)\\
&= I(W_0, W_1; Y_{11}^{n_1}, Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) + \epsilon_n && (3.448)\\
&= I(W_0, W_1; Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) + I(W_0, W_1; Y_{11}^{n_1}|Z_1^{n_1}, Z_2^{n-n_1}, Y_{12}^{n-n_1}) + \epsilon_n && (3.449)
\end{aligned}$$

where (3.447) is due to Fano's lemma, (3.448) follows from the fact that the eavesdropper's channel is degraded with respect to the first user's channel. The first term of (3.449) is already bounded in (3.443). The second term can be bounded as

$$I(W_0, W_1; Y_{11}^{n_1}|Z_1^{n_1}, Z_2^{n-n_1}, Y_{12}^{n-n_1}) \leq \sum_{i=1}^{n_1} I(X_{1,i}; Y_{11,i}|Z_{1,i}) \tag{3.450}$$

which can be obtained following the lines from (3.282) to (3.288). Hence, plugging (3.443) and (3.450) into (3.449), we get

$$H(W_0, W_1|Z_1^{n_1}, Z_2^{n-n_1}) \leq \sum_{i=1}^{n-n_1} I(U_{2,i}; Y_{12,i}|Z_{2,i}) + \sum_{i=1}^{n_1} I(X_{1,i}; Y_{11,i}|Z_{1,i}) + \epsilon_n \tag{3.451}$$

Similarly, we can obtain

$$H(W_0, W_2|Z_1^{n_1}, Z_2^{n-n_1}) \leq \sum_{i=1}^{n-n_1} I(X_{2,i}; Y_{22,i}|Z_{2,i}) + \sum_{i=1}^{n_1} I(U_{1,i}; Y_{21,i}|Z_{1,i}) + \epsilon_n \quad (3.452)$$

Finally, we derive the outer bounds for the sum secrecy rate,

$$\begin{aligned} H(W_0, W_1, W_2|Z_1^{n_1}, Z_2^{n-n_1}) &\leq I(W_0, W_1; Y_{11}^{n_1}, Y_{12}^{n-n_1}) + I(W_2; Y_{21}^{n_1}, Y_{22}^{n-n_1}|W_0, W_1) \\ &\quad - I(W_0, W_1, W_2; Z_1^{n_1}, Z_2^{n-n_1}) + \epsilon_n \quad (3.453) \\ &= I(W_0, W_1; Y_{11}^{n_1}, Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) + I(W_2; Y_{21}^{n_1}, Y_{22}^{n-n_1}|W_0, W_1, Z_1^{n_1}, Z_2^{n-n_1}) + \epsilon_n \quad (3.454) \\ &= I(W_0, W_1; Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) + I(W_0, W_1; Y_{11}^{n_1}|Z_1^{n_1}, Z_2^{n-n_1}, Y_{12}^{n-n_1}) \\ &\quad + I(W_2; Y_{21}^{n_1}|W_0, W_1, Z_1^{n_1}, Z_2^{n-n_1}) + I(W_2; Y_{22}^{n-n_1}|W_0, W_1, Z_1^{n_1}, Z_2^{n-n_1}, Y_{21}^{n_1}) + \epsilon_n \quad (3.455) \\ &= I(W_0, W_1, Y_{21}^{n_1}; Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}) - I(Y_{21}^{n_1}; Y_{12}^{n-n_1}|Z_1^{n_1}, Z_2^{n-n_1}, W_0, W_1) \\ &\quad + I(W_0, W_1; Y_{11}^{n_1}|Z_1^{n_1}, Z_2^{n-n_1}, Y_{12}^{n-n_1}) + I(W_2; Y_{21}^{n_1}|W_0, W_1, Z_1^{n_1}, Z_2^{n-n_1}) \\ &\quad + I(W_2; Y_{22}^{n-n_1}|W_0, W_1, Z_1^{n_1}, Z_2^{n-n_1}, Y_{21}^{n_1}) + \epsilon_n \quad (3.456) \\ &= S_1 - S_2 + S_3 + S_4 + S_5 + \epsilon_n \quad (3.457) \end{aligned}$$

where in (3.453), we used Fano's lemma and (3.454) follows from the fact that the eavesdropper's channel is degraded with respect to both users' channels. We can again use the analysis carried out in the converse proof of Theorem 3.4 to bound

(3.457). For example, following lines from (3.298) to (3.320), we can obtain

$$S_4 + S_3 - S_2 \leq \sum_{i=1}^{n_1} I(X_{1,i}; Y_{11,i}|Z_{1,i}) \tag{3.458}$$

Similarly, if we follow the analysis from (3.322) to (3.328), we can get

$$S_5 \leq \sum_{i=1}^{n-n_1} I(X_{2,i}; Y_{22,i}|U_{2,i}, Z_{2,i}) \tag{3.459}$$

and if we follow the lines from (3.332) to (3.337), we can get

$$S_1 \leq \sum_{i=1}^{n-n_1} I(U_{2,i}; Y_{12,i}|Z_{2,i}) \tag{3.460}$$

Thus, plugging (3.458), (3.459) and (3.460) into (3.457), we get

$$\begin{aligned} H(W_0, W_1, W_2|Z_1^{n_1}, Z_2^{n-n_1}) \leq & \sum_{i=1}^{n_1} I(X_{1,i}; Y_{11,i}|Z_{1,i}) + \sum_{i=1}^{n-n_1} I(U_{2,i}; Y_{12,i}|Z_{2,i}) \\ & + \sum_{i=1}^{n-n_1} I(X_{2,i}; Y_{22,i}|U_{2,i}, Z_{2,i}) + \epsilon_n \end{aligned} \tag{3.461}$$

Similarly, it can be shown that

$$\begin{aligned} H(W_0, W_1, W_2|Z_1^{n_1}, Z_2^{n-n_1}) \leq & \sum_{i=1}^{n_1} I(U_{1,i}, Y_{21,i}|Z_{2,i}) + \sum_{i=1}^{n_1} I(X_{1,i}; Y_{11,i}|U_{1,i}, Z_{1,i}) \\ & + \sum_{i=1}^{n-n_1} I(X_{2,i}; Y_{22,i}|Z_{2,i}) \end{aligned} \tag{3.462}$$

So far, we derived outer bounds on the secrecy capacity region which match the achievable region. Hence, to claim that this is indeed the capacity region, we need to show that computing the outer bounds over all distributions of the form $p(u_1, x_1)p(u_2, x_2)$ yields the same region which we would obtain by computing over all $p(u_1, u_2, x_1, x_2)$. Since all the expressions involved in the outer bounds depend on either $p(u_1, x_1)$ or $p(u_2, x_2)$ but not on the joint distribution $p(u_1, u_2, x_1, x_2)$, this argument follows, establishing the secrecy capacity region.

Chapter 4

Capacity Region of the Gaussian MIMO Broadcast Channel with Common and Confidential Messages

4.1 Introduction

In this chapter, we consider the two-user Gaussian MIMO broadcast channel with common and confidential messages, where the transmitter sends a confidential message to each user which needs to be kept perfectly secret from the other user in addition to a common message directed to both users (see Figure 4.1). In other words, in this channel model, there are three messages W_0, W_1, W_2, where W_0 denotes the common message sent to both users, W_1 denotes the first user's confidential message that needs to be kept hidden from the second user, and W_2 denotes the second user's confidential message that needs to be kept hidden from the first user.

The Gaussian MIMO broadcast channel with common and confidential messages subsumes several other channel models as special cases. These special cases can be obtained from our channel model by disabling some of the messages W_0, W_1, W_2. The first such channel model is the Gaussian MIMO wiretap channel, where the transmitter has only one confidential message for one (legitimate) user, which is kept perfectly secret from the other user (eavesdropper). This channel model can be obtained from our channel model by setting $W_0 = W_2 = \phi$. The secrecy capacity

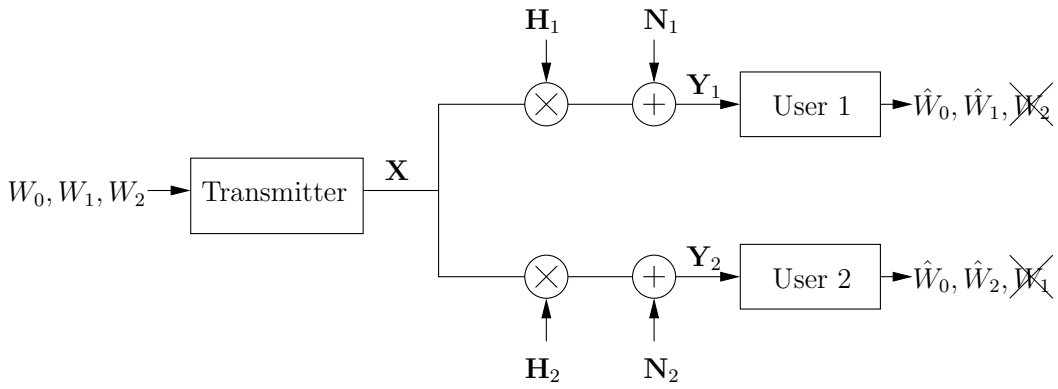

Figure 4.1: Gaussian MIMO broadcast channel with common and confidential messages.

of the Gaussian MIMO wiretap channel is obtained in [15, 16] for the general case, in [17] for the 2-2-1 case. The second such channel model is the Gaussian MIMO wiretap channel with common message [18], in which the transmitter sends a common message to both the legitimate user and the eavesdropper, and a confidential message to the legitimate user that is kept perfectly secret from the eavesdropper. This channel model can be obtained from our channel model by setting $W_2 = \phi$. The capacity region of the Gaussian MIMO wiretap channel with common message is obtained in [18]. The third such channel model is the Gaussian MIMO broadcast channel with confidential messages [8], where the transmitter sends a confidential message to each user which is kept perfectly secret from the other user. This channel model can be obtained from our channel model by setting $W_0 = \phi$. The capacity region of the Gaussian MIMO broadcast channel with confidential messages is established in [8].

Here, we obtain the capacity region of the Gaussian MIMO broadcast channel

with common and confidential messages[1]. In particular, we show that a variant of the secret dirty-paper coding (S-DPC) scheme proposed in [8] is capacity-achieving. Since the S-DPC scheme proposed in [8] is for the transmission of only two confidential messages, it is modified here to incorporate the transmission of a common message as well. Similar to [8], we also notice an invariance property of this achievable scheme with respect to the encoding order used in the S-DPC scheme. In other words, two achievable rate regions arising from two possible encoding orders used in the S-DPC scheme are identical, and equal to the capacity region. We provide the proof of this statement as well as the converse proof for the capacity region by using the channel enhancement technique [4] and an extremal inequality [5].

We also explore the connections between our channel model and its non-confidential counterpart, i.e., the (two-user) Gaussian MIMO broadcast channel with common and private messages. In the Gaussian MIMO broadcast channel with common and private messages, the transmitter again sends a common message to both users, and a private message to each user, for which there is no secrecy constraint now, i.e., private message of each user does not need to be kept secret from the other user. Thus, the channel model we study here can be viewed as a constrained version of the Gaussian MIMO broadcast channel with common and private messages, where the constraint comes through forcing the private messages to be confidential. We note that although there are partial results for the Gaussian MIMO broadcast channel with common and private messages [9, 10], its capacity

[1]The same result is obtained independently and concurrently in [31, 32]. The conference version [31] and the conference version of the work in this chapter [33] appeared concurrently at the IEEE ISIT 2010 as well as at [arXiv: 1001.2806] and [arXiv:1001:3297].

region is not known completely. However, here, we are able to obtain the entire capacity region for a constrained version of the Gaussian MIMO broadcast channel with common and private messages. We provide an intuitive explanation of this at-first-sight surprising point as well as the invariance property of the achievable rate region with respect to the encoding orders that can be used in the S-DPC scheme, by using a result from [10]. In particular, we use the following result from [10]: For a given common message rate, the private message sum rate capacity of the Gaussian MIMO broadcast channel with common and private messages is achieved by the dirty-paper coding (DPC) scheme in [34], and any one of the two possible encoding orders that can be used in DPC gives the private message sum rate capacity. Using this result, we show that there is a one-to-one correspondence between the points on the boundary of the achievable rate region of the Gaussian MIMO broadcast channel with common and confidential messages that are obtained by using a specific encoding order in the S-DPC scheme, and those points which are private message sum rate capacity achieving for the Gaussian MIMO broadcast channel with common and private messages. This correspondence intuitively explains why the achievable rate regions arising from the use of different encoding orders in S-DPC are the same, and also why we can obtain the entire capacity region of the Gaussian MIMO broadcast channel with common and confidential messages although the capacity region of its non-confidential counterpart is not known completely.

4.2 Channel Model and Main Result

We study the two-user Gaussian MIMO broadcast channel (see Figure 4.1) which is defined by

$$\mathbf{Y}_1 = \mathbf{H}_1\mathbf{X} + \mathbf{N}_1 \tag{4.1}$$

$$\mathbf{Y}_2 = \mathbf{H}_2\mathbf{X} + \mathbf{N}_2 \tag{4.2}$$

where the channel input $\mathbf{X}$ is a $t \times 1$ vector, $\mathbf{H}_j$ is the channel gain matrix of size $r_j \times t$, the channel output of the jth user $\mathbf{Y}_j$ is a $r_j \times 1$ vector, and the Gaussian random vector $\mathbf{N}_j$ is of size $r_j \times 1$ with a covariance matrix $\mathbf{\Sigma}_j$ which is assumed to be strictly positive-definite, i.e., $\mathbf{\Sigma}_j \succ \mathbf{0}$. We consider a covariance constraint on the channel input as follows

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{4.3}$$

where $\mathbf{S} \succeq \mathbf{0}$.

We study the following scenario for the Gaussian MIMO broadcast channel: There are three independent messages (W_0, W_1, W_2) with rates (R_0, R_1, R_2), respectively, where W_0 is the common message that needs to be delivered to both users, W_1 is the confidential message of the first user which needs to be kept perfectly secret from the second user, and similarly, W_2 is the confidential message of the second user which needs to be kept perfectly secret from the first user. The secrecy of the confidential messages is measured by the normalized mutual information rates [2, 3],

i.e, we require

$$\frac{1}{n}I(W_1; W_0, W_2, \mathbf{Y}_2^n) \to 0 \;\text{ and }\; \frac{1}{n}I(W_2; W_0, W_1, \mathbf{Y}_1^n) \to 0 \tag{4.4}$$

as $n \to \infty$, where n denotes the number of channel uses. The closure of all achievable rate triples (R_0, R_1, R_2) is defined to be the capacity region, and will be denoted by $\mathcal{C}(\mathbf{S})$. We next define the following shorthand notations

$$R_{0j}(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{H}_j\mathbf{S}\mathbf{H}_j^\top + \mathbf{\Sigma}_j|}{|\mathbf{H}_j(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_j^\top + \mathbf{\Sigma}_j|}, \quad j = 1, 2 \tag{4.5}$$

$$R_1(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{H}_1(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_1^\top + \mathbf{\Sigma}_1|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top + \mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{H}_2(\mathbf{K}_1+\mathbf{K}_2)\mathbf{H}_2^\top + \mathbf{\Sigma}_2|}{|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top + \mathbf{\Sigma}_2|} \tag{4.6}$$

$$R_2(\mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_1^\top + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{4.7}$$

using which, our main result can be stated as follows.

Theorem 4.1 *The capacity region of the Gaussian MIMO broadcast channel with common and confidential messages* $\mathcal{C}(\mathbf{S})$ *is given by*

$$\mathcal{C}(\mathbf{S}) = \mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S}) = \mathcal{R}_{21}^{\text{S-DPC}}(\mathbf{S}) \tag{4.8}$$

where $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})$ *is given by the union of rate triples* (R_0, R_1, R_2) *satisfying*

$$R_0 \leq \min\{R_{01}(\mathbf{K}_1, \mathbf{K}_2), R_{02}(\mathbf{K}_1, \mathbf{K}_2)\} \tag{4.9}$$

$$R_1 \leq R_1(\mathbf{K}_1, \mathbf{K}_2) \tag{4.10}$$

$$R_2 \leq R_2(\mathbf{K}_2) \tag{4.11}$$

for some positive semi-definite matrices $\mathbf{K}_1, \mathbf{K}_2$ *such that* $\mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$*, and* $\mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$ *can be obtained from* $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})$ *by swapping the subscripts* 1 *and 2.*

Theorem 4.1 states that the common message, for which a covariance matrix $\mathbf{S} - \mathbf{K}_1 - \mathbf{K}_2$ is allotted, should be encoded by using a standard Gaussian codebook, and the confidential messages, for which covariance matrices $\mathbf{K}_1, \mathbf{K}_2$ are allotted, need to be encoded by using the S-DPC scheme proposed in [8]. S-DPC is a modified version of DPC [12] to meet the secrecy requirements. The receivers first decode the common message by treating the confidential messages as noise, and then each receiver decodes the confidential message intended to itself. Depending on the encoding order used in S-DPC, one of the users gets a clean link for the transmission of its confidential message, where there is no interference originating from the other user's confidential message. Although one might expect that the two achievable regions arising from two possible encoding orders that can be used in S-DPC could be different, i.e., $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S}) \neq \mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$, and taking a convex closure of these two regions would yield a larger achievable rate region, Theorem 4.1 states that $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S}) = \mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$, i.e., the achievable rate region is invariant with respect to the encoding order used in S-DPC. This invariance property of S-DPC was first

noticed in [8] for the case where there was no common message to be transmitted.

We acknowledge [31, 32], where the authors obtain Theorem 4.1 (capacity region of the Gaussian MIMO broadcast channel with common and confidential messages) independently and concurrently. Their proof is identical to the one we present here.

4.2.1 Aligned Channel

We define a sub-class of Gaussian MIMO broadcast channels called the aligned Gaussian MIMO broadcast channel, which can be obtained from (4.1)-(4.2) by setting $\mathbf{H}_1 = \mathbf{H}_2 = \mathbf{I}$, i.e.,

$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{N}_1 \tag{4.12}$$

$$\mathbf{Y}_2 = \mathbf{X} + \mathbf{N}_2 \tag{4.13}$$

To distinguish the notation used for the aligned Gaussian MIMO broadcast channel from the one used for the general model in (4.1)-(4.2), we denote the capacity region of the aligned channel by $\mathcal{C}^{\mathrm{AL}}(\mathbf{S})$, the rate expressions in (4.5)-(4.7) for the special case $\mathbf{H}_1 = \mathbf{H}_2 = \mathbf{I}$ by $\{R_{0j}^{\mathrm{AL}}(\mathbf{K}_1, \mathbf{K}_2)\}_{j=1}^{2}, R_1^{\mathrm{AL}}(\mathbf{K}_1, \mathbf{K}_2), R_2^{\mathrm{AL}}(\mathbf{K}_2)$, and the regions $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S}), \mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$ for the special case $\mathbf{H}_1 = \mathbf{H}_2 = \mathbf{I}$ by $\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S}), \mathcal{R}_{21}^{\mathrm{S-DPC-AL}}(\mathbf{S})$.

In this work, we first prove Theorem 4.1 for the aligned Gaussian MIMO broadcast channel. Then, we establish the capacity region for the general channel model in (4.1)-(4.2) by following the analysis in Section V.B of [4] and Section 7.1

of [19] in conjunction with the capacity result we obtain for the aligned channel.

4.2.2 Capacity Region under a Power Constraint

We note that the covariance constraint on the channel input in (4.3) is a rather general constraint that subsumes the power constraint

$$E\left[\mathbf{X}^{\top}\mathbf{X}\right] = \mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^{\top}\right]\right) \leq P \tag{4.14}$$

as a special case, see Lemma 1 and Corollary 1 of [4]. Therefore, using Theorem 4.1, the capacity region arising from the average power constraint in (4.14), $\mathcal{C}(P)$, can be found as follows.

Corollary 4.1 *The capacity region of the Gaussian MIMO broadcast channel with common and confidential messages subject to a power constraint P, $\mathcal{C}(P)$, is given by*

$$\mathcal{C}(P) = \mathcal{R}_{12}^{\mathrm{S-DPC}}(P) = \mathcal{R}_{21}^{\mathrm{S-DPC}}(P) \tag{4.15}$$

where $\mathcal{R}_{12}^{\mathrm{S-DPC}}(P)$ is given by the union of rate triples (R_0, R_1, R_2) satisfying

$$R_0 \leq \min\{R_{01}(\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_c), R_{02}(\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_c)\} \tag{4.16}$$

$$R_1 \leq R_1(\mathbf{K}_1, \mathbf{K}_2) \tag{4.17}$$

$$R_2 \leq R_2(\mathbf{K}_2) \tag{4.18}$$

for some positive semi-definite matrices $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_c$ *such that* $\mathrm{tr}(\mathbf{K}_1+\mathbf{K}_2+\mathbf{K}_c) \leq P$*, and* $\{R_{0j}(\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_c)\}_{j=1}^2$ *are defined as*

$$R_{0j}(\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_c) = \frac{1}{2} \log \frac{|\mathbf{H}_j(\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{K}_c)\mathbf{H}_j^\top + \mathbf{\Sigma}_j|}{|\mathbf{H}_j(\mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_j^\top + \mathbf{\Sigma}_j|}, \quad j = 1, 2 \tag{4.19}$$

Moreover, $\mathcal{R}_{21}^{\mathrm{S-DPC}}(P)$ *can be obtained from* $\mathcal{R}_{12}^{\mathrm{S-DPC}}(P)$ *by swapping the subscripts* 1 *and 2.*

4.3 Proof of Theorem 4.1 for the Aligned Case

4.3.1 Achievability

Here, we prove the achievability of the regions $\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})$ and $\mathcal{R}_{21}^{\mathrm{S-DPC-AL}}(\mathbf{S})$. To this end, we consider the two-user discrete memoryless channel with common and confidential messages. For this case, we have the following achievable rate region [35].

Lemma 4.1 ([35, Theorem 1]) *The rate triples* (R_0, R_1, R_2) *satisfying*

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} \tag{4.20}$$

$$R_1 \leq [I(V_1; Y_1|U) - I(V_1; Y_2, V_2|U)]^+ \tag{4.21}$$

$$R_2 \leq [I(V_2; Y_2|U) - I(V_2; Y_1, V_1|U)]^+ \tag{4.22}$$

for some (U, V_1, V_2) *such that* $(U, V_1, V_2) \to X \to (Y_1, Y_2)$[2] *are achievable.*

[2]In [35], the necessary Markov chain that $(U, V_1, V_2, X, Y_1, Y_2)$ needs to satisfy is given by $U \to (V_1, V_2) \to X \to (Y_1, Y_2)$. However, their achievable rate region is valid for the looser Markov chain $(U, V_1, V_2) \to X \to (Y_1, Y_2)$ as well, which we use here.

We now use Lemma 4.1 to show the achievability of the region $\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})$. We first introduce three independent Gaussian random vectors $\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2$ with covariance matrices $\mathbf{S}-\mathbf{K}_1-\mathbf{K}_2, \mathbf{K}_1, \mathbf{K}_2$, respectively. Using these Gaussian random vectors, we set the auxiliary random variables in Lemma 4.1 as follows

$$U = \mathbf{U}_0 \tag{4.23}$$

$$V_1 = \mathbf{U}_1 + \mathbf{U}_0 \tag{4.24}$$

$$V_2 = \mathbf{U}_2 + \mathbf{A}\mathbf{U}_1 + \mathbf{U}_0 \tag{4.25}$$

where $\mathbf{A} = \mathbf{K}_2 \left[\mathbf{K}_2 + \mathbf{\Sigma}_2\right]^{-1}$ is the precoding matrix for the second user to suppress the interference originating from $\mathbf{U}_1$ [12]. Furthermore, we set the channel input $\mathbf{X}$ as follows

$$\mathbf{X} = \mathbf{U}_0 + \mathbf{U}_1 + \mathbf{U}_2 \tag{4.26}$$

Using the definitions in (4.23)-(4.26) for the common message rate given in Lemma 4.1, we get

$$R_0 = \min\left\{\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_1|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_1|}, \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_2|}\right\} \tag{4.27}$$

Next, we compute the confidential message rates. To this end, we note the following identity

$$I(V_2;\mathbf{Y}_2|U) - I(V_2;V_1|U) = \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} \tag{4.28}$$

which is due to Theorem 1 in [12]. Now, we compute the second user's confidential message rate as follows

$$\begin{aligned}
R_2 &= I(V_2;\mathbf{Y}_2|U) - I(V_2;\mathbf{Y}_1,V_1|U) && (4.29)\\
&= I(V_2;\mathbf{Y}_2|U) - I(V_2;V_1|U) - I(V_2;\mathbf{Y}_1|U,V_1) && (4.30)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - I(V_2;\mathbf{Y}_1|U,V_1) && (4.31)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} && (4.32)
\end{aligned}$$

where (4.31) is due to (4.28). Next, we compute the first user's confidential message rate as follows

$$\begin{aligned}
R_1 &= I(V_1;\mathbf{Y}_1|U) - I(V_1;\mathbf{Y}_2,V_2|U) && (4.33)\\
&= I(V_1;\mathbf{Y}_1|U) - I(V_1;\mathbf{Y}_2|U,V_2) - I(V_1;V_2|U) && (4.34)\\
&= I(V_1;\mathbf{Y}_1|U) - I(V_1,V_2;\mathbf{Y}_2|U) + I(V_2;\mathbf{Y}_2|U) - I(V_1;V_2|U) && (4.35)\\
&= I(V_1;\mathbf{Y}_1|U) - I(V_1,V_2;\mathbf{Y}_2|U) + \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} && (4.36)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_1|}{|\mathbf{K}_2+\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} && (4.37)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_1|}{|\mathbf{K}_2+\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{K}_2+\mathbf{\Sigma}_2|} && (4.38)
\end{aligned}$$

where (4.36) is due to (4.28). Hence, we show the achievability of the region $\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})$. Due to the symmetry, achievability of $\mathcal{R}_{21}^{\mathrm{S-DPC-AL}}(\mathbf{S})$ follows.

4.3.2 Converse

Since the capacity region $\mathcal{C}^{\mathrm{AL}}(\mathbf{S})$ is convex due to time-sharing, it can be characterized by the tangent planes to it, i.e., by the solution of

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}^{\mathrm{AL}}(\mathbf{S})} \mu_0 R_0 + \mu_1 R_1 + \mu_2 R_2 \tag{4.39}$$

for $\mu_j \in [0,\infty),\ j=0,1,2$. We already have

$$\max_{(R_0,R_1,R_2)\in\mathcal{R}^{\mathrm{S-DPC-AL}}(\mathbf{S})} \mu_0 R_0 + \mu_1 R_1 + \mu_2 R_2 \leq \max_{(R_0,R_1,R_2)\in\mathcal{C}^{\mathrm{AL}}(\mathbf{S})} \mu_0 R_0 + \mu_1 R_1 + \mu_2 R_2 \tag{4.40}$$

due to achievability of $\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})$ and $\mathcal{R}_{21}^{\mathrm{S-DPC-AL}}(\mathbf{S})$, where $\mathcal{R}^{\mathrm{S-DPC-AL}}(\mathbf{S})$ is given by

$$\mathcal{R}^{\mathrm{S-DPC-AL}}(\mathbf{S}) = \mathrm{conv}\left(\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S}) \bigcup \mathcal{R}_{21}^{\mathrm{S-DPC-AL}}(\mathbf{S})\right) \tag{4.41}$$

and conv is the convex hull operator. Here, we show that

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}^{\mathrm{AL}}(\mathbf{S})} \mu_0 R_0+\mu_1 R_1+\mu_2 R_2 \leq \max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})} \mu_0 R_0+\mu_1 R_1+\mu_2 R_2 \tag{4.42}$$

$$= \max_{(R_0,R_1,R_2)\in\mathcal{R}_{21}^{\mathrm{S-DPC-AL}}(\mathbf{S})} \mu_0 R_0+\mu_1 R_1+\mu_2 R_2 \tag{4.43}$$

to provide the converse proof. We first characterize the boundary of $\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})$ by studying the following optimization problem

$$\max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})} \mu_0 R_0+\mu_1 R_1+\mu_2 R_2 \tag{4.44}$$

which can be written as

$$\max_{\substack{\mathbf{0}\preceq\mathbf{K}_j,\ j=1,2\\ \mathbf{K}_1+\mathbf{K}_2\preceq\mathbf{S}}} \mu_0 \min\{R_{01}^{\mathrm{AL}}(\mathbf{K}_1,\mathbf{K}_2), R_{02}^{\mathrm{AL}}(\mathbf{K}_1,\mathbf{K}_2)\}+\mu_1 R_1^{\mathrm{AL}}(\mathbf{K}_1,\mathbf{K}_2)+\mu_2 R_2^{\mathrm{AL}}(\mathbf{K}_2) \tag{4.45}$$

Let $\mathbf{K}_1^*, \mathbf{K}_2^*$ be the maximizer of (4.45). The necessary KKT conditions that $\mathbf{K}_1^*, \mathbf{K}_2^*$ need to satisfy are given in the following lemma.

Lemma 4.2 $\mathbf{K}_1^*, \mathbf{K}_2^*$ *need to satisfy*

$$(\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1=(\mu_0\lambda+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1} + (\mu_0\bar{\lambda}+\mu_1)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_S \quad (4.46)$$

$$(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_2=(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1 \quad (4.47)$$

for some positive semi-definite matrices $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_S$ *such that*

$$\mathbf{K}_1^*\mathbf{M}_1=\mathbf{M}_1\mathbf{K}_1^*=\mathbf{0} \quad (4.48)$$

$$\mathbf{K}_2^*\mathbf{M}_2=\mathbf{M}_2\mathbf{K}_2^*=\mathbf{0} \quad (4.49)$$

$$(\mathbf{S}-\mathbf{K}_1^*-\mathbf{K}_2^*)\mathbf{M}_S=\mathbf{M}_S(\mathbf{S}-\mathbf{K}_1^*-\mathbf{K}_2^*)=\mathbf{0} \quad (4.50)$$

and for some $\lambda=1-\bar{\lambda}$ *such that it satisfies* $0\le\lambda\le 1$ *and*

$$\lambda\begin{cases} = 0 & \text{if} \quad R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) > R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) \\ = 1 & \text{if} \quad R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) < R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) \\ \neq 0,1 & \text{if} \quad R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) = R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) \end{cases} \quad (4.51)$$

The proof of Lemma 4.2 is given in Appendix 4.7.1.

We now use channel enhancement [4] to define a new noise covariance matrix $\tilde{\mathbf{\Sigma}}$ as follows

$$(\mu_1+\mu_2)(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}=(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_2 \quad (4.52)$$

This new noise covariance matrix $\tilde{\mathbf{\Sigma}}$ has useful properties which are listed in the following lemma.

Lemma 4.3 *We have the following facts.*

- $\mathbf{0} \prec \tilde{\mathbf{\Sigma}}$
- $\tilde{\mathbf{\Sigma}} \preceq \mathbf{\Sigma}_1$, $\tilde{\mathbf{\Sigma}} \preceq \mathbf{\Sigma}_2$
- $(\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1} = (\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1$
- $(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}\tilde{\mathbf{\Sigma}} = (\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}\mathbf{\Sigma}_2$
- $(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}) = (\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^*+\mathbf{\Sigma}_1)$

The proof of Lemma 4.3 is given in Appendix 4.7.2. We now construct an enhanced channel using the new covariance matrix $\tilde{\mathbf{\Sigma}}$ as follows

$$\tilde{\mathbf{Y}}_1 = \mathbf{X} + \tilde{\mathbf{N}} \tag{4.53}$$

$$\tilde{\mathbf{Y}}_2 = \mathbf{X} + \tilde{\mathbf{N}} \tag{4.54}$$

$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{N}_1 \tag{4.55}$$

$$\mathbf{Y}_2 = \mathbf{X} + \mathbf{N}_2 \tag{4.56}$$

where $\tilde{\mathbf{N}}$ is a Gaussian random vector with a covariance matrix $\tilde{\mathbf{\Sigma}}$. In the enhanced channel defined by (4.53)-(4.56), the enhanced first and second users have the same observation, i.e., $\Pr[\tilde{\mathbf{Y}}_1 = \tilde{\mathbf{Y}}_2] = 1$. From now on, we denote the observations of the enhanced first and second users by a single random vector $\tilde{\mathbf{Y}}$. We now consider the following scenario for the enhanced channel in (4.53)-(4.56): There

are three independent messages (W_0, W_1, W_2) with rates (R_0, R_1, R_2), respectively, where the common message W_0 is directed to all users, i.e., the users with observations $\tilde{\mathbf{Y}}_1, \tilde{\mathbf{Y}}_2, \mathbf{Y}_1, \mathbf{Y}_2$; W_1 is the confidential message of the enhanced first user, i.e., the one with observation $\tilde{\mathbf{Y}}$, which needs to be kept perfectly secret from the second user, i.e., the one with observation $\mathbf{Y}_2$; and W_2 is the confidential message of the enhanced second user, i.e., the one with observation $\tilde{\mathbf{Y}}$, which needs to be kept perfectly secret from the first user, i.e., the one with observation $\mathbf{Y}_1$. Here also, we measure the secrecy of the confidential messages by normalized equivocation rates, i.e., we require

$$\lim_{n\to\infty} \frac{1}{n} I(W_1; \mathbf{Y}_2^n, W_0) = 0 \quad \text{and} \quad \lim_{n\to\infty} \frac{1}{n} I(W_2; \mathbf{Y}_1^n, W_0) = 0 \tag{4.57}$$

We define the capacity region of the enhanced channel in (4.53)-(4.56) arising from this scenario as the convex closure of all achievable rate pairs (R_0, R_1, R_2) and denote it by $\tilde{C}(\mathbf{S})$.

We note that the process of obtaining a new enhanced channel from the original one by means of channel enhancement can be visualized as shown in Figure 4.2 and Figure 4.3. First, we provide an alternative view of the original channel model as depicted in Figure 4.2. In this alternative view, each user is split into two identical users where one of them (user 11 for the first user and user 22 for the second user) gets a confidential message, and the other one (user 10 for the first user and user 20 for the second user) gets the common message and eavesdrops the other confidential message. Second, we enhance the users who are getting the confidential messages,

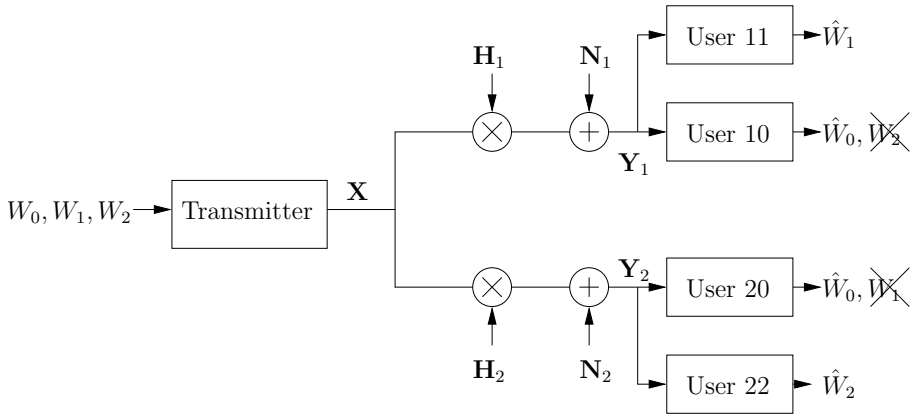

Figure 4.2: An alternative view of the Gaussian MIMO broadcast channel with common and confidential messages.

i.e., user 11 and user 22, to improve their observations as shown in Figure 4.3. This idea of splitting users and then enhancing them is also used in [18]. Since in the enhanced channel, the receivers to which only the common message is sent are identical to the receivers in the original channel in (4.12)-(4.13), and the receivers to which confidential messages are sent have better observations with respect to the receivers in the original channel in (4.12)-(4.13), we have $\mathcal{C}^{\mathrm{AL}}(\mathbf{S}) \subseteq \tilde{C}(\mathbf{S})$. We next introduce an outer bound on $\tilde{C}(\mathbf{S})$ in the following lemma.

Lemma 4.4 *The capacity region of the enhanced channel in (4.53)-(4.56),* $\tilde{C}(\mathbf{S})$*, is contained in the union of rate triples* (R_0, R_1, R_2) *satisfying*

$$R_0 \leq \min\{I(U;\mathbf{Y}_1), I(U;\mathbf{Y}_2)\} \tag{4.58}$$

$$R_1 \leq I(\mathbf{X};\tilde{\mathbf{Y}}|U) - I(\mathbf{X};\mathbf{Y}_2|U) \tag{4.59}$$

$$R_2 \leq I(\mathbf{X};\tilde{\mathbf{Y}}|U) - I(\mathbf{X};\mathbf{Y}_1|U) \tag{4.60}$$

for some $(U, \mathbf{X})$ *such that* $U \to \mathbf{X} \to \tilde{\mathbf{Y}} \to (\mathbf{Y}_1, \mathbf{Y}_2)$ *and* $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}$.

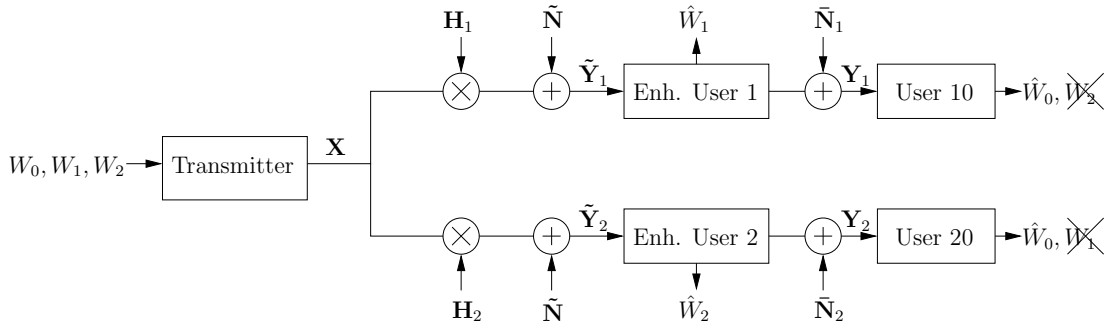

Figure 4.3: The new Gaussian MIMO broadcast channel obtained by channel enhancement.

The proof of this lemma is given in Appendix 4.7.3. We also introduce the following extremal inequality from [5]:

Lemma 4.5 ([5, Corollary 4]) *Let $(U, \mathbf{X})$ be an arbitrarily correlated random vector, where $\mathbf{X}$ has a covariance constraint $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$ and $\mathbf{S} \succ \mathbf{0}$. Let $\tilde{\mathbf{N}}, \mathbf{N}_1, \mathbf{N}_2$ be Gaussian random vectors with covariance matrices $\tilde{\mathbf{\Sigma}}, \mathbf{\Sigma}_1, \mathbf{\Sigma}_2$, respectively. They are independent of $(U, \mathbf{X})$. Furthermore, $\tilde{\mathbf{\Sigma}}, \mathbf{\Sigma}_1, \mathbf{\Sigma}_2$ satisfy $\tilde{\mathbf{\Sigma}} \preceq \mathbf{\Sigma}_j,\ j = 1, 2$. Assume that there exists a covariance matrix $\mathbf{K}^*$ such that $\mathbf{K}^* \preceq \mathbf{S}$ and*

$$\beta(\mathbf{K}^* + \tilde{\mathbf{\Sigma}})^{-1} = \sum_{j=1}^{2} \gamma_j (\mathbf{K}^* + \mathbf{\Sigma}_j)^{-1} + \mathbf{M}_S \tag{4.61}$$

where $\beta \geq 0, \gamma_j \geq 0,\ j = 1, 2$ and $\mathbf{M}_S$ is positive semi-definite matrix such that $(\mathbf{S} - \mathbf{K}^*)\mathbf{M}_S = \mathbf{0}$. Then, for any $(U, \mathbf{X})$, we have

$$\begin{aligned} \beta h(\mathbf{X} + \tilde{\mathbf{N}}|U) - \sum_{j=1}^{2} \gamma_j h(\mathbf{X} + \mathbf{N}_j|U) \leq \frac{\beta}{2} \log|(2\pi e)(\mathbf{K}^* + \tilde{\mathbf{\Sigma}})| \\ - \sum_{j=1}^{2} \frac{\gamma_j}{2} \log|(2\pi e)(\mathbf{K}^* + \mathbf{\Sigma}_j)| \end{aligned} \tag{4.62}$$

We now use this lemma. For that purpose, we note that using the second statement of Lemma 4.3 in (4.46) yields

$$(\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1} = (\mu_0\lambda+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1} + (\mu_0\bar{\lambda}+\mu_1)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_S \tag{4.63}$$

using which in conjunction with Lemma 4.5, we get

$$\begin{aligned}&(\mu_1+\mu_2)h(\tilde{\mathbf{Y}}|U)-(\mu_0\lambda+\mu_2)h(\mathbf{Y}_1|U)-(\mu_0\bar{\lambda}+\mu_1)h(\mathbf{Y}_2|U)\\ &\quad\le \frac{\mu_1+\mu_2}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})|-\frac{\mu_0\lambda+\mu_2}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)|\\ &\qquad-\frac{\mu_0\bar{\lambda}+\mu_1}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)|\end{aligned} \tag{4.64}$$

which will be used subsequently.

We are now ready to complete the converse proof as follows:

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}^{\mathrm{AL}}(\mathbf{S})}\mu_0R_0+\mu_1R_1+\mu_2R_2\le\max_{(R_0,R_1,R_2)\in\tilde{\mathcal{C}}(\mathbf{S})}\mu_0R_0+\mu_1R_1+\mu_2R_2 \tag{4.65}$$

$$\le\max_{\substack{U\to\mathbf{X}\to\tilde{\mathbf{Y}}\to\mathbf{Y}_1,\mathbf{Y}_2\\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}}\mu_0\min\{I(U;\mathbf{Y}_1),I(U;\mathbf{Y}_2)\}+\mu_1\Big[I(\mathbf{X};\tilde{\mathbf{Y}}|U)-I(\mathbf{X};\mathbf{Y}_2|U)\Big]+\mu_2\Big[I(\mathbf{X};\tilde{\mathbf{Y}}|U)-I(\mathbf{X};\mathbf{Y}_1|U)\Big] \tag{4.66}$$

$$\le\max_{\substack{U\to\mathbf{X}\to\tilde{\mathbf{Y}}\to\mathbf{Y}_1,\mathbf{Y}_2\\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}}\mu_0\lambda I(U;\mathbf{Y}_1)+\mu_0\bar{\lambda}I(U;\mathbf{Y}_2)+\mu_1\Big[I(\mathbf{X};\tilde{\mathbf{Y}}|U)-I(\mathbf{X};\mathbf{Y}_2|U)\Big]+\mu_2\Big[I(\mathbf{X};\tilde{\mathbf{Y}}|U)-I(\mathbf{X};\mathbf{Y}_1|U)\Big] \tag{4.67}$$

$$= \max_{\substack{U\to\mathbf{X}\to\tilde{\mathbf{Y}}\to\mathbf{Y}_1,\mathbf{Y}_2 \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} \mu_0\lambda h(\mathbf{Y}_1) + \mu_0\bar{\lambda}h(\mathbf{Y}_2) + (\mu_1+\mu_2)h(\tilde{\mathbf{Y}}|U) - (\mu_0\lambda+\mu_2)h(\mathbf{Y}_1|U)$$

$$- (\mu_0\bar{\lambda}+\mu_1)h(\mathbf{Y}_2|U) - \frac{\mu_1}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_2|} - \frac{\mu_2}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_1|} \tag{4.68}$$

$$\leq \frac{\mu_0\lambda}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_1)| + \frac{\mu_0\bar{\lambda}}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)|$$

$$+ \max_{\substack{U\to\mathbf{X}\to\tilde{\mathbf{Y}}\to\mathbf{Y}_1,\mathbf{Y}_2 \\ E\left[\mathbf{X}\mathbf{X}^\top\right]\preceq\mathbf{S}}} (\mu_1+\mu_2)h(\tilde{\mathbf{Y}}|U) - (\mu_0\lambda+\mu_2)h(\mathbf{Y}_1|U) - (\mu_0\bar{\lambda}+\mu_1)h(\mathbf{Y}_2|U)$$

$$- \frac{\mu_1}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_2|} - \frac{\mu_2}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_1|} \tag{4.69}$$

$$\leq \frac{\mu_0\lambda}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_1)| + \frac{\mu_0\bar{\lambda}}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)|$$

$$+ \frac{(\mu_1+\mu_2)}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})| - \frac{(\mu_0\lambda+\mu_2)}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)|$$

$$- \frac{(\mu_0\bar{\lambda}+\mu_1)}{2}\log|(2\pi e)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)| - \frac{\mu_1}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_2|} - \frac{\mu_2}{2}\log\frac{|\tilde{\mathbf{\Sigma}}|}{|\mathbf{\Sigma}_1|} \tag{4.70}$$

$$= \frac{\mu_0\lambda}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_1|}{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1|} + \frac{\mu_0\bar{\lambda}}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2|}$$

$$+ \frac{\mu_1}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_2|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)\tilde{\mathbf{\Sigma}}|} + \frac{\mu_2}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_1|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)\tilde{\mathbf{\Sigma}}|} \tag{4.71}$$

$$= \mu_0\min\{R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*), R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*)\} + \frac{\mu_1}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_2|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)\tilde{\mathbf{\Sigma}}|}$$

$$+ \frac{\mu_2}{2}\log\frac{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_1|}{|(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)\tilde{\mathbf{\Sigma}}|} \tag{4.72}$$

$$= \mu_0\min\{R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*), R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*)\} + \mu_1 R_1^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) + \mu_2 R_2^{\mathrm{AL}}(\mathbf{K}_2^*) \tag{4.73}$$

where (4.65) comes from the fact that $\mathcal{C}^{\mathrm{AL}}(\mathbf{S}) \subseteq \tilde{\mathcal{C}}(\mathbf{S})$, (4.66) is due to Lemma 4.4, (4.67) results from the fact that $0 \leq \lambda = 1-\bar{\lambda} \leq 1$, (4.69) is due to the maximum entropy theorem, (4.70) comes from (4.64), (4.72) results from

$$\lambda R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) + \bar{\lambda}R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*) = \min\{R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*), R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*,\mathbf{K}_2^*)\} \tag{4.74}$$

and (4.73) will be shown next. We first note the following

$$R_1^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*) = \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_2|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_2|} \tag{4.75}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}|}{|\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_2|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_2|} \tag{4.76}$$

$$= \frac{1}{2}\log\frac{|(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_2|}{|(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_2)\tilde{\mathbf{\Sigma}}|} \tag{4.77}$$

where (4.76) is due to the fourth statement of Lemma 4.3 and (4.77) comes from the third statement of Lemma 4.3. We next note the following identity

$$R_2^{\mathrm{AL}}(\mathbf{K}_2^*) = \frac{1}{2}\log\frac{|\mathbf{K}_2^* + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2^* + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{4.78}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}|}{|\tilde{\mathbf{\Sigma}}|} - \frac{1}{2}\log\frac{|\mathbf{K}_2^* + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{4.79}$$

$$= \frac{1}{2}\log\frac{|(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}})\mathbf{\Sigma}_1|}{|(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)\tilde{\mathbf{\Sigma}}|} \tag{4.80}$$

where (4.79) is due to the third statement of Lemma 4.3, and (4.80) comes from the fourth statement of Lemma 4.3. Identities in (4.77) and (4.80) give (4.73).

Thus, in the view of (4.73), we have shown that

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}^{\mathrm{AL}}(\mathbf{S})} \mu_0 R_0 + \mu_1 R_1 + \mu_2 R_2 = \max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\mathrm{S-DPC-AL}}(\mathbf{S})} \mu_0 R_0 + \mu_1 R_1 + \mu_2 R_2 \tag{4.81}$$

Similarly, we can show the following

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}^{\mathrm{AL}}(\mathbf{S})} \mu_0 R_0 + \mu_1 R_1 + \mu_2 R_2 = \max_{(R_0,R_1,R_2)\in\mathcal{R}_{21}^{\mathrm{S-DPC-AL}}(\mathbf{S})} \mu_0 R_0 + \mu_1 R_1 + \mu_2 R_2 \tag{4.82}$$

completing the converse proof.

4.4 Proof of Theorem 4.1 for the General Case

We now prove Theorem 4.1 for the general channel model in (4.1)-(4.2). Achievability of Theorem 4.1 for the general channel model in (4.1)-(4.2) can be shown as we did for the aligned case in the previous section. In particular, the only difference of the achievability proof for the general channel model in (4.1)-(4.2) from the achievability proof for the aligned case will be the selection of the precoding matrix $\mathbf{A}$, which needs to be chosen as $\mathbf{A} = \mathbf{K}_2\mathbf{H}_2^\top(\mathbf{\Sigma}_2 + \mathbf{H}_2\mathbf{K}_2\mathbf{H}_2^\top)^{-1}\mathbf{H}_2$ in this general case. Thus, in the rest of this section, we consider the converse proof. For that purpose, we follow the analysis in Section V.B of [4] and Section 7.1 of [19] in conjunction with the capacity result obtained for the aligned case in the previous section. To this end, we first note that, following the approaches in Section V.B of [4] and Section 7.1 of [19], it can be shown that a new channel can be constructed from any channel described by (4.1)-(4.2), such that the new channel has the same capacity region as the original one, and in the new channel, both receivers have the same number of antennas as the transmitter, i.e., $r_1 = r_2 = t$. Thus, without loss of generality, we assume that $r_1 = r_2 = t$. We next apply singular-value decomposition

to the channel gain matrices $\mathbf{H}_1, \mathbf{H}_2$ as follows

$$\mathbf{H}_j = \mathbf{U}_j \mathbf{\Lambda}_j \mathbf{V}_j^\top, \quad j = 1, 2 \tag{4.83}$$

where $\mathbf{U}_j, \mathbf{V}_j$ are $t \times t$ orthogonal matrices, and $\mathbf{\Lambda}_j$ is a diagonal matrix. We now define a new Gaussian MIMO broadcast channel as follows

$$\overline{\mathbf{Y}}_1 = \overline{\mathbf{H}}_1 \mathbf{X} + \mathbf{N}_1 \tag{4.84}$$

$$\overline{\mathbf{Y}}_2 = \overline{\mathbf{H}}_2 \mathbf{X} + \mathbf{N}_2 \tag{4.85}$$

where $\overline{\mathbf{H}}_j$ is defined as

$$\overline{\mathbf{H}}_j = \mathbf{U}_j (\mathbf{\Lambda}_j + \alpha \mathbf{I}) \mathbf{V}_j^\top \tag{4.86}$$

for some $\alpha > 0$. We denote the capacity region of the channel defined in (4.84)-(4.85) by $\mathcal{C}_\alpha(\mathbf{S})$, and achievable rate regions for this channel by $\mathcal{R}_{12,\alpha}^{\text{S-DPC}}(\mathbf{S}), \mathcal{R}_{21,\alpha}^{\text{S-DPC}}(\mathbf{S})$. Since $\overline{\mathbf{H}}_1, \overline{\mathbf{H}}_2$ are invertible, the capacity region of the channel in (4.84)-(4.85) is equal to the capacity region of the following aligned channel

$$\overline{\overline{\mathbf{Y}}}_1 = \mathbf{X} + \overline{\mathbf{H}}_1^{-1} \mathbf{N}_1 \tag{4.87}$$

$$\overline{\overline{\mathbf{Y}}}_2 = \mathbf{X} + \overline{\mathbf{H}}_2^{-1} \mathbf{N}_2 \tag{4.88}$$

Thus, using the capacity result for the aligned case, which was proved in the previous section, we get

$$\mathcal{C}_\alpha(\mathbf{S}) = \mathcal{R}_{12,\alpha}^{\text{S-DPC}}(\mathbf{S}) = \mathcal{R}_{21,\alpha}^{\text{S-DPC}}(\mathbf{S}) \tag{4.89}$$

We next show the following inclusion

$$\mathcal{C}(\mathbf{S}) \subseteq \lim_{\alpha \to 0} \mathcal{C}_\alpha(\mathbf{S}) \tag{4.90}$$

To this end, assume that (R_0, R_1, R_2) is achievable in the channel given by (4.1)-(4.2), i.e., $(R_0, R_1, R_2) \in \mathcal{C}(\mathbf{S})$. To prove the inclusion in (4.90), we need to show that $(R_0, R_1, R_2) \in \lim_{\alpha \to 0} \mathcal{C}_\alpha(\mathbf{S})$. To this end, we note the following Markov chains

$$\mathbf{X} \to \overline{\mathbf{Y}}_j \to \mathbf{Y}_j, \quad j = 1, 2 \tag{4.91}$$

which imply that if the message triple (W_0, W_1, W_2) with rates (R_0, R_1, R_2) is transmitted with a vanishingly small probability of error in the original channel given by (4.1)-(4.2), they will be transmitted with a vanishingly small probability of error in the channel given by (4.84)-(4.85) as well. In other words, each receiver in the channel given by (4.84)-(4.85) will decode the messages intended to itself. However, we still need to check the secrecy requirements on the confidential messages W_1, W_2.

We first check the secrecy of the first user's confidential message as follows

$$\lim_{n\to\infty}\frac{1}{n}I(W_1;\overline{\mathbf{Y}}_2^n,W_0,W_2)=\lim_{n\to\infty}\frac{1}{n}I(W_1;\overline{\mathbf{Y}}_2^n,W_0,W_2)-\frac{1}{n}I(W_1;\mathbf{Y}_2^n,W_0,W_2) \tag{4.92}$$

where we used the fact that since $(R_0,R_1,R_2)\in\mathcal{C}(\mathbf{S})$, we have

$$\lim_{n\to\infty}\frac{1}{n}I(W_1;\mathbf{Y}_2^n,W_0,W_2)=0 \tag{4.93}$$

We now bound the term on the right hand-side of as follows (4.92)

$$
\begin{aligned}
& I(W_1; \overline{\mathbf{Y}}_2^n, W_0, W_2) - I(W_1; \mathbf{Y}_2^n, W_0, W_2) \\
& \quad = I(W_1; \overline{\mathbf{Y}}_2^n | W_0, W_2) - I(W_1; \mathbf{Y}_2^n | W_0, W_2) && (4.94) \\
& \quad = I(W_1; \overline{\mathbf{Y}}_2^n | W_0, W_2, \mathbf{Y}_2^n) && (4.95) \\
& \quad = \sum_{i=1}^{n} I(W_1; \overline{\mathbf{Y}}_{2,i} | W_0, W_2, \mathbf{Y}_2^n, \overline{\mathbf{Y}}_2^{i-1}) && (4.96) \\
& \quad \leq \sum_{i=1}^{n} h(\overline{\mathbf{Y}}_{2,i} | \mathbf{Y}_{2,i}) - h(\overline{\mathbf{Y}}_{2,i} | W_0, W_2, \mathbf{Y}_2^n, \overline{\mathbf{Y}}_2^{i-1}, W_1, \mathbf{X}_i) && (4.97) \\
& \quad = \sum_{i=1}^{n} I(\mathbf{X}_i; \overline{\mathbf{Y}}_{2,i} | \mathbf{Y}_{2,i}) && (4.98) \\
& \quad = \sum_{i=1}^{n} I(\mathbf{X}_i; \overline{\mathbf{Y}}_{2,i}) - I(\mathbf{X}_i; \mathbf{Y}_{2,i}) && (4.99) \\
& \quad = \sum_{i=1}^{n} h(\overline{\mathbf{Y}}_{2,i}) - h(\mathbf{Y}_{2,i}) && (4.100) \\
& \quad \leq \sum_{i=1}^{n} \frac{1}{2} \log \frac{\left| \overline{\mathbf{H}}_2 E\left[\mathbf{X}_i \mathbf{X}_i^\top\right] \overline{\mathbf{H}}_2^\top + \mathbf{\Sigma}_2 \right|}{\left| \mathbf{H}_2 E\left[\mathbf{X}_i \mathbf{X}_i^\top\right] \mathbf{H}_2^\top + \mathbf{\Sigma}_2 \right|} && (4.101) \\
& \quad \leq \frac{n}{2} \log \frac{\left| \overline{\mathbf{H}}_2 \left(\sum_{i=1}^{n} \frac{1}{n} E\left[\mathbf{X}_i \mathbf{X}_i^\top\right] \right) \overline{\mathbf{H}}_2^\top + \mathbf{\Sigma}_2 \right|}{\left| \mathbf{H}_2 \left(\sum_{i=1}^{n} \frac{1}{n} E\left[\mathbf{X}_i \mathbf{X}_i^\top\right] \right) \mathbf{H}_2^\top + \mathbf{\Sigma}_2 \right|} && (4.102) \\
& \quad \leq \frac{n}{2} \log \frac{\left| \overline{\mathbf{H}}_2 \mathbf{S} \overline{\mathbf{H}}_2^\top + \mathbf{\Sigma}_2 \right|}{\left| \mathbf{H}_2 \mathbf{S} \mathbf{H}_2^\top + \mathbf{\Sigma}_2 \right|} && (4.103)
\end{aligned}
$$

where (4.95) is due to the Markov chain in (4.91), (4.97) comes from the fact that conditioning cannot increase entropy, (4.98) is due to the fact that the channel is memoryless, (4.99) results from the Markov chain in (4.91), and (4.101) can be shown by using the worst additive noise lemma in [36, 37]. Before showing the steps

in (4.102) and (4.103), we note that the following function

$$\log \frac{\left|\overline{\mathbf{H}}_2 \mathbf{K} \overline{\mathbf{H}}_2^\top + \mathbf{\Sigma}_2\right|}{\left|\mathbf{H}_2 \mathbf{K} \mathbf{H}_2^\top + \mathbf{\Sigma}_2\right|} \tag{4.104}$$

is concave and monotonically increasing in positive semi-definite matrices $\mathbf{K}$, see Lemma 4 in [38]. Thus, (4.102) follows from the Jensen's inequality by noting the concavity of the function in (4.104) and (4.103) comes from the monotonicity of the function in (4.104) and the covariance constraint on the channel input. Hence, using (4.103) in (4.92), we have

$$\lim_{n\to\infty} \frac{1}{n} I(W_1; \overline{\mathbf{Y}}_2^n, W_0, W_2) \leq \frac{1}{2} \log \frac{\left|\overline{\mathbf{H}}_2 \mathbf{S} \overline{\mathbf{H}}_2^\top + \mathbf{\Sigma}_2\right|}{\left|\mathbf{H}_2 \mathbf{S} \mathbf{H}_2^\top + \mathbf{\Sigma}_2\right|} \tag{4.105}$$

where the right hand-side vanishes as $\alpha \to 0$, i.e.,

$$\lim_{\alpha\to 0} \frac{1}{2} \log \frac{\left|\overline{\mathbf{H}}_2 \mathbf{S} \overline{\mathbf{H}}_2^\top + \mathbf{\Sigma}_2\right|}{\left|\mathbf{H}_2 \mathbf{S} \mathbf{H}_2^\top + \mathbf{\Sigma}_2\right|} = 0 \tag{4.106}$$

due to the continuity of $\log|\cdot|$ in positive semi-definite matrices and $\lim_{\alpha\to 0} \overline{\mathbf{H}}_2 = \mathbf{H}_2$. Thus, we have shown that if a confidential message W_1 with rate R_1 can be transmitted in perfect secrecy in the original channel given by (4.1)-(4.2), we have

$$\lim_{\alpha\to 0} \lim_{n\to\infty} \frac{1}{n} I(W_1; \overline{\mathbf{Y}}_2^n, W_0, W_2) = 0 \tag{4.107}$$

Similarly, if a confidential message W_2 with rate R_2 can be transmitted in perfect secrecy in the original channel given by (4.1)-(4.2), we have

$$\lim_{\alpha\to 0}\lim_{n\to\infty}\frac{1}{n}I(W_2;\overline{\mathbf{Y}}_1^n,W_0,W_1)=0 \tag{4.108}$$

These two conditions in (4.107) and (4.108) enable us to conclude that if $(R_0,R_1,R_2)\in\mathcal{C}(\mathbf{S})$, we also have $(R_0,R_1,R_2)\in\lim_{\alpha\to 0}\mathcal{C}_\alpha(\mathbf{S})$. Thus, we have shown that

$$\mathcal{C}(\mathbf{S})\subseteq\lim_{\alpha\to 0}\mathcal{C}_\alpha(\mathbf{S})=\lim_{\alpha\to 0}\mathcal{R}_{12,\alpha}^{\mathrm{S-DPC}}(\mathbf{S})=\lim_{\alpha\to 0}\mathcal{R}_{21,\alpha}^{\mathrm{S-DPC}}(\mathbf{S}) \tag{4.109}$$

where we have

$$\lim_{\alpha\to 0}\mathcal{R}_{12,\alpha}^{\mathrm{S-DPC}}(\mathbf{S})=\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S}) \tag{4.110}$$

$$\lim_{\alpha\to 0}\mathcal{R}_{21,\alpha}^{\mathrm{S-DPC}}(\mathbf{S})=\mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S}) \tag{4.111}$$

due to the continuity of the rate expressions in $\mathcal{R}_{12,\alpha}^{\mathrm{S-DPC}}(\mathbf{S})$ and $\mathcal{R}_{21,\alpha}^{\mathrm{S-DPC}}(\mathbf{S})$ in α. Since $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})$ and $\mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$ are achievable in the channel defined by (4.1)-(4.2), we have

$$\mathcal{C}(\mathbf{S})=\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})=\mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S}) \tag{4.112}$$

in the view of (4.109)-(4.111); completing the proof.

4.5 Connections to the Gaussian MIMO Broadcast Channel with Common and Private Messages

Here, we provide intuitive explanations for the two facts that Theorem 4.1 reveals: i) The achievable rate region does not depend on the encoding order used in S-DPC, i.e., $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S}) = \mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$; and ii) the capacity region of the Gaussian MIMO broadcast channel with common and confidential messages can be completely characterized, although the capacity region of the its non-confidential counterpart, i.e., the Gaussian MIMO broadcast channel with common and private messages, is not known completely.

In the Gaussian MIMO broadcast channel with common and private messages, there are again three messages W_0, W_1, W_2 with rates R_0, R_1, R_2, respectively, such that W_0 is again sent to both users, W_1 (resp. W_2) is again directed to only the first (resp. second) user, however, there are no secrecy constraints on W_1, W_2. The capacity region of the Gaussian MIMO broadcast channel with common and private messages will be denoted by $\mathcal{C}^{\mathrm{NS}}(\mathbf{S})$. The achievable rate region for the Gaussian MIMO broadcast channel with common and private messages that can be obtained by using DPC will be denoted by $\mathcal{R}_{12}^{\mathrm{NS-DPC}}(\mathbf{S}), \mathcal{R}_{21}^{\mathrm{NS-DPC}}(\mathbf{S})$ (depending on the encoding order), where $\mathcal{R}_{12}^{\mathrm{NS-DPC}}(\mathbf{S})$ is given by the rate triples (R_0, R_1, R_2) satisfying

$$R_0 \leq \min\{R_{01}^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2), R_{02}^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2)\} \tag{4.113}$$

$$R_1 \leq R_1^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2) \tag{4.114}$$

$$R_2 \leq R_2^{\mathrm{NS}}(\mathbf{K}_2) \tag{4.115}$$

for some positive semi-definite matrices $\mathbf{K}_1, \mathbf{K}_2$ such that $\mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$, and $\{R_{0j}^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2)\}_{j=1}^{2}$,

$R_1^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2), R_2^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2)$ are defined as

$$R_{0j}^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_j|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_j|}, \quad j = 1, 2 \tag{4.116}$$

$$R_1^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_1|}{|\mathbf{K}_2 + \mathbf{\Sigma}_1|} \tag{4.117}$$

$$R_2^{\mathrm{NS}}(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} \tag{4.118}$$

Moreover, $\mathcal{R}_{21}^{\mathrm{NS-DPC}}(\mathbf{S})$ can be obtained from $\mathcal{R}_{12}^{\mathrm{NS-DPC}}(\mathbf{S})$ by swapping the subscripts 2 and 1. We now state a result of [10] on the capacity region of the Gaussian MIMO broadcast channel with common and private messages: For a given common message rate R_0, the private message sum rate capacity, i.e., $R_1 + R_2$, is achieved by both $\mathcal{R}_{12}^{\mathrm{NS}}(\mathbf{S})$ and $\mathcal{R}_{21}^{\mathrm{NS}}(\mathbf{S})$. This result can also be stated as follows

$$\max_{(R_0,R_1,R_2)\in\mathcal{C}^{\mathrm{NS}}(\mathbf{S})} \mu_0' R_0 + \mu_1' R_1 + \mu_2' R_2 = \max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\mathrm{NS-DPC}}(\mathbf{S})} \mu_0' R_0 + \mu_1' R_1 + \mu_2' R_2 \tag{4.119}$$

$$= \max_{(R_0,R_1,R_2)\in\mathcal{R}_{21}^{\mathrm{NS-DPC}}(\mathbf{S})} \mu_0' R_0 + \mu_1' R_1 + \mu_2' R_2 \tag{4.120}$$

for $\mu_1' = \mu_2' = \mu'$. This result is crucial to understand the aforementioned two points suggested by Theorem 4.1, which will be explained next using (4.119)-(4.120).

In the proof of Theorem 4.1, first, we characterize the boundary of $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})$ by finding the properties of the covariance matrices that achieve the boundary of

$\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})$, see Lemma 4.2. According to Lemma 4.2, the boundary of $\mathcal{R}_{12}^{\text{S-DPC}}(\mathbf{S})$ can be achieved by using the covariance matrices $\mathbf{K}_1^*, \mathbf{K}_2^*$ satisfying

$$(\mu_1+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1=(\mu_0\lambda+\mu_2)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1} + (\mu_0\bar{\lambda}+\mu_1)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_S \tag{4.121}$$

$$(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_2=(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1 \tag{4.122}$$

On the other hand, using these covariance matrices, we can also achieve the boundary points of $\mathcal{R}_{12}^{\text{NS-DPC}}(\mathbf{S})$, which are actually on the boundary of the capacity region $\mathcal{C}^{\text{NS}}(\mathbf{S})$ as well, and are the private message sum rate capacity points for a given common message rate. To see this point, we define $\mu'=\mu_1+\mu_2, \mu_0'=\mu_0+\mu_1+\mu_2$ and $\gamma=\frac{\mu_0\lambda+\mu_2}{\mu_0+\mu_1+\mu_2}$, i.e., $\bar{\gamma}=1-\gamma=\frac{\mu_0\bar{\lambda}+\mu_1}{\mu_0+\mu_1+\mu_2}$. Thus, the conditions in (4.121)-(4.122) can be written as

$$\mu'(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1=\mu_0'\gamma(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mu_0'\bar{\gamma}(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1} + \mathbf{M}_S \tag{4.123}$$

$$\mu'(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_2=\mu'(\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1 \tag{4.124}$$

which are the necessary conditions that the following problem needs to satisfy

$$\max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\text{NS-DPC}}(\mathbf{S})} \mu_0'R_0+\mu'(R_1+R_2) \tag{4.125}$$

On the other hand, due to (4.119)-(4.120), we know that the solution of (4.125) gives us the private message sum rate capacity for a given common message rate, i.e., the points that achieve the maximum in (4.125) are on the boundary of the capacity region $\mathcal{C}^{\mathrm{NS}}(\mathbf{S})$. Furthermore, the maximum value in (4.125) can also be achieved by using the other possible encoding order, i.e.,

$$\max_{(R_0,R_1,R_2)\in\mathcal{R}_{12}^{\mathrm{NS-DPC}}(\mathbf{S})} \mu_0' R_0 + \mu'(R_1+R_2) = \max_{(R_0,R_1,R_2)\in\mathcal{R}_{21}^{\mathrm{NS-DPC}}(\mathbf{S})} \mu_0' R_0 + \mu'(R_1+R_2) \tag{4.126}$$

Thus, this discussion reveals that there is a one-to-one correspondence between any rate triple on the boundary of $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})$ and the private message sum rate capacity points on $\mathcal{C}^{\mathrm{NS}}(\mathbf{S})$. Hence, the boundary of $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})$, similarly $\mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$, can be constructed by considering the private message sum rate capacity points on $\mathcal{C}^{\mathrm{NS}}(\mathbf{S})$. This connection between the private message sum rate capacity points and the boundaries of $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S})$, $\mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$ intuitively explains the two facts suggested by Theorem 4.1: i) The achievable rate region for the Gaussian MIMO broadcast channel with common and confidential messages is invariant with respect to the encoding order, i.e., $\mathcal{R}_{12}^{\mathrm{S-DPC}}(\mathbf{S}) = \mathcal{R}_{21}^{\mathrm{S-DPC}}(\mathbf{S})$ because the boundaries of these two regions correspond to those points on the DPC region for the Gaussian MIMO broadcast channel with common and private messages, for which encoding order does not matter either; and ii) we can obtain the entire capacity region of the Gaussian MIMO broadcast channel with common and confidential messages, although the capacity region of its non-confidential counterpart is not known completely. The

reason is that the boundary of the capacity region of the Gaussian MIMO broadcast channel with common and confidential messages comes from those points on the boundary of the DPC region of its non-confidential counterpart, which are known to be tight, i.e., which are known to be on the boundary of the capacity region of the Gaussian MIMO broadcast channel with common and private messages.

4.6 Conclusions

In this chapter, we study the Gaussian MIMO broadcast channel with common and confidential messages, and obtain its entire capacity region. We show that a combination of superposition coding and the S-DPC scheme proposed in [8] is capacity-achieving. We provide the converse proof by using channel enhancement [4] and an extremal inequality from [5]. We also uncover the connections between the Gaussian MIMO broadcast channel with common and confidential messages and its non-confidential counterpart, i.e., the Gaussian MIMO broadcast channel with common and private messages, to provide further insight into the capacity result we obtained.

4.7 Appendix

4.7.1 Proof of Lemma 4.2

Since the program in (4.45) is not necessarily convex, the KKT conditions are necessary but not sufficient. We first rewrite the program in (4.45) as follows

$$\begin{aligned} \max_{\substack{\mathbf{0} \preceq \mathbf{K}_j,\ j=1,2 \\ \mathbf{K}_1+\mathbf{K}_2 \preceq \mathbf{S} \\ a}} \quad & \mu_0 a + \mu_1 R_1^{\mathrm{AL}}(\mathbf{K}_1, \mathbf{K}_2) + \mu_2 R_2^{\mathrm{AL}}(\mathbf{K}_2) \\ \text{s.t.} \quad & R_{01}^{\mathrm{AL}}(\mathbf{K}_1, \mathbf{K}_2) \geq a \\ & R_{02}^{\mathrm{AL}}(\mathbf{K}_1, \mathbf{K}_2) \geq a \end{aligned} \tag{4.127}$$

where we introduce an additional variable a. Thus, the optimization in (4.127) is over three variables $a, \mathbf{K}_1, \mathbf{K}_2$. The Lagrangian of (4.127) is given by

$$\begin{aligned} \mathcal{L} = \mu_0 a + \mu_1 R_1^{\mathrm{AL}}(\mathbf{K}_1, \mathbf{K}_2) + \mu_2 R_2^{\mathrm{AL}}(\mathbf{K}_2) + \mu_0 \sum_{j=1}^{2} \lambda_j (R_{0j}^{\mathrm{AL}}(\mathbf{K}_1, \mathbf{K}_2) - a) + \mathrm{tr}(\mathbf{K}_1 \mathbf{M}_1) \\ + \mathrm{tr}(\mathbf{K}_2 \mathbf{M}_2) + \mathrm{tr}((\mathbf{S} - \mathbf{K}_1 - \mathbf{K}_2)\mathbf{M}_S) \end{aligned} \tag{4.128}$$

where $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_S$ are positive semi-definite matrices and $\lambda_j \geq 0,\ j = 1, 2$. Let $(a^*, \mathbf{K}_1^*, \mathbf{K}_2^*)$ be the maximizer for (4.127). The necessary KKT conditions that they

need to satisfy are given as follows

$$\frac{\partial \mathcal{L}}{\partial a} \mid_{a=a^*} = 0 \tag{4.129}$$

$$\nabla_{\mathbf{K}_1} \mathcal{L} \mid_{\mathbf{K}_1=\mathbf{K}_1^*} = \mathbf{0} \tag{4.130}$$

$$\nabla_{\mathbf{K}_2} \mathcal{L} \mid_{\mathbf{K}_2=\mathbf{K}_2^*} = \mathbf{0} \tag{4.131}$$

$$\mathrm{tr}(\mathbf{K}_1^* \mathbf{M}_1) = 0 \tag{4.132}$$

$$\mathrm{tr}(\mathbf{K}_2^* \mathbf{M}_2) = 0 \tag{4.133}$$

$$\mathrm{tr}((\mathbf{S} - \mathbf{K}_1^* - \mathbf{K}_2^*)\mathbf{M}_S) = 0 \tag{4.134}$$

$$\lambda_j (R_{0j}^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*) - a^*) = 0, \quad j = 1, 2 \tag{4.135}$$

The first KKT condition in (4.129) implies $\lambda_1 + \lambda_2 = 1$. We define $\lambda = \lambda_1$ and consequently $\bar{\lambda} = 1 - \lambda = \lambda_2$. The second KKT condition in (4.130) implies

$$\mu_1(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 = \mu_0 \lambda (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + (\mu_0 \bar{\lambda} + \mu_1)(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \mathbf{M}_S \tag{4.136}$$

Adding $\mu_2(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}$ to both sides yields (4.50). Subtracting (4.130) from (4.131) yields (4.47). Since $\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA})$ and $\mathrm{tr}(\mathbf{AB}) \geq 0$ for $\mathbf{A} \succeq \mathbf{0}, \mathbf{B} \succeq \mathbf{0}$, (4.132)-(4.134) imply (4.48)-(4.50). Furthermore, (4.135) states the conditions if $R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*) > R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*)$, $\lambda = 0$, if $R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*) < R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*)$, $\lambda = 1$, and if $R_{01}^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*) = R_{02}^{\mathrm{AL}}(\mathbf{K}_1^*, \mathbf{K}_2^*)$, λ is arbitrary, i.e., $0 < \lambda < 1$.

4.7.2 Proof of Lemma 4.3

We first note the following identities

$$(\mu_1+\mu_2)(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}=(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\mathbf{M}_2 \tag{4.137}$$

$$(\mu_1+\mu_2)(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}})^{-1}=(\mu_1+\mu_2)(\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1 \tag{4.138}$$

where (4.137) is the definition of the new noise covariance matrix in (4.52) and (4.138) comes from plugging (4.52) in (4.47). Using the fact that for $\mathbf{A}\succ\mathbf{0}$, $\mathbf{B}\succ\mathbf{0}$, if $\mathbf{A}\preceq\mathbf{B}$, then $\mathbf{A}^{-1}\succeq\mathbf{B}^{-1}$ in (4.137)-(4.138) yields the second statement of the lemma.

Now, we prove the first statement of the lemma as follows

$$\tilde{\mathbf{\Sigma}}=\left[(\mathbf{K}_2^*+\mathbf{\Sigma}_2)^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]^{-1}-\mathbf{K}_2^* \tag{4.139}$$

$$=\left[\mathbf{I}+\frac{1}{\mu_1+\mu_2}(\mathbf{K}_2^*+\mathbf{\Sigma}_2)\mathbf{M}_2\right]^{-1}(\mathbf{K}_2^*+\mathbf{\Sigma}_2)-\mathbf{K}_2^* \tag{4.140}$$

$$=\left[\mathbf{I}+\frac{1}{\mu_1+\mu_2}\mathbf{\Sigma}_2\mathbf{M}_2\right]^{-1}(\mathbf{K}_2^*+\mathbf{\Sigma}_2)-\mathbf{K}_2^* \tag{4.141}$$

$$=\left[\mathbf{\Sigma}_2^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]^{-1}\mathbf{\Sigma}_2^{-1}(\mathbf{K}_2^*+\mathbf{\Sigma}_2)-\mathbf{K}_2^* \tag{4.142}$$

$$=\left[\mathbf{\Sigma}_2^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]^{-1}+\left[\mathbf{\Sigma}_2^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]^{-1}\mathbf{\Sigma}_2^{-1}\mathbf{K}_2^*-\mathbf{K}_2^* \tag{4.143}$$

$$=\left[\mathbf{\Sigma}_2^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]^{-1}+\left[\mathbf{\Sigma}_2^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]^{-1}\left[\mathbf{\Sigma}_2^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]\mathbf{K}_2^*$$
$$-\mathbf{K}_2^* \tag{4.144}$$

$$=\left[\mathbf{\Sigma}_2^{-1}+\frac{1}{\mu_1+\mu_2}\mathbf{M}_2\right]^{-1} \tag{4.145}$$

$$\succ\mathbf{0} \tag{4.146}$$

where (4.139) is due to (4.137), and (4.141) and (4.144) follow from (4.49).

We next show the third statement of the lemma as follows

$$\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}} = \mathbf{K}_1^* + \left[(\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1} \tag{4.147}$$

$$= \mathbf{K}_1^* + \left[\mathbf{I} + \frac{1}{\mu_1 + \mu_2}(\mathbf{K}_2^* + \mathbf{\Sigma}_1)\mathbf{M}_1\right]^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{4.148}$$

$$= \mathbf{K}_1^* + \left[\mathbf{I} + \frac{1}{\mu_1 + \mu_2}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)\mathbf{M}_1\right]^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{4.149}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{4.150}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} \times (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1 - \mathbf{K}_1^*) \tag{4.151}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}\mathbf{K}_1^* \tag{4.152}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1}\left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]\mathbf{K}_1^* \tag{4.153}$$

$$= \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]^{-1} \tag{4.154}$$

where (4.147) is due to (4.138), (4.149) and (4.153) come from (4.48).

We now show the fourth statement of the lemma as follows

$$(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}})^{-1}\tilde{\mathbf{\Sigma}} = \mathbf{I} - (\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}})^{-1}\mathbf{K}_2^* \tag{4.155}$$

$$= \mathbf{I} - \left[(\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_2\right]\mathbf{K}_2^* \tag{4.156}$$

$$= \mathbf{I} - (\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1}\mathbf{K}_2^* \tag{4.157}$$

$$= (\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1}\mathbf{\Sigma}_2 \tag{4.158}$$

where (4.156) comes from (4.137), and (4.157) is due to (4.49).

We finally show the last, i.e., fifth, statement of the lemma as follows

$$(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}})^{-1}(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}) = \mathbf{I} - (\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}})^{-1}\mathbf{K}_1^* \tag{4.159}$$

$$= \mathbf{I} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\mu_1 + \mu_2}\mathbf{M}_1\right]\mathbf{K}_1^* \tag{4.160}$$

$$= \mathbf{I} - (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}\mathbf{K}_1^* \tag{4.161}$$

$$= (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{4.162}$$

where (4.160) comes from the second statement of this lemma, and (4.161) is due to (4.48).

4.7.3 Proof of Lemma 4.4

We prove this lemma for a discrete memoryless broadcast channel with a transition probability $p(\tilde{y}_1, \tilde{y}_2, y_1, y_2|x)$ which satisfies $p(\tilde{y}_1|x) = p(\tilde{y}_2|x) = p(\tilde{y}|x)$ and

$$X \to \tilde{Y} \to (Y_1, Y_2) \tag{4.163}$$

Consequently, Lemma 4.4 can be concluded from the proof for this discrete memoryless broadcast channel. We note that if (R_0, R_1, R_2) is achievable, we need to have ϵ_n, γ_n such that both ϵ_n and γ_n vanish as $n \to \infty$, and

$$H(W_0|Y_j^n) \leq n\epsilon_n, \quad j = 1, 2 \tag{4.164}$$

$$H(W_j|\tilde{Y}^n, W_0) \leq n\epsilon_n, \quad j = 1, 2 \tag{4.165}$$

$$I(W_1; Y_2^n, W_0) \leq n\gamma_n \tag{4.166}$$

$$I(W_2; Y_1^n, W_0) \leq n\gamma_n \tag{4.167}$$

where (4.164)-(4.165) are due to Fano's lemma, and (4.166)-(4.167) comes from the perfect secrecy conditions in (4.57). We define the following auxiliary random variables

$$U_i = W_0\tilde{Y}^{i-1}, \quad i = 1, \ldots, n \tag{4.168}$$

which satisfy the following Markov chains for all i,

$$U_i \to X_i \to \tilde{Y}_i \to (Y_{1i}, Y_{2i}) \tag{4.169}$$

since the channel is memoryless, and degraded, i.e., satisfies the Markov chain in (4.163).

We first bound the common message rate R_0 as follows

$$\begin{aligned} nR_0 &= H(W_0) && (4.170)\\ &\leq I(W_0; Y_1^n) + n\epsilon_n && (4.171)\\ &= \sum_{i=1}^{n} I(W_0; Y_{1i}|Y_1^{i-1}) + n\epsilon_n && (4.172)\\ &\leq \sum_{i=1}^{n} I(W_0, \tilde{Y}^{i-1}, Y_1^{i-1}; Y_{1i}) + n\epsilon_n && (4.173)\\ &= \sum_{i=1}^{n} I(W_0, \tilde{Y}^{i-1}; Y_{1i}) + n\epsilon_n && (4.174)\\ &= \sum_{i=1}^{n} I(U_i; Y_{1i}) + n\epsilon_n && (4.175) \end{aligned}$$

where (4.174) comes from the Markov chain

$$Y_1^{i-1} \to \tilde{Y}^{i-1} \to (W_0, Y_{1i}) \tag{4.176}$$

which is a consequence of the fact that the channel is degraded, i.e., satisfies the

Markov chain in (4.163). Similarly, we can get

$$nR_0 \leq \sum_{i=1}^{n} I(U_i; Y_{2i}) + n\epsilon_n \tag{4.177}$$

We next bound the confidential message rate of the enhanced first user, i.e., R_1, as follows

$$\begin{aligned}
nR_1 &= H(W_1|W_0) && (4.178)\\
&\leq I(W_1; \tilde{Y}^n|W_0) - I(W_1; Y_2^n|W_0) + n(\epsilon_n + \gamma_n) && (4.179)\\
&\leq I(W_1; \tilde{Y}^n|W_0, Y_2^n) + n(\epsilon_n + \gamma_n) && (4.180)\\
&= \sum_{i=1}^{n} I(W_1; \tilde{Y}_i|W_0, Y_2^n, \tilde{Y}^{i-1}) + n(\epsilon_n + \gamma_n) && (4.181)\\
&= \sum_{i=1}^{n} I(W_1; \tilde{Y}_i|W_0, Y_{2i}^n, \tilde{Y}^{i-1}) + n(\epsilon_n + \gamma_n) && (4.182)\\
&\leq \sum_{i=1}^{n} I(W_1, X_i; \tilde{Y}_i|W_0, Y_{2i}^n, \tilde{Y}^{i-1}) + n(\epsilon_n + \gamma_n) && (4.183)\\
&= \sum_{i=1}^{n} I(X_i; \tilde{Y}_i|W_0, Y_{2i}^n, \tilde{Y}^{i-1}) + n(\epsilon_n + \gamma_n) && (4.184)\\
&= \sum_{i=1}^{n} H(\tilde{Y}_i|W_0, Y_{2i}^n, \tilde{Y}^{i-1}) - H(\tilde{Y}_i|W_0, Y_{2i}^n, \tilde{Y}^{i-1}, X_i) + n(\epsilon_n + \gamma_n) && (4.185)\\
&\leq \sum_{i=1}^{n} H(\tilde{Y}_i|W_0, Y_{2i}, \tilde{Y}^{i-1}) - H(\tilde{Y}_i|W_0, Y_{2i}^n, \tilde{Y}^{i-1}, X_i) + n(\epsilon_n + \gamma_n) && (4.186)\\
&= \sum_{i=1}^{n} H(\tilde{Y}_i|W_0, Y_{2i}, \tilde{Y}^{i-1}) - H(\tilde{Y}_i|W_0, Y_{2i}, \tilde{Y}^{i-1}, X_i) + n(\epsilon_n + \gamma_n) && (4.187)\\
&= \sum_{i=1}^{n} I(X_i; \tilde{Y}_i|U_i, Y_{2i}) + n(\epsilon_n + \gamma_n) && (4.188)\\
&= \sum_{i=1}^{n} I(X_i; \tilde{Y}_i|U_i) - I(X_i; Y_{2i}|U_i) + n(\epsilon_n + \gamma_n) && (4.189)
\end{aligned}$$

where (4.182) comes from the Markov chain

$$W_0, W_1, Y_{2i}^n \rightarrow \tilde{Y}^{i-1} \rightarrow Y_2^{i-1} \tag{4.190}$$

which is a consequence of the fact that the channel is degraded, i.e., satisfies the Markov chain in (4.163), (4.184) comes from the Markov chain

$$W_0, W_1, \tilde{Y}^{i-1}, Y_{2(i+1)}^n \rightarrow X_i \rightarrow \tilde{Y}_i, Y_{2i} \tag{4.191}$$

which is due to the fact that the channel is memoryless, (4.186) comes from the fact that conditioning cannot increase entropy, (4.187) results from the Markov chain in (4.191), and (4.189) stems from the Markov chain in (4.169). Similarly, we can get the following bound on the confidential message rate of the enhanced second user R_2

$$nR_2 \leq \sum_{i=1}^{n} I(X_i; \tilde{Y}_i|U_i) - I(X_i; Y_{2,i}|U_i) + n(\epsilon_n + \gamma_n) \tag{4.192}$$

The bounds in (4.175), (4.177), (4.189) and (4.192) can be single-letterized yielding the following bounds

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} \tag{4.193}$$

$$R_1 \leq I(X; \tilde{Y}|U) - I(X; Y_2|U) \tag{4.194}$$

$$R_2 \leq I(X; \tilde{Y}|U) - I(X; Y_1|U) \tag{4.195}$$

from which, Lemma 4.4 can be concluded.

Chapter 5

Secrecy Capacity Region of the Gaussian MIMO Multi-receiver Wiretap Channel

5.1 Introduction

In this chapter, we study the Gaussian MIMO multi-receiver wiretap channel where the transmitter wants to have confidential communication with an arbitrary number of legitimate users in the presence of an external eavesdropper. We obtain the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel for the most general case. Toward that end, we first consider the Gaussian scalar multi-receiver wiretap channel, and find its secrecy capacity region. There are two reasons for the presentation of the scalar case separately. The first one is to show that, existing converse techniques for the Gaussian scalar broadcast channel, i.e., the converse proofs of Bergmans [39] and El Gamal [40], cannot be extended in a straightforward manner to provide a converse proof for the Gaussian scalar multi-receiver wiretap channel. We explicitly show that the main ingredient of these two converses in [39, 40], which is the entropy-power inequality [41–43][1], is insufficient to conclude a converse for the secrecy capacity region. The second reason for the

[1]Throughout this chapter, the entropy-power inequality refers to the original form of this inequality that was proposed by Shannon [41], but not its subsequent variants such as Costa's entropy-power inequality [44]. Indeed, the shortcoming of the entropy-power inequality [41–43] to prove the secrecy capacity region of the Gaussian scalar multi-receiver wiretap channel can be alleviated by using Costa's entropy-power inequality as shown in [45].

separate presentation is to present the main ingredients of the technique that we will use to provide a converse proof for the general MIMO channel in an isolated manner in a simpler context. We provide two converse proofs for the Gaussian scalar multi-receiver wiretap channel. The first one uses the connection between the minimum-mean-square-error (MMSE) and the mutual information along with the properties of the MMSE [46, 47]. In additive Gaussian channels, the Fisher information, another important quantity in estimation theory, and the MMSE have a one-to-one relationship in the sense that one of them determines the other one, and vice versa [48]. Thus, the converse proof relying on the MMSE has a counterpart which replaces the MMSE with the Fisher information in the corresponding converse proof. Hence, the second converse uses the connection between the Fisher information and the differential entropy via the de Bruijn identity [41–43] along with the properties of the Fisher information. This reveals that the Fisher information matrix or equivalently the MMSE matrix should play an important role in the converse proof of the MIMO case.

Keeping this motivation in mind, we consider the Gaussian MIMO multi-receiver wiretap channel next. Instead of directly tackling the most general case in which each receiver has an arbitrary number of antennas and an arbitrary noise covariance matrix, we first consider two sub-classes of MIMO channels. In the first sub-class, all receivers have the same number of antennas and the noise covariance matrices exhibit a positive semi-definite order, which implies the degradedness of these channels. Hereafter, we call this channel model the *degraded Gaussian MIMO multi-receiver wiretap channel*. In the second sub-class, although all receivers still

have the same number of antennas as in the degraded case, the noise covariance matrices do not have to satisfy any positive semi-definite order. Hereafter, we call this channel model the *aligned Gaussian MIMO multi-receiver wiretap channel*. Our approach will be to first find the secrecy capacity region of the degraded case, then to generalize this result to the aligned case by using the *channel enhancement* technique [4]. Once we obtain the secrecy capacity region of the aligned case, we use this result to find the secrecy capacity region of the most general case by some limiting arguments as in [4, 21].

The main contribution and the novelty of our work in this chapter is the way we prove the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel, since the remaining steps from then on are mainly adaptations of the existing proof techniques [4, 21] to an eavesdropper and/or multi-user setting. Moreover, the technique we use to obtain the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel can be useful to evaluate the single-letter descriptions of other (vector) Gaussian models. In particular, using the same technique, we are able to provide an alternative proof for the capacity region of the degraded Gaussian MIMO broadcast channel and an outer bound for the rate-distortion region of the vector Gaussian CEO problem. We provide these applications of our new proof technique in Appendices 5.9.7 and 5.9.8.

The single-user version of the Gaussian MIMO multi-receiver wiretap channel we study here, i.e., the Gaussian MIMO wiretap channel, was solved by [15, 16] for the general case and by [17] for the 2-2-1 case. Their common proof technique was to derive a Sato-type outer bound on the secrecy capacity, and then to tighten this

outer bound by searching over all possible correlation structures among the noise vectors of the legitimate user and the eavesdropper. Later, [21] gave an alternative, simpler proof by using the channel enhancement technique.

5.2 Degraded Multi-receiver Wiretap Channels

In this section, we revisit the degraded multi-receiver wiretap channel (see Figure 5.1) that we consider in Chapter 3, since it will be needed in the proof of the secrecy capacity region for the degraded Gaussian MIMO multi-receiver wiretap channel. The general multi-receiver wiretap channel consists of one transmitter with an input alphabet $\mathcal{X}$, K legitimate receivers with output alphabets $\mathcal{Y}_k$, $k = 1, \ldots, K$, and an eavesdropper with output alphabet $\mathcal{Z}$. The transmitter sends a confidential message to each user, say $w_k \in \mathcal{W}_k$ to the kth user, and all messages are to be kept secret from the eavesdropper. The channel is memoryless with a transition probability $p(y_1, y_2, \ldots, y_K, z|x)$.

A $(2^{nR_1}, \ldots, 2^{nR_K}, n)$ code for this channel consists of K message sets, $\mathcal{W}_k = \{1, \ldots, 2^{nR_k}\}$, $k = 1, \ldots, K$, an encoder $f : \mathcal{W}_1 \times \ldots \times \mathcal{W}_K \to \mathcal{X}^n$, K decoders, one at each legitimate receiver, $g_k : \mathcal{Y}_k \to \mathcal{W}_k$, $k = 1, \ldots, K$. The probability of error is defined as $P_e^n = \max_{k=1,\ldots,K} \Pr\left[g_k(Y_k^n) \neq W_k\right]$, where W_k is a uniformly distributed random variable in $\mathcal{W}_k$, $k = 1, \ldots, K$. A rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if there exists a code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z^n) \geq \sum_{k\in\mathcal{S}(W)} R_k, \quad \forall\, \mathcal{S}(W) \tag{5.1}$$

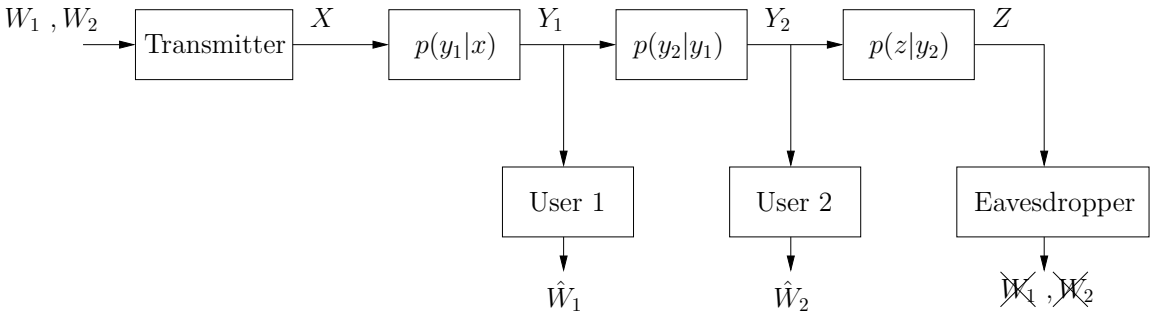

Figure 5.1: Degraded multi-receiver wiretap channel for $K = 2$.

where $\mathcal{S}(W)$ denotes any subset of $\{W_1, \ldots, W_K\}$. The degraded multi-receiver wiretap channel exhibits the following Markov chain

$$X \to Y_1 \to \ldots \to Y_K \to Z \tag{5.2}$$

for which, we already obtain the secrecy capacity region in Chapter 3.

Theorem 5.1 (Chapter 3, Corollary 3.1) *The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of the rate tuples* $(R_1, \ldots, R_K)$ *satisfying*[2]

$$R_k \leq I(U_k; Y_k|U_{k+1}, Z), \quad k = 1, \ldots, K \tag{5.3}$$

where $U_1 = X, U_{K+1} = \emptyset$*, and the union is over all probability distributions of the*

[2]Although in Corollary 3.1 of Chapter 3, this secrecy capacity region is expressed in a different form, the equivalence of the two expressions can be shown.

form

$$p(u_K)p(u_{K-1}|u_K)\dots p(u_2|u_3)p(x|u_2) \tag{5.4}$$

We remark here that since the channel is degraded, i.e., we have the Markov chain in (5.2), the capacity expressions in (5.3) are equivalent to

$$R_k \leq I(U_k;Y_k|U_{k+1}) - I(U_k;Z|U_{k+1}),\ \ k=1,\dots,K \tag{5.5}$$

We will use this equivalent expression frequently hereafter. For the case of two users and one eavesdropper, i.e., $K=2$, the expressions in (5.5) reduce to:

$$R_1 \leq I(X;Y_1|U_2) - I(X;Z|U_2) \tag{5.6}$$

$$R_2 \leq I(U_2;Y_2) - I(U_2;Z) \tag{5.7}$$

Finding the secrecy capacity region of the two-user degraded multi-receiver wiretap channel is tantamount to finding the optimal joint distributions of (X,U_2) that trace the boundary of the secrecy capacity region given in (5.6)-(5.7). For the K-user degraded multi-receiver wiretap channel, we need to find the optimal joint distributions of $(X,U_2,\dots,U_K)$ in the form given in (5.4) that trace the boundary of the region expressed in (5.3).

5.3 Gaussian MIMO Multi-receiver Wiretap Channel

5.3.1 Degraded Gaussian MIMO Multi-receiver Wiretap Channel

In this chapter, we first consider the degraded Gaussian MIMO multi-receiver wiretap channel, see Figure 5.2, which is defined through

$$\mathbf{Y}_k = \mathbf{X} + \mathbf{N}_k, \quad k = 1, \ldots, K \tag{5.8}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{5.9}$$

where the channel input $\mathbf{X}$ is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{5.10}$$

where $\mathbf{S} \succ 0$, and $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ are zero-mean Gaussian random vectors with covariance matrices $\{\mathbf{\Sigma}_k\}_{k=1}^K, \mathbf{\Sigma}_Z$ which satisfy the following ordering

$$\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \ldots \preceq \mathbf{\Sigma}_K \preceq \mathbf{\Sigma}_Z \tag{5.11}$$

In a multi-receiver wiretap channel, since the capacity-equivocation rate region depends only on the conditional marginal distributions of the transmitter-receiver links, but not on the entire joint distribution of the channel, the correlations among $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ have no consequence on the capacity-equivocation rate region. Thus, without changing the corresponding secrecy capacity region, we can adjust the correlation structure among these noise vectors to ensure that they satisfy the following

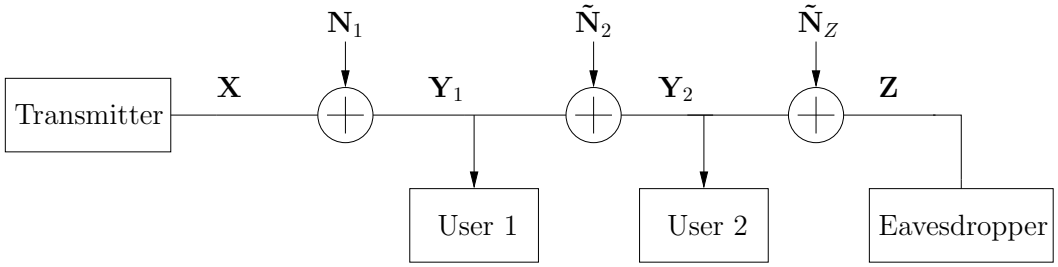

Figure 5.2: Degraded Gaussian MIMO multi-receiver wiretap channel for $K = 2$.

Markov chain

$$\mathbf{X} \to \mathbf{Y}_1 \to \ldots \to \mathbf{Y}_K \to \mathbf{Z} \tag{5.12}$$

which is always possible because of our assumption regarding the covariance matrices in (5.11). Moreover, the Markov chain in (5.12) implies that any Gaussian MIMO multi-receiver wiretap channel satisfying the semi-definite ordering in (5.11) can be treated as a degraded multi-receiver wiretap channel, hence Theorem 5.1 gives its capacity region. Hereafter, we will assume that the degraded Gaussian MIMO wiretap channel satisfies the Markov chain in (5.12).

In Section 5.5, we obtain the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel, which is stated in the following theorem.

Theorem 5.2 *The secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is given by the union of the rate tuples $R_1, \ldots, R_K$ satisfying*

$$R_k \leq \frac{1}{2} \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_k \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k \right|} - \frac{1}{2} \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}, \quad k = 1, \ldots, K \tag{5.13}$$

where the union is over all positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^K$ *that satisfy*

$$\sum_{i=1}^{K} \mathbf{K}_i = \mathbf{S} \tag{5.14}$$

We prove Theorem 5.2 by showing that jointly Gaussian $(\mathbf{X}, U_2, \ldots, U_K)$ are sufficient to evaluate the region given in Theorem 5.1 for the degraded Gaussian MIMO multi-receiver wiretap channel. The details of the proof of Theorem 5.2 are deferred to Section 5.5. We acknowledge an independent and concurrent work in [45], where the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is found for $K = 2$. Their proof is different than ours in the sense that it first provides a vector generalization of Costa's entropy-power inequality [44], and next uses this generalized inequality to establish the secrecy capacity region of the two-user degraded Gaussian MIMO multi-receiver wiretap channel.

5.3.2 Aligned Gaussian MIMO Multi-receiver Wiretap Channel

Next, we consider the aligned Gaussian MIMO multi-receiver wiretap channel which is again defined by (5.8)-(5.9), and the input is again subject to a covariance constraint as in (5.10) with $\mathbf{S} \succ \mathbf{0}$. However, for the aligned Gaussian MIMO multi-receiver wiretap channel, noise covariance matrices do not have any semi-definite ordering, as opposed to the degraded case which exhibits the ordering in (5.11). For the aligned Gaussian MIMO multi-receiver wiretap channel, the only assumption on the noise covariance matrices is that they are strictly positive-definite, i.e., $\mathbf{\Sigma}_i \succ \mathbf{0},\ i = 1, \ldots, K$ and $\mathbf{\Sigma}_Z \succ \mathbf{0}$. Since this channel does not have any ordering

among the noise covariance matrices, it cannot be considered as a degraded channel, thus there is no single-letter formula for its secrecy capacity region. Moreover, we do not expect superposition coding with stochastic encoding to be optimal, as it was optimal for the degraded channel. Indeed, we will show that dirty-paper coding with stochastic encoding is optimal in this case.

In Section 5.6, we obtain the secrecy capacity region of the aligned Gaussian MIMO multi-receiver wiretap channel, which will be stated next. To this end, we introduce some notation which is necessary to express the secrecy capacity region of the aligned Gaussian MIMO multi-receiver wiretap channel. Given the covariance matrices $\{\mathbf{K}_i\}_{i=1}^K$ such that $\sum_{i=1}^K \mathbf{K}_i \preceq \mathbf{S}$, let us define the following rates,

$$R_k^{\mathrm{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right) = \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_{\pi(k)}\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \ldots, K \tag{5.15}$$

where $\pi(\cdot)$ is a one-to-one permutation on $\{1, \ldots, K\}$. We also note that the subscript of $R_k^{\mathrm{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right)$ does not denote the kth user, instead it denotes the $(K-k+1)$th user in line to be encoded. Rather, the secrecy rate of the kth user is given by

$$R_{\pi^{-1}(k)}^{\mathrm{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right) \tag{5.16}$$

when dirty-paper coding with stochastic encoding is used with an encoding order of π. We define the following region:

$$\begin{aligned}
&\mathcal{R}^{\mathrm{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right) \\
&= \left\{ (R_1, \ldots, R_K) \;\middle|\; \begin{array}{c} R_k \le R_{\pi^{-1}(k)}^{\mathrm{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right),\ k = 1, \ldots, K, \\ \text{for some } \{\mathbf{K}_i\}_{i=1}^K \text{ such that } \mathbf{K}_i \succeq 0,\ i = 1, \ldots, K, \\ \text{and } \sum_{i=1}^K \mathbf{K}_i \preceq \mathbf{S} \end{array} \right\}
\end{aligned} \tag{5.17}$$

The secrecy capacity region of the aligned Gaussian MIMO broadcast channel is given by the following theorem.

Theorem 5.3 *The secrecy capacity region of the aligned Gaussian MIMO multi-receiver wiretap channel is given by the convex closure of the following union*

$$\bigcup_{\pi \in \Pi} \mathcal{R}^{\mathrm{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right) \tag{5.18}$$

where Π *is the set of all possible one-to-one permutations on* $\{1, \ldots, K\}$.

We show the achievability of the region in Theorem 5.3 by using dirty-paper coding with stochastic encoding. We provide the converse proof of Theorem 5.3 by using our capacity result for the degraded Gaussian MIMO multi-receiver wiretap channel given in Theorem 5.2 in conjunction with the channel enhancement technique [4]. The details of the proof of Theorem 5.3 are deferred to Section 5.6.

5.3.3 General Gaussian MIMO Multi-receiver Wiretap Channel

Finally, we consider the most general form of the Gaussian MIMO multi-receiver wiretap channel, see Figure 5.3 which is given by

$$\mathbf{Y}_k = \mathbf{H}_k\mathbf{X} + \mathbf{N}_k, \quad k = 1, \ldots, K \tag{5.19}$$

$$\mathbf{Z} = \mathbf{H}_Z\mathbf{X} + \mathbf{N}_Z \tag{5.20}$$

where the channel input $\mathbf{X}$, which is a $t \times 1$ column vector, is again subject to a covariance constraint as in (5.10) with $\mathbf{S} \succeq \mathbf{0}$. The channel output for the kth user is denoted by $\mathbf{Y}_k$ which is a column vector of size $r_k \times 1,\ k = 1, \ldots, K$. The eavesdropper's observation $\mathbf{Z}$ is of size $r_Z \times 1$. The covariance matrices of the Gaussian random vectors $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ are denoted by $\{\mathbf{\Sigma}_k\}_{k=1}^K, \mathbf{\Sigma}_Z$[3], which are assumed to be strictly positive definite. The channel gain matrices $\{\mathbf{H}_k\}_{k=1}^K, \mathbf{H}_Z$ are of sizes $\{r_k \times t\}_{k=1}^K, r_Z \times t$, respectively, and they are known to the transmitter, all legitimate users and the eavesdropper.

Similar to the aligned Gaussian MIMO multi-receiver wiretap channel, we obtain the secrecy capacity region of the general Gaussian MIMO multi-receiver wiretap channel by showing the optimality of the dirty-paper coding with stochastic encoding. Next, we state the secrecy capacity region of the general Gaussian MIMO multi-receiver wiretap channel. To this end, we introduce some notation which is necessary to express the secrecy capacity region of the general Gaussian MIMO

[3]Although, for the general Gaussian MIMO multi-receiver wiretap channel, there is no loss of generality to assume that the noise covariance matrices are identity matrices, we let them be arbitrary for the consistency of our presentation.

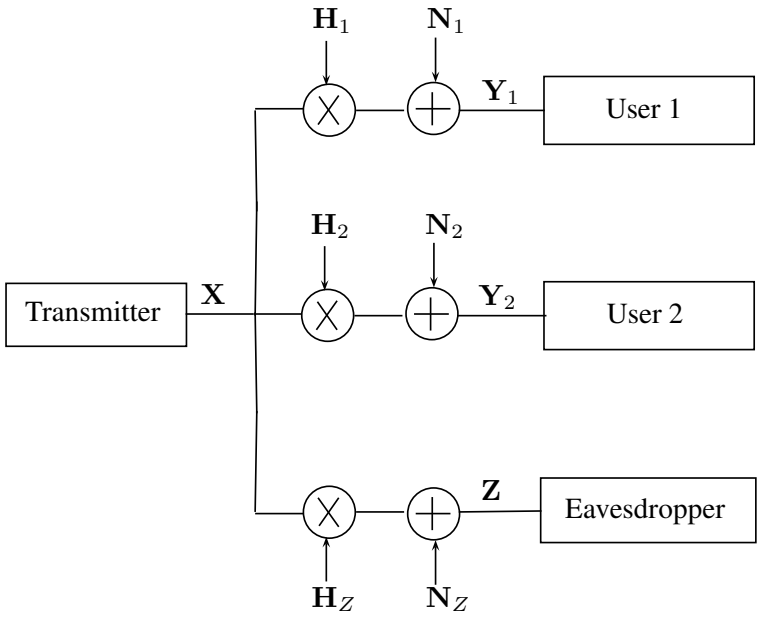

Figure 5.3: General Gaussian MIMO multi-receiver wiretap channel for $K = 2$.

multi-receiver wiretap channel. Given the covariance matrices $\{\mathbf{K}_k\}_{k=1}^K$ such that $\sum_{k=1}^K \mathbf{K}_k \preceq \mathbf{S}$, we define the following rates

$$R_k^{\mathrm{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right)$$
$$= \frac{1}{2}\log\frac{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|}{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\mathbf{H}_Z\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|}{\left|\mathbf{H}_Z\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|},$$
$$k = 1, \ldots, K \tag{5.21}$$

where $\pi(\cdot)$ is a one-to-one permutation on $\{1, \ldots, K\}$. We also note that the subscript of $R_k^{\mathrm{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right)$ does not denote the kth user, instead it denotes the $(K-k+1)$th user in line to be encoded. Rather,

the secrecy rate of the kth user is given by

$$R^{\mathrm{DPC}}_{\pi^{-1}(k)}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right) \tag{5.22}$$

when dirty-paper coding with stochastic encoding is used with an encoding order of π.

We define the following region.

$$\begin{aligned}
&\mathcal{R}^{\mathrm{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right) \\
&= \left\{ (R_1, \ldots, R_K) \;\middle|\; \begin{array}{c} R_k \leq R^{\mathrm{DPC}}_{\pi^{-1}(k)}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right), \\ k = 1, \ldots, K, \text{ for some } \{\mathbf{K}_i\}_{i=1}^K \text{ such that } \mathbf{K}_i \succeq 0, \\ i = 1, \ldots, K, \text{ and } \sum_{i=1}^K \mathbf{K}_i \preceq \mathbf{S} \end{array} \right\}
\end{aligned} \tag{5.23}$$

The secrecy capacity region of the general Gaussian MIMO broadcast channel is given by the following theorem.

Theorem 5.4 *The secrecy capacity region of the general Gaussian MIMO multi-receiver wiretap channel is given by the convex closure of the following union*

$$\bigcup_{\pi \in \Pi} \mathcal{R}^{\mathrm{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right) \tag{5.24}$$

where Π *is the set of all possible one-to-one permutations on* $\{1, \ldots, K\}$.

We prove Theorem 5.4 by using some limiting arguments in conjunction with

our capacity result for the aligned Gaussian MIMO multi-receiver wiretap channel given in Theorem 5.3. The details of the proof of Theorem 5.4 are deferred to Section 5.7.

5.3.4 A Comment on the Covariance Constraint

In the literature, it is more common to define capacity regions under a total power constraint, i.e., $\mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^{\top}\right]\right) \leq P$, instead of the covariance constraint that we imposed, i.e., $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}$. However, as shown in [4], once the capacity region is obtained under a covariance constraint, then the capacity region under more lenient constraints on the channel inputs can be obtained, if these constraints can be expressed as compact sets defined over the input covariance matrices. For example, the total power constraint and the per-antenna power constraint can be described by compact sets of input covariance matrices as follows

$$\mathcal{S}^{\mathrm{total}} = \{\mathbf{S} \succeq \mathbf{0} : \mathrm{tr}(\mathbf{S}) \leq P\} \tag{5.25}$$

$$\mathcal{S}^{\mathrm{per-ant}} = \{\mathbf{S} \succeq \mathbf{0} : \mathbf{S}_{ii} \leq P_i,\ i = 1, \ldots, t\} \tag{5.26}$$

respectively, where $\mathbf{S}_{ii}$ is the ith diagonal entry of $\mathbf{S}$, and t denotes the number of transmit antennas. Thus, if the secrecy capacity region under a covariance constraint $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}$ is found and denoted by $\mathcal{C}(\mathbf{S})$, then the secrecy capacity regions under the total power constraint and the per-antenna power constraint can be expressed

as

$$\mathcal{C}^{\text{total}} = \bigcup_{\mathbf{S}\in\mathcal{S}^{\text{total}}} \mathcal{C}(\mathbf{S}) \tag{5.27}$$

$$\mathcal{C}^{\text{per-ant}} = \bigcup_{\mathbf{S}\in\mathcal{S}^{\text{per-ant}}} \mathcal{C}(\mathbf{S}) \tag{5.28}$$

respectively.

One other comment about the covariance constraint on the channel input is regarding the positive definiteness of $\mathbf{S}$. Following Lemma 2 of [4], it can be shown that, for any degraded (resp. aligned) Gaussian MIMO multi-receiver channel under a covariance constraint $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}$ where $\mathbf{S}$ is a non-invertible positive semi-definite matrix, i.e., $\mathbf{S} \succeq \mathbf{0}$ and $|\mathbf{S}| = 0$, we can find another equivalent degraded (resp. aligned) channel with fewer transmit and receive antennas under a covariance constraint $E\big[\hat{\mathbf{X}}\hat{\mathbf{X}}^{\top}\big] \preceq \mathbf{S}'$ such that $\mathbf{S}' \succ \mathbf{0}$. Here the equivalence refers to the fact that both of these channels will have the same secrecy capacity region. Thus, as long as a degraded or an aligned channel is considered, there is no loss of generality in imposing a covariance constraint with a strictly positive definite matrix $\mathbf{S}$, and this is why we assumed that $\mathbf{S}$ is strictly positive definite for the degraded and the aligned channels.

5.4 Gaussian SISO Multi-receiver Wiretap Channel

We first visit the Gaussian SISO multi-receiver wiretap channel. The aims of this section are to show that a straightforward extension of existing converse techniques

for the Gaussian scalar broadcast channel fails to provide a converse proof for the Gaussian SISO multi-receiver wiretap channel, and to provide an alternative proof technique using either the MMSE or the Fisher information along with their connections with the differential entropy. To this end, we first define the Gaussian SISO multi-receiver wiretap channel

$$Y_k = X + N_k, \quad k = 1, 2 \tag{5.29}$$

$$Z = X + N_Z \tag{5.30}$$

where we also restrict our attention to the two-user case for simplicity of the presentation. The channel input X is subject to a power constraint $E[X^2] \leq P$. The variances of the zero-mean Gaussian random variables N_1, N_2, N_Z are given by $\sigma_1^2, \sigma_2^2, \sigma_Z^2$, respectively, and satisfy the following order

$$\sigma_1^2 \leq \sigma_2^2 \leq \sigma_Z^2 \tag{5.31}$$

Since the correlations among N_1, N_2, N_Z have no effect on the secrecy capacity region, we can adjust the correlation structure to ensure the following Markov chain

$$X \to Y_1 \to Y_2 \to Z \tag{5.32}$$

Thus, this channel can be considered as a degraded channel, and its secrecy capacity region is given by Theorem 5.1, in particular, by (5.6) and (5.7). Hence, to compute

the secrecy capacity region explicitly, we need to find the optimal joint distributions of (X, U_2) in (5.6) and (5.7). The corresponding secrecy capacity region is given by the following theorem.

Theorem 5.5 *The secrecy capacity region of the two-user Gaussian SISO wiretap channel is given by the union of the rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{5.33}$$

$$R_2 \leq \frac{1}{2}\log\left(1+\frac{\bar{\alpha} P}{\alpha P+\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\bar{\alpha} P}{\alpha P+\sigma_Z^2}\right) \tag{5.34}$$

where the union is over all $\alpha \in [0,1]$*, and* $\bar{\alpha}$ *denotes* $1-\alpha$*.*

The achievability of this region can be shown by selecting (X, U_2) to be jointly Gaussian in Theorem 5.1. We focus on the converse proof.

5.4.1 Revisiting Converse Proofs for the Gaussian Scalar Broadcast Channel

As a natural approach, one might try to adopt the converse proofs of the scalar Gaussian broadcast channel for the converse proof of Theorem 5.5. In the literature, there are two converses for the Gaussian scalar broadcast channel which share some main principles. The first converse was given by Bergmans [39] who used Fano's lemma in conjunction with the entropy-power inequality [41–43] to find the capacity region. Later, El Gamal gave a relatively simple proof [40] which does not recourse to Fano's lemma. Rather, he started from the single-letter expression for the capacity

region and used entropy-power inequality [41–43] to evaluate this region. Thus, the entropy-power inequality [41–43] is the main ingredient of these converses[4].

We now attempt to extend these converses to our secrecy context, i.e., to provide the converse proof of Theorem 5.5, and show where the argument breaks. In particular, what we will show in the following discussion is that a stand-alone use of the entropy-power inequality [41–43] falls short of proving the optimality of Gaussian signalling in this secrecy context, as opposed to the Gaussian scalar broadcast channel. For that purpose, we consider El Gamal's converse for the Gaussian scalar broadcast channel. However, since the entropy-power inequality is in a central role for both El Gamal's and Bergmans' converse, the upcoming discussion can be carried out by using Bergmans' proof as well.

First, we consider the bound on the second user's secrecy rate. Using (5.7), we have

$$I(U_2;Y_2) - I(U_2;Z) = \big[I(X;Y_2) - I(X;Z)\big] - \big[I(X;Y_2|U_2) - I(X;Z|U_2)\big] \quad (5.35)$$

where the right-hand side is obtained by using the chain rule, and the Markov chain $U_2 \to X \to (Y_1, Y_2, Z)$. The expression in the first bracket is maximized by Gaussian

[4]We again note that, in this chapter, the entropy-power inequality refers to the original form of this inequality which was proposed by Shannon [41], but not the subsequent variants of this inequality such as Costa's entropy-power inequality [44]. Indeed, using Costa's entropy-power inequality, it is possible to provide a converse proof for the secrecy capacity region of the Gaussian scalar multi-receiver wiretap channel [45].

X [49] yielding

$$I(X;Y_2) - I(X;Z) \leq \frac{1}{2}\log\left(1+\frac{P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right) \tag{5.36}$$

Moreover, using the Markov chain $U_2 \to X \to Y_2 \to Z$, we can bound the expression in the second bracket as

$$0 \leq I(X;Y_2|U_2) - I(X;Z|U_2) \tag{5.37}$$

$$\leq I(X;Y_2) - I(X;Z) \tag{5.38}$$

$$\leq \frac{1}{2}\log\left(1+\frac{P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right) \tag{5.39}$$

which implies that for any (X, U_2) pair, there exists an $\alpha \in [0,1]$ such that

$$I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{5.40}$$

Combining (5.36) and (5.40) in (5.35) yields the desired bound on R_2 given in (5.34).

From now on, we focus on obtaining the bound given in (5.33) on the first user's

secrecy rate. To this end, one needs to solve the following optimization problem[5]

$$\max \; I(X;Y_1|U_2) - I(X;Z|U_2) \tag{5.41}$$

$$\text{s.t.} \quad I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{5.42}$$

When the term $I(X;Z|U_2)$ is absent in both the objective function and the constraint, as in the case of the Gaussian scalar broadcast channel, the entropy-power inequality [41–43] can be used to solve this optimization problem. However, the presence of this term complicates the situation, and a stand-alone use of the entropy-power inequality [41–43] does not seem to be sufficient. To substantiate this claim, let us consider the objective function in (5.41)

$$I(X;Y_1|U_2) - I(X;Z|U_2) = h(Y_1|U_2) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{5.43}$$

$$\leq \frac{1}{2}\log\left(e^{2h(Z|U_2)} - 2\pi e\left(\sigma_Z^2 - \sigma_1^2\right)\right) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{5.44}$$

where the inequality is obtained by using the entropy-power inequality [41–43]. Since the right-hand side of (5.44) is monotonically increasing in $h(Z|U_2)$, to show the optimality of Gaussian signalling, we need

$$h(Z|U_2) \leq \frac{1}{2}\log 2\pi e(\alpha P + \sigma_Z^2) \tag{5.45}$$

[5]Equivalently, one can consider the following optimization problem

$$\max \; I(X;Y_1|U_2) - I(X;Y_2|U_2)$$

$$\text{s.t.} \quad I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right)$$

which, in turn, would yield a similar contradiction.

which will result in the desired bound on (5.41), i.e., the desired end-result in (5.33).

We now check whether (5.45) holds under the constraint given in (5.42). To this end, consider the difference of mutual informations in (5.42)

$$I(X;Y_2|U_2) - I(X;Z|U_2) = h(Y_2|U_2) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \tag{5.46}$$

$$\leq \frac{1}{2}\log\left(e^{2h(Z|U_2)} - 2\pi e\left(\sigma_Z^2 - \sigma_2^2\right)\right) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \tag{5.47}$$

where the inequality is obtained by using the entropy-power inequality [41–43]. Now, using the constraint given in (5.42) in (5.47), we get

$$\frac{1}{2}\log\left(\frac{\alpha P + \sigma_2^2}{\alpha P + \sigma_Z^2}\right) \leq \frac{1}{2}\log\left(e^{2h(Z|U_2)} - 2\pi e\left(\sigma_Z^2 - \sigma_2^2\right)\right) - h(Z|U_2) \tag{5.48}$$

which implies

$$\frac{1}{2}\log 2\pi e(\alpha P + \sigma_Z^2) \leq h(Z|U_2) \tag{5.49}$$

Thus, as opposed to the inequality that we need to show the optimality of Gaussian signalling via the entropy-power inequality [41–43], i.e., the bound in (5.45), we have an opposite inequality. This discussion reveals that if Gaussian signalling is optimal, then its proof cannot be deduced from a straightforward extension of the converse proofs for the Gaussian scalar broadcast channel in [39, 40]. Thus, we need a new technique to provide the converse for Theorem 5.5. We now present two different proofs. The first proof relies on the relationship between the MMSE and the mutual

information along with the properties of the MMSE, and the second proof replaces the MMSE with the Fisher information.

5.4.2 Converse for Theorem 5.5 Using the MMSE

We now provide a converse which uses the connection between the MMSE and the mutual information established in [46, 47]. In [47], the authors also give an alternative converse for the scalar Gaussian broadcast channel. Our proof will follow this converse, and generalize it to the context where there are secrecy constraints.

First, we briefly state the necessary background information. Let N be a zero-mean unit-variance Gaussian random variable, and (U, X) be a pair of arbitrarily correlated random variables which are independent of N. The MMSE of X when it is observed through U and $\sqrt{t}X + N$ is

$$\text{mmse}(X, t|U) = E\left[\left(X - E\left[X|\sqrt{t}X + N, U\right]\right)^2\right] \tag{5.50}$$

As shown in [46, 47], the MMSE and the conditional mutual information are related through

$$I(X; \sqrt{t}X + N|U) = \frac{1}{2}\int_0^t \text{mmse}(X, t|U)dt \tag{5.51}$$

For our converse, we need the following proposition which was proved in [47].

Proposition 5.1 ([47, Proposition 12]) *Let U, X, N be as specified above. The*

function

$$f(t) = \frac{\sigma^2}{\sigma^2 t + 1} - \text{mmse}(X, t|U) \tag{5.52}$$

has at most one zero in $[0, \infty)$ *unless* X *is Gaussian conditioned on* U *with variance* σ^2*, in which case the function is identically zero on* $[0, \infty)$*. In particular, if* $t_0 < \infty$ *is the unique zero, then* $f(t)$ *is strictly increasing on* $[0, t_0]$*, and strictly positive on* (t_0, ∞)*.*

We now give the converse. We use exactly the same steps from (5.35) to (5.40) to establish the bound on the secrecy rate of the second user given in (5.34). To bound the secrecy rate of the first user, we first restate (5.40) as

$$\begin{aligned} & I(X; Y_2|U_2) - I(X; Z|U_2) \\ & \quad = I(X; (1/\sigma_2)X + N|U_2) - I(X; (1/\sigma_Z)X + N|U_2) && (5.53) \\ & \quad = \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_Z^2}\right) && (5.54) \\ & \quad = \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \frac{\alpha P}{t\alpha P + 1} dt && (5.55) \end{aligned}$$

Furthermore, due to (5.51), we also have

$$I(X; Y_2|U_2) - I(X; Z|U_2) = \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \text{mmse}(X, t|U_2) dt \tag{5.56}$$

Comparing (5.55) and (5.56) reveals that either we have

$$\text{mmse}(X, t|U_2) = \frac{\alpha P}{t\alpha P + 1} \tag{5.57}$$

for all $t \in [1/\sigma_Z^2, 1/\sigma_2^2]$, or there exists a unique $t_0 \in (1/\sigma_Z^2, 1/\sigma_2^2)$ such that

$$\text{mmse}(X, t_0|U_2) = \frac{\alpha P}{t_0\alpha P + 1} \tag{5.58}$$

and

$$\text{mmse}(X, t|U_2) \leq \frac{\alpha P}{t\alpha P + 1} \tag{5.59}$$

for $t > t_0$, because of Proposition 5.1. The former case occurs if X is Gaussian conditioned on U_2 with variance αP, in which case we arrive at the desired bound on the secrecy rate of the first user given in (5.33). If we assume that the latter case in (5.58)-(5.59) occurs, then, we can use the following sequence of derivations

to bound the first user's secrecy rate

$$
\begin{aligned}
&I(X;Y_1|U_2) - I(X;Z|U_2) \\
&\quad = I(X;(1/\sqrt{\sigma_1})X + N|U_2) - I(X;(1/\sqrt{\sigma_Z})X + N|U_2) && (5.60)\\
&\quad = \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_1^2} \mathrm{mmse}(X,t|U_2)dt && (5.61)\\
&\quad = \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \mathrm{mmse}(X,t|U_2)dt + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \mathrm{mmse}(X,t|U_2)dt && (5.62)\\
&\quad = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \\
&\qquad + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \mathrm{mmse}(X,t|U_2)dt && (5.63)\\
&\quad \le \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \frac{\alpha P}{t\alpha P+1}dt && (5.64)\\
&\quad = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) && (5.65)
\end{aligned}
$$

where (5.63) follows from (5.55) and (5.56), and (5.64) is due to (5.59). Since (5.65) is the desired bound on the secrecy rate of the first user given in (5.33), this completes the converse proof.

5.4.3 Converse for Theorem 5.5 Using the Fisher Information

We now provide an alternative converse which replaces the MMSE with the Fisher information in the above proof. We first provide some basic definitions. The unconditional versions of the following definition and the upcoming results regarding the Fisher information can be found in standard detection-estimation texts; to note one, [50] is a good reference for a detailed treatment of the subject.

Definition 5.1 *Let X, U be arbitrarily correlated random variables with well-defined densities, and $f(x|u)$ be the corresponding conditional density. The conditional Fisher information of X is defined by*

$$J(X|U) = E\left[\left(\frac{\partial \log f(x|u)}{\partial x}\right)^2\right] \tag{5.66}$$

where the expectation is over (U, X).

The vector generalization of the following conditional form of the Fisher information inequality will be given in Lemma 5.15 in Section 5.5.4, thus its proof is omitted here.

Lemma 5.1 *Let U, X, Y be random variables, and let the density for any combination of them exist. Moreover, let us assume that given U, X and Y are independent. Then, we have*

$$J(X + Y|U) \leq \beta^2 J(X|U) + (1 - \beta)^2 J(Y|U) \tag{5.67}$$

for any $\beta \in [0, 1]$.

Corollary 5.1 *Let X, Y, U be as specified above. Then, we have*

$$\frac{1}{J(X + Y|U)} \geq \frac{1}{J(X|U)} + \frac{1}{J(Y|U)} \tag{5.68}$$

Proof: Select

$$\beta = \frac{J(Y|U)}{J(X|U) + J(Y|U)} \tag{5.69}$$

in the previous lemma. □

Similarly, the vector generalization of the following conditional form of the Cramer-Rao inequality will be given in Lemma 5.13 in Section 5.5.4, and hence, its proof is omitted here.

Lemma 5.2 *Let X, U be arbitrarily correlated random variables with well-defined densities. Then, we have*

$$J(X|U) \geq \frac{1}{\mathrm{Var}(X|U)} \tag{5.70}$$

with equality if (U, X) is jointly Gaussian.

We now provide the conditional form of the De Bruijn identity [41–43]. The vector generalization of this lemma will be provided in Lemma 5.17 in Section 5.5.4, and hence, its proof is omitted here.

Lemma 5.3 *Let X, U be arbitrarily correlated random variables with finite second order moments. Moreover, assume that they are independent of N which is a zero-mean unit-variance Gaussian random variable. Then, we have*

$$\frac{dh(X + \sqrt{t}N|U)}{dt} = \frac{1}{2} J(X + \sqrt{t}N|U) \tag{5.71}$$

We now note the following complementary relationship between the MMSE and the Fisher information [46, 48]

$$J(\sqrt{t}X + N) = 1 - t \cdot \text{mmse}(X, t) \tag{5.72}$$

which itself suggests the existence of an alternative converse which uses the Fisher information instead of the MMSE. We now provide the alternative converse based on the Fisher information. We first bound the secrecy rate of the second user as in the previous section, by following the exact steps from (5.35) to (5.40). To bound the secrecy rate of the first user, we first rewrite (5.40) as follows

$$\begin{aligned}
&I(X; Y_2|U_2) - I(X; Z|U_2) \\
&\quad = h(X + \sigma_2 N|U_2) - h(X + \sigma_Z N|U_2) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} && (5.73)\\
&\quad = -\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X + \sqrt{t}N|U_2)dt - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} && (5.74)\\
&\quad = -\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X + \sqrt{t - t^*}N' + \sqrt{t^*}N''|U_2)dt - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} && (5.75)
\end{aligned}$$

where (5.74) follows from Lemma 5.3, and in (5.75), we used the stability of Gaussian random variables where, N', N'' are two independent zero-mean unit-variance Gaussian random variables. Moreover, t^* is selected in the range of $(0, \sigma_2^2)$. We now

use Corollary 5.1 to bound the conditional Fisher information in (5.75) as follows

$$\frac{1}{J(X+\sqrt{t-t^*}N'+\sqrt{t^*}N''|U_2)} \geq \frac{1}{J(X+\sqrt{t^*}N''|U_2)} + \frac{1}{J(\sqrt{t-t^*}N'|U_2)} \tag{5.76}$$

$$= \frac{1}{J(X+\sqrt{t^*}N''|U_2)} + (t-t^*) \tag{5.77}$$

where the equality follows from Lemma 5.2. The inequality in (5.77) is equivalent to

$$J(X+\sqrt{t-t^*}N'+\sqrt{t^*}N''|U_2) \leq \frac{J(X+\sqrt{t^*}N''|U_2)}{1+J(X+\sqrt{t^*}N''|U_2)(t-t^*)} \tag{5.78}$$

using which in (5.75) yields

$$\begin{aligned} &I(X;Y_2|U_2) - I(X;Z|U_2) \\ &\quad \geq -\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} \frac{J(X+\sqrt{t^*}N''|U_2)}{1+J(X+\sqrt{t^*}N''|U_2)(t-t^*)}dt - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \qquad (5.79) \\ &\quad = -\frac{1}{2}\log\frac{1+J(X+\sqrt{t^*}N''|U_2)(\sigma_Z^2-t^*)}{1+J(X+\sqrt{t^*}N''|U_2)(\sigma_2^2-t^*)} - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \qquad (5.80) \end{aligned}$$

We remind that we had already fixed the left-hand side of this inequality as

$$I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{5.81}$$

in (5.40). Comparison of (5.80) and (5.81) results in

$$J(X+\sqrt{t^*}N''|U_2) \geq \frac{1}{\alpha P + t^*}, \quad 0 < t^* \leq \sigma_2^2 \tag{5.82}$$

At this point, we compare the inequalities in (5.59) and (5.82). These two inequalities imply each other through the complementary relationship between the MMSE and the Fisher information given in (5.72) after appropriate change of variables and by noting that $J(aX) = (1/a^2)J(X)$ [50]. We now find the desired bound on the secrecy rate of the first user via using the inequality in (5.82)

$$
\begin{aligned}
&I(X;Y_1|U_2) - I(X;Z|U_2) \\
&\quad = h(X+\sigma_1 N|U_2) - h(X+\sigma_Z N|U_2) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (5.83)\\
&\quad = -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (5.84)\\
&\quad = -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U_2)dt \\
&\qquad - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (5.85)\\
&\quad = -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right) \\
&\qquad - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (5.86)\\
&\quad \le -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} \frac{1}{\alpha P+t}dt - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (5.87)\\
&\quad = -\frac{1}{2}\log\left(\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_1^2}\right) - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (5.88)\\
&\quad = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) && (5.89)
\end{aligned}
$$

where (5.86) follows from (5.74) and (5.81), and (5.87) is due to (5.82). Since (5.89) provides the desired bound on the secrecy rate of the first user given in (5.33), this completes the converse proof.

5.4.4 Summary of the SISO Case, Outlook for the MIMO Case

In this section, we first revisited the standard converse proofs [39, 40] of the Gaussian scalar broadcast channel, and showed that a straightforward extension of these proofs will not be able to provide a converse proof for the Gaussian SISO multi-receiver wiretap channel. Basically, a stand-alone use of the entropy-power inequality [41–43] falls short of resolving the ambiguity on the auxiliary random variables. We showed that, in this secrecy context, either the connection between the mutual information and the MMSE or equivalently the connection between the differential entropy and the Fisher information can be used, along with their properties, to come up with a converse.

In the next section, we will generalize this converse proof technique to the degraded MIMO channel. One way of generalizing this converse technique to the MIMO case might be to use the channel enhancement technique, which was successfully used in extending Bergmans' converse proof from the Gaussian scalar broadcast channel to the degraded vector Gaussian broadcast channel. In the degraded Gaussian MIMO broadcast channel, the non-trivial part of the converse proof was to extend Bergmans' converse to a vector case, and this was accomplished by the invention of the channel enhancement technique. However, as we have shown in Section 5.4.1, even in the Gaussian SISO multi-receiver wiretap channel, a Bergmans type converse does not work. Thus, we do not expect that the channel enhancement technique will be sufficient to extend our converse proof from the SISO case to the MIMO case, similar to [5], where the channel enhancement technique alone

was not sufficient for the extension of a converse proof technique from the scalar Gaussian case to the vector Gaussian case. Consequently, we will not pursue a channel enhancement approach to extend our proof from the SISO channel to the degraded MIMO channel. Instead, we will use the connections between the Fisher information and the differential entropy, as we did in Section 5.4.3, to come up with a converse proof for the degraded MIMO channel. We will then use the channel enhancement technique to extend our converse proof to the aligned MIMO channel from the degraded MIMO channel. Finally, we will use some limiting arguments, as in [4, 21], to come up with a converse proof for the most general MIMO channel.

5.5 Degraded Gaussian MIMO Multi-receiver Wiretap Channel

In this section, we establish the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel, which was stated in Theorem 5.2. The achievability of the rates in Theorem 5.2 follows from Theorem 5.1 by selecting $(\mathbf{X}, U_2, \ldots, U_K)$ to be jointly Gaussian. Thus, to prove Theorem 5.2, we only need to provide a converse. Since the converse proof is rather long and involves technical digressions, we first present the converse proof for $K = 2$. In this process, we will develop all necessary tools which we will use to provide the converse proof for arbitrary K in Section 5.5.5.

The secrecy capacity region of the two-user degraded MIMO channel, from

(5.13), is the union of the rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{5.90}$$

$$R_2 \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} \tag{5.91}$$

where the union is over all selections of $\mathbf{K}_1$ that satisfies $\mathbf{0} \preceq \mathbf{K}_1 \preceq \mathbf{S}$. We note that these rates are achievable by choosing $\mathbf{X} = \mathbf{U}_2 + \mathbf{V}$ in Theorem 5.1, where $\mathbf{U}_2$ and $\mathbf{V}$ are independent Gaussian random vectors with covariance matrices $\mathbf{S} - \mathbf{K}_1$ and $\mathbf{K}_1$, respectively. Next, we prove that the union of the rate pairs in (5.90) and (5.91) constitute the secrecy capacity region of the two-user degraded MIMO channel.

5.5.1 Proof of Theorem 5.2 for $K = 2$

To prove that (5.90) and (5.91) give the secrecy capacity region, we need the results of some intermediate optimization problems. The first one is the so-called worst additive noise lemma [36, 37].

Lemma 5.4 ([36, Lemma II.2]) *Let* $\mathbf{N}$ *be a Gaussian random vector with covariance matrix* $\mathbf{\Sigma}$*, and* $\mathbf{K}_X$ *be a positive semi-definite matrix. Consider the following optimization problem,*

$$\begin{aligned} \min_{p(\mathbf{x})} \quad & I(\mathbf{N}; \mathbf{N}+\mathbf{X}) \\ \text{s.t.} \quad & \mathrm{Cov}(\mathbf{X}) = \mathbf{K}_X \end{aligned} \tag{5.92}$$

where $\mathbf{X}$ *and* $\mathbf{N}$ *are independent. A Gaussian* $\mathbf{X}$ *is the minimizer of this optimization problem.*

The second optimization problem that will be useful in the upcoming proof is the conditional version of the following theorem.

Theorem 5.6 *Let* $\mathbf{X}, \mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ *be independent random vectors, where* $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ *are zero-mean Gaussian random vectors with covariance matrices* $\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z$*, respectively. Moreover, assume that the second moment of* $\mathbf{X}$ *is constrained as*

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{5.93}$$

where $\mathbf{S}$ *is a positive definite matrix. Then, for any admissible* $\mathbf{X}$*, there exists a matrix* $\mathbf{K}^*$ *such that* $\mathbf{0} \preceq \mathbf{K}^* \preceq \mathbf{S}$*, and*

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{5.94}$$

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_1) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{5.95}$$

The conditional version of Theorem 5.6 is given as follows.

Theorem 5.7 *Let* $\mathbf{U}, \mathbf{X}$ *be arbitrarily correlated random vectors which are independent of* $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$*, where* $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ *are zero-mean Gaussian random vectors with covariance matrices* $\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z$*, respectively. Moreover, assume that the*

second moment of $\mathbf{X}$ *is constrained as*

$$E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S} \tag{5.96}$$

where $\mathbf{S}$ *is a positive definite matrix. Then, for any admissible* $(\mathbf{U}, \mathbf{X})$ *pair, there exists a matrix* $\mathbf{K}^*$ *such that* $\mathbf{0} \preceq \mathbf{K}^* \preceq \mathbf{S}$*, and*

$$h(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - h(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{5.97}$$

$$h(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - h(\mathbf{X}+\mathbf{N}_1|\mathbf{U}) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{5.98}$$

Theorem 5.6 serves as a step towards the proof of Theorem 5.7. Proofs of these two theorems are deferred to Sections 5.5.3 and 5.5.4.

We are now ready to show that the secrecy capacity region of the two-user degraded MIMO channel is given by (5.90)-(5.91). We first consider R_2, and bound it using Theorem 5.1 as follows

$$R_2 \leq I(U_2;\mathbf{Y}_2) - I(U_2;\mathbf{Z}) \tag{5.99}$$

$$= [I(\mathbf{X};\mathbf{Y}_2) - I(\mathbf{X};\mathbf{Z})] - [I(\mathbf{X};\mathbf{Y}_2|U_2) - I(\mathbf{X};\mathbf{Z}|U_2)] \tag{5.100}$$

where the equality is obtained by using the chain rule and the Markov chain $U_2 \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}_2, \mathbf{Z})$. We now consider the expression in the first bracket of (5.100)

$$I(\mathbf{X};\mathbf{Y}_2) - I(\mathbf{X};\mathbf{Z}) = h(\mathbf{Y}_2) - h(\mathbf{Y}_2|\mathbf{X}) - h(\mathbf{Z}) + h(\mathbf{Z}|\mathbf{X}) \tag{5.101}$$

$$= h(\mathbf{Y}_2) - h(\mathbf{Z}) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_Z|} \tag{5.102}$$

where the second equality follows from the facts that $h(\mathbf{Y}_2|\mathbf{X}) = h(\mathbf{N}_2)$ and $h(\mathbf{Z}|\mathbf{X}) = h(\mathbf{N}_Z)$. We now consider the difference of differential entropies in (5.102). To this end, let us introduce the Gaussian random vector $\tilde{\mathbf{N}}_2$ with covariance matrix $\mathbf{\Sigma}_Z - \mathbf{\Sigma}_2$, which is independent of $\mathbf{X}, \mathbf{N}_2$. Then, we have

$$h(\mathbf{Y}_2) - h(\mathbf{Z}) = h(\mathbf{Y}_2) - h(\mathbf{Y}_2 + \tilde{\mathbf{N}}_2) \tag{5.103}$$

$$= -I(\tilde{\mathbf{N}}_2; \mathbf{Y}_2 + \tilde{\mathbf{N}}_2) \tag{5.104}$$

$$\leq \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2}\log\frac{|\mathbf{K} + \mathbf{\Sigma}_2|}{|\mathbf{K} + \mathbf{\Sigma}_Z|} \tag{5.105}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_2|}{|\mathbf{S} + \mathbf{\Sigma}_Z|} \tag{5.106}$$

where (5.103) follows from the fact that the difference of entropies depends only on the marginal distributions of $\mathbf{Y}_2$ and $\mathbf{Z}$, and the stability of Gaussian random vectors[6], (5.105) follows from Lemma 5.4, and (5.106) is a consequence of the fact

[6]Stability of Gaussian random vectors refers to the fact that the sum of two independent Gaussian random vectors is Gaussian, and the corresponding covariance matrix is the sum of the covariance matrices of the independent Gaussian random vectors.

that

$$\frac{|\mathbf{B}|}{|\mathbf{A}+\mathbf{B}|} \leq \frac{|\mathbf{B}+\mathbf{\Delta}|}{|\mathbf{A}+\mathbf{B}+\mathbf{\Delta}|} \tag{5.107}$$

when $\mathbf{A}, \mathbf{B}, \mathbf{\Delta} \succeq 0$, and $\mathbf{A}+\mathbf{B} \succ 0$ [4]. Plugging (5.106) into (5.102) yields

$$I(\mathbf{X};\mathbf{Y}_2) - I(\mathbf{X};\mathbf{Z}) \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{5.108}$$

We now consider the expression in the second bracket of (5.100). For that purpose, we use Theorem 5.7. According to Theorem 5.7, for any admissible pair $(U_2, \mathbf{X})$, there exists a $\mathbf{K}^*$ such that

$$h(\mathbf{X}+\mathbf{N}_Z|U_2) - h(\mathbf{X}+\mathbf{N}_2|U_2) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{5.109}$$

which is equivalent to

$$I(\mathbf{X};\mathbf{Z}|U_2) - I(\mathbf{X};\mathbf{Y}_2|U_2) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} \tag{5.110}$$

Thus, using (5.108) and (5.110) in (5.100), we get

$$R_2 \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} - \frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_Z|} \tag{5.111}$$

which is the desired bound on R_2 given in (5.91). We now obtain the desired bound on R_1 given in (5.90). To this end, we first bound R_1 using Theorem 5.1

$$R_1 \leq I(\mathbf{X};\mathbf{Y}_1|U_2) - I(\mathbf{X};\mathbf{Z}|U_2) \tag{5.112}$$

$$= h(\mathbf{Y}_1|U_2) - h(\mathbf{Y}_1|U_2,\mathbf{X}) - h(\mathbf{Z}|U_2) + h(\mathbf{Z}|U_2,\mathbf{X}) \tag{5.113}$$

$$= h(\mathbf{Y}_1|U_2) - h(\mathbf{Z}|U_2) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \tag{5.114}$$

where the second equality follows from the facts that $h(\mathbf{Y}_1|U_2,\mathbf{X}) = h(\mathbf{N}_1)$ and $h(\mathbf{Z}|U_2,\mathbf{X}) = h(\mathbf{N}_Z)$. To bound the difference of conditional differential entropies in (5.114), we use Theorem 5.7. Theorem 5.7 states that for any admissible pair $(U_2,\mathbf{X})$, there exists a matrix $\mathbf{K}^*$ such that it satisfies (5.109) and also

$$h(\mathbf{Z}|U_2) - h(\mathbf{Y}_1|U_2) \geq \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_1|} \tag{5.115}$$

Thus, using (5.115) in (5.114), we get

$$R_1 \leq \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{5.116}$$

which is the desired bound on R_1 given in (5.90), completing the converse proof for $K = 2$.

As we have seen, the main ingredient in the above proof was Theorem 5.7. Therefore, to complete the converse proof for the degraded channel for $K = 2$, from this point on, we will focus on the proof of Theorem 5.7. We will give the proof

of Theorem 5.7 in Section 5.5.4. In preparation to that, we will give the proof of Theorem 5.6, which is the unconditional version of Theorem 5.7, in Section 5.5.3. The proof of Theorem 5.6 involves the use of properties of the Fisher information, and its connection to the differential entropy, which are provided next.

5.5.2 The Fisher Information Matrix

We start with the definition [50].

Definition 5.2 *Let* $\mathbf{U}$ *be a length-n random vector with differentiable density* $f_U(\mathbf{u})$*. The Fisher information matrix of* $\mathbf{U}$*,* $\mathbf{J}(\mathbf{U})$*, is defined as*

$$\mathbf{J}(\mathbf{U}) = E\left[\boldsymbol{\rho}(\mathbf{U})\boldsymbol{\rho}(\mathbf{U})^\top\right] \tag{5.117}$$

where $\boldsymbol{\rho}(\mathbf{u})$ *is the score function which is given by*

$$\boldsymbol{\rho}(\mathbf{u}) = \nabla \log f_U(\mathbf{u}) = \left[\begin{array}{ccc} \dfrac{\partial \log f_U(\mathbf{u})}{\partial u_1} & \ldots & \dfrac{\partial \log f_U(\mathbf{u})}{\partial u_n} \end{array}\right]^\top \tag{5.118}$$

Since we are mainly interested in the additive Gaussian channel, how the Fisher information matrix behaves under the addition of two independent random vectors is crucial. Regarding this, we have the following lemma which is due to [51].

Lemma 5.5 ([51, Lemma 3]) *Let* $\mathbf{U}$ *be a random vector with differentiable density, and let* $\boldsymbol{\Sigma}_U \succ \mathbf{0}$ *be its covariance matrix. Moreover, let* $\mathbf{V}$ *be another random vector with differentiable density, and be independent of* $\mathbf{U}$*. Then, we have the following facts:*

1. *Matrix form of the Cramer-Rao inequality*

$$\mathbf{J}(\mathbf{U}) \succeq \mathbf{\Sigma}_U^{-1} \tag{5.119}$$

which is satisfied with equality if $\mathbf{U}$ *is Gaussian.*

2. *For any square matrix* $\mathbf{A}$*,*

$$\mathbf{J}(\mathbf{U}+\mathbf{V}) \preceq \mathbf{A}\mathbf{J}(\mathbf{U})\mathbf{A}^\top + (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{V})(\mathbf{I}-\mathbf{A})^\top \tag{5.120}$$

We will use the following consequences of this lemma.

Corollary 5.2 *Let* $\mathbf{U}, \mathbf{V}$ *be as specified before. Then,*

1. $\mathbf{J}(\mathbf{U}+\mathbf{V}) \preceq \mathbf{J}(\mathbf{U})$

2. $\mathbf{J}(\mathbf{U}+\mathbf{V}) \preceq \left[\mathbf{J}(\mathbf{U})^{-1} + \mathbf{J}(\mathbf{V})^{-1}\right]^{-1}$

Proof: The first part of the corollary is obtained by choosing $\mathbf{A} = \mathbf{I}$, and the second part is obtained by choosing

$$\mathbf{A} = \left[\mathbf{J}(\mathbf{U})^{-1} + \mathbf{J}(\mathbf{V})^{-1}\right]^{-1}\mathbf{J}(\mathbf{U})^{-1} \tag{5.121}$$

and also by noting that $\mathbf{J}(\cdot)$ is always a symmetric matrix. □

The following lemma regarding the Fisher information matrix is also useful in the proof of Theorem 5.6.

Lemma 5.6 *Let* $\mathbf{U}, \mathbf{V}_1, \mathbf{V}_2$ *be random vectors such that* $\mathbf{U}$ *and* $(\mathbf{V}_1, \mathbf{V}_2)$ *are independent. Moreover, let* $\mathbf{V}_1, \mathbf{V}_2$ *be Gaussian random vectors with covariance matrices* $\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2$*. Then, we have*

$$\mathbf{J}(\mathbf{U} + \mathbf{V}_2)^{-1} - \mathbf{\Sigma}_2 \succeq \mathbf{J}(\mathbf{U} + \mathbf{V}_1)^{-1} - \mathbf{\Sigma}_1 \tag{5.122}$$

Proof: Without loss of generality, let $\mathbf{V}_2 = \mathbf{V}_1 + \tilde{\mathbf{V}}_1$ such that $\tilde{\mathbf{V}}_1$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_2 - \mathbf{\Sigma}_1$, and independent of $\mathbf{V}_1$. Due to the second part of Corollary 5.2, we have

$$\mathbf{J}(\mathbf{U} + \mathbf{V}_2) = \mathbf{J}(\mathbf{U} + \mathbf{V}_1 + \tilde{\mathbf{V}}_1) \preceq \left[\mathbf{J}(\mathbf{U} + \mathbf{V}_1)^{-1} + \mathbf{J}(\tilde{\mathbf{V}}_1)^{-1}\right]^{-1} \tag{5.123}$$

$$= \left[\mathbf{J}(\mathbf{U} + \mathbf{V}_1)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_1\right]^{-1} \tag{5.124}$$

which is equivalent to

$$\mathbf{J}(\mathbf{U} + \mathbf{V}_2)^{-1} \succeq \mathbf{J}(\mathbf{U} + \mathbf{V}_1)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_1 \tag{5.125}$$

which proves the lemma. □

Moreover, we need the relationship between the Fisher information matrix and the differential entropy, which is due to [52].

Lemma 5.7 ([52, Theorem 4] *Let* $\mathbf{X}$ *and* $\mathbf{N}$ *be independent random vectors, where* $\mathbf{N}$ *is zero-mean Gaussian with covariance matrix* $\mathbf{\Sigma}_N \succ \mathbf{0}$*, and* $\mathbf{X}$ *has a finite*

second order moment. Then, we have

$$\nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}) = \frac{1}{2}\mathbf{J}(\mathbf{X}+\mathbf{N}) \tag{5.126}$$

5.5.3 Proof of Theorem 5.6

To prove Theorem 5.6, we first consider the following expression

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) \tag{5.127}$$

and show that (5.127) is bounded and finite due to the covariance constraint on $\mathbf{X}$. In particular, we have

$$\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{S}+\mathbf{\Sigma}_2|} \leq h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) \leq \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_2|} \tag{5.128}$$

where the lower bound can be shown by following the analysis given in (5.103)-(5.106). To show the upper bound in (5.128), first, we define $\tilde{\mathbf{N}}$ which is Gaussian with covariance matrix $\mathbf{\Sigma}_Z - \mathbf{\Sigma}_2$, and is independent of $\mathbf{N}_2$ and $\mathbf{X}$. Thus, without loss of generality, we can assume $\mathbf{Z} = \mathbf{X}+\mathbf{N}_2+\tilde{\mathbf{N}}$ by noting the stability of Gaussian

random vectors. Then, the right-hand side of (5.128) follows from

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) = I(\tilde{\mathbf{N}}; \mathbf{X}+\mathbf{N}_Z) \tag{5.129}$$

$$= h(\tilde{\mathbf{N}}) - h(\tilde{\mathbf{N}}|\mathbf{X}+\mathbf{N}_Z) \tag{5.130}$$

$$\leq h(\tilde{\mathbf{N}}) - h(\tilde{\mathbf{N}}|\mathbf{X}+\mathbf{N}_Z, \mathbf{X}) \tag{5.131}$$

$$= h(\tilde{\mathbf{N}}) - h(\tilde{\mathbf{N}}|\mathbf{N}_Z) \tag{5.132}$$

$$= I(\tilde{\mathbf{N}}; \mathbf{N}_Z) \tag{5.133}$$

$$= \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_2|} \tag{5.134}$$

where (5.131) comes from the fact that conditioning cannot increase entropy, and (5.132) is due to the fact that $\mathbf{X}$ and $(\mathbf{N}_2, \tilde{\mathbf{N}})$ are independent. Thus, we can fix the difference of the differential entropies in (5.128) to an α in this range, i.e., we can set

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) = \alpha \tag{5.135}$$

where $\alpha \in \left[\frac{1}{2}\log|\mathbf{S}+\mathbf{\Sigma}_Z|/|\mathbf{S}+\mathbf{\Sigma}_2|, \frac{1}{2}\log|\mathbf{\Sigma}_Z|/|\mathbf{\Sigma}_2|\right]$. We now would like to understand how the constraint in (5.135) affects the set of admissible random vectors. For that purpose, we use Lemma 5.7, and express this difference of entropies as an

integral of the Fisher information matrix[7]

$$\alpha = h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) = \frac{1}{2}\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \mathbf{J}(\mathbf{X}+\mathbf{N}) d\mathbf{\Sigma}_N \tag{5.136}$$

Using the stability of Gaussian random vectors, we can express $\mathbf{J}(\mathbf{X}+\mathbf{N})$ as

$$\mathbf{J}(\mathbf{X}+\mathbf{N}) = \mathbf{J}(\mathbf{X}+\mathbf{N}_2+\tilde{\mathbf{N}}) \tag{5.137}$$

where $\tilde{\mathbf{N}}$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N - \mathbf{\Sigma}_2 \succeq \mathbf{0}$, and is independent of $\mathbf{N}_2$. Using the second part of Corollary 5.2 in (5.137), we get

$$\mathbf{J}(\mathbf{X}+\mathbf{N}) = \mathbf{J}(\mathbf{X}+\mathbf{N}_2+\tilde{\mathbf{N}}) \preceq \left[\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} + \mathbf{J}(\tilde{\mathbf{N}})^{-1}\right]^{-1} \tag{5.138}$$

$$= \left[\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} + \mathbf{\Sigma}_N - \mathbf{\Sigma}_2\right]^{-1} \tag{5.139}$$

where we used the fact that $\mathbf{J}(\tilde{\mathbf{N}}) = (\mathbf{\Sigma}_N - \mathbf{\Sigma}_2)^{-1}$ which is a consequence of the first part of Lemma 5.5 by noting that $\tilde{\mathbf{N}}$ is Gaussian. We now bound the integral in (5.136) by using (5.139). For that purpose, we introduce the following lemma.

Lemma 5.8 *Let* $\mathbf{K}_1, \mathbf{K}_2$ *be positive semi-definite matrices satisfying* $\mathbf{0} \preceq \mathbf{K}_1 \preceq \mathbf{K}_2$, *and* $\mathbf{f}(\mathbf{K})$ *be a matrix-valued function such that* $\mathbf{f}(\mathbf{K}) \succeq \mathbf{0}$ *for* $\mathbf{K}_1 \preceq \mathbf{K} \preceq \mathbf{K}_2$.

[7]The integration in (5.136), i.e., $\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \mathbf{J}(\cdot) d\mathbf{\Sigma}$, is a line integral of the vector-valued function $\mathbf{J}(\cdot)$. Moreover, since $\mathbf{J}(\cdot)$ is the gradient of a scalar field, the integration expressed in $\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \mathbf{J}(\cdot) d\mathbf{\Sigma}$ is path-free, i.e., it yields the same value for any path from $\mathbf{\Sigma}_2$ to $\mathbf{\Sigma}_Z$. This remark applies to all upcoming integrals of $\mathbf{J}(\cdot)$.

Moreover, $\mathbf{f}(\mathbf{K})$ *is assumed to be the gradient of some scalar field. Then, we have*

$$\int_{\mathbf{K}_1}^{\mathbf{K}_2} \mathbf{f}(\mathbf{K}) d\mathbf{K} \geq 0 \tag{5.140}$$

Proof: Since $\mathbf{f}(\mathbf{K})$ is the gradient of some scalar field, the integral in (5.140) is path-free. Thus, this integral is equivalent to

$$\int_{\mathbf{K}_1}^{\mathbf{K}_2} \mathbf{f}(\mathbf{K}) d\mathbf{K} = \int_0^1 \mathbf{1}^\top \left[\mathbf{f}\big(\mathbf{K}_1 + t(\mathbf{K}_2 - \mathbf{K}_1)\big) \odot (\mathbf{K}_2 - \mathbf{K}_1) \right] \mathbf{1} dt \tag{5.141}$$

where $\odot$ denotes the Schur (Hadamard) product, and $\mathbf{1} = [1 \ \ldots \ 1]^\top$ with appropriate size. Since the Schur product of two positive semi-definite matrices is positive semi-definite [53], the integrand is non-negative implying the non-negativity of the integral. $\square$

In light of this lemma, using (5.139) in (5.136), we get

$$\alpha \leq \frac{1}{2} \int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \left[\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} + \mathbf{\Sigma}_N - \mathbf{\Sigma}_2 \right]^{-1} d\mathbf{\Sigma}_N \tag{5.142}$$

$$= \frac{1}{2} \log \frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_2|}{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1}|} \tag{5.143}$$

where we used the well-known fact that $\nabla_{\mathbf{\Sigma}} \log |\mathbf{\Sigma}| = \mathbf{\Sigma}^{-\top}$ for $\mathbf{\Sigma} \succ \mathbf{0}$. We also note that the denominator in (5.143) is strictly positive because

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} \succeq \mathbf{J}(\mathbf{N}_2)^{-1} = \mathbf{\Sigma}_2 \succ \mathbf{0} \tag{5.144}$$

which implies $|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1}| > 0$.

Following similar steps, we can also find a lower bound on α. Again, using the stability of Gaussian random vectors, we have

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_Z) = \mathbf{J}(\mathbf{X}+\mathbf{N}+\tilde{\mathbf{N}}) \tag{5.145}$$

where $\mathbf{N}, \tilde{\mathbf{N}}$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_N, \mathbf{\Sigma}_Z - \mathbf{\Sigma}_N$, respectively, $\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_Z$, and they are independent. Using the second part of Corollary 5.2 in (5.145) yields

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_Z) = \mathbf{J}(\mathbf{X}+\mathbf{N}+\tilde{\mathbf{N}}) \preceq \left[\mathbf{J}(\mathbf{X}+\mathbf{N})^{-1} + \mathbf{J}(\tilde{\mathbf{N}})^{-1}\right]^{-1} \tag{5.146}$$

$$= \left[\mathbf{J}(\mathbf{X}+\mathbf{N})^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_N\right]^{-1} \tag{5.147}$$

where we used the fact that $\mathbf{J}(\tilde{\mathbf{N}}) = (\mathbf{\Sigma}_Z - \mathbf{\Sigma}_N)^{-1}$ which follows from the first part of Lemma 5.5 due to the Gaussianity of $\tilde{\mathbf{N}}$. Then, (5.147) is equivalent to

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} \succeq \mathbf{J}(\mathbf{X}+\mathbf{N})^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_N \tag{5.148}$$

and that implies

$$\left[\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_N - \mathbf{\Sigma}_Z\right]^{-1} \preceq \mathbf{J}(\mathbf{X}+\mathbf{N}) \tag{5.149}$$

Use of Lemma 5.8 and (5.149) in (5.136) yields

$$\alpha \geq \int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \left[\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_N - \mathbf{\Sigma}_Z\right]^{-1} d\mathbf{\Sigma}_N \tag{5.150}$$

$$= \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1}|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_Z|} \tag{5.151}$$

where we again used $\nabla_{\mathbf{\Sigma}} \log|\mathbf{\Sigma}| = \mathbf{\Sigma}^{-\top}$ for $\mathbf{\Sigma} \succ \mathbf{0}$. Here also, the denominator is strictly positive because

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_Z \succeq \mathbf{J}(\mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_Z = \mathbf{\Sigma}_2 \succ \mathbf{0} \tag{5.152}$$

which implies $|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_Z| > 0$. Combining the two bounds on α given in (5.143) and (5.151) yields

$$\frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1}|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_Z|} \leq \alpha \leq \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_2|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1}|} \tag{5.153}$$

Next, we will discuss the implications of (5.153). First, we have a digression of technical nature to provide the necessary information for such a discussion. We present the following lemma from [53].

Lemma 5.9 ([53, Theorem 7.6.4]) *Let $\mathbf{A}, \mathbf{B} \in M_n$, where M_n is the set of all square matrices of size $n \times n$ over the complex numbers, be two Hermitian matrices and suppose that there is a real linear combination of $\mathbf{A}$ and $\mathbf{B}$ that is positive definite. Then there exists a non-singular matrix $\mathbf{C}$ such that both $\mathbf{C}^H\mathbf{A}\mathbf{C}$ and $\mathbf{C}^H\mathbf{B}\mathbf{C}$ are diagonal, where $(\cdot)^H$ denotes the conjugate transpose.*

Lemma 5.10 *Consider the function*

$$r(t) = \frac{1}{2} \log \frac{|\mathbf{A} + \mathbf{B} + t\mathbf{\Delta}|}{|\mathbf{A} + t\mathbf{\Delta}|}, \qquad 0 \leq t \leq 1 \tag{5.154}$$

where $\mathbf{A}, \mathbf{B}, \mathbf{\Delta}$ *are real, symmetric matrices, and* $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}, \mathbf{\Delta} \succeq \mathbf{0}$. *The function* $r(t)$ *is continuous and monotonically decreasing in* t.

Proof: We first define the function inside the $\log(\cdot)$ as

$$f(t) = \frac{|\mathbf{A} + \mathbf{B} + t\mathbf{\Delta}|}{|\mathbf{A} + t\mathbf{\Delta}|}, \qquad 0 \leq t \leq 1 \tag{5.155}$$

We first prove the continuity of $r(t)$. To this end, consider the function

$$g(t) = |\mathbf{E} + t\mathbf{\Delta}|, \qquad 0 \leq t \leq 1 \tag{5.156}$$

where $\mathbf{E} \succ \mathbf{0}$ is a real, symmetric matrix. By Lemma 5.9, there exists a non-singular matrix $\mathbf{C}$ such that both $\mathbf{C}^\top \mathbf{E} \mathbf{C}$ and $\mathbf{C}^\top \mathbf{\Delta} \mathbf{C}$ are diagonal. Thus, using this fact, we get

$$g(t) = \left|\mathbf{C}^{-\top} \mathbf{C}^\top \mathbf{E} \mathbf{C} \mathbf{C}^{-1} + t\mathbf{C}^{-\top} \mathbf{C}^\top \mathbf{\Delta} \mathbf{C} \mathbf{C}^{-1}\right| \tag{5.157}$$

$$= \left|\mathbf{C}^{-\top}\right| \left|\mathbf{C}^\top \mathbf{E} \mathbf{C} + t\mathbf{C}^\top \mathbf{\Delta} \mathbf{C}\right| \left|\mathbf{C}^{-1}\right| \tag{5.158}$$

$$= \frac{1}{|\mathbf{C}|^2} \left|\mathbf{C}^\top \mathbf{E} \mathbf{C} + t\mathbf{C}^\top \mathbf{\Delta} \mathbf{C}\right| \tag{5.159}$$

$$= \frac{1}{|\mathbf{C}|^2} |\mathbf{D}_E + t\mathbf{D}_\Delta| \tag{5.160}$$

where (5.158) follows from the fact that $|\mathbf{AB}| = |\mathbf{A}||\mathbf{B}|$, (5.159) comes from the fact that $\left|\mathbf{C}^{-\top}\right| = |\mathbf{C}^{-1}| = 1/|\mathbf{C}|$, and in (5.160), we defined the diagonal matrices $\mathbf{D}_E = \mathbf{C}^\top \mathbf{E}\mathbf{C}$, $\mathbf{D}_\Delta = \mathbf{C}^\top \boldsymbol{\Delta}\mathbf{C}$. Let the diagonal elements of $\mathbf{D}_E$ and $\mathbf{D}_\Delta$ be $\{d_{E,i}\}_{i=1}^n$ and $\{d_{\Delta,i}\}_{i=1}^n$, respectively. Then, $g(t)$ can be expressed as

$$g(t) = \frac{1}{|\mathbf{C}|^2} \prod_{i=1}^{n} (d_{E,i} + t d_{\Delta,i}) \tag{5.161}$$

which is polynomial in t, thus $g(t)$ is continuous in t. Being the ratio of two non-zero continuous functions, $f(t)$ is continuous as well. Then, continuity of $r(t)$ follows from the fact that composition of two continuous functions is also continuous.

We now show the monotonicity of $r(t)$. To this end, consider the derivative of $r(t)$

$$\frac{dr(t)}{dt} = \frac{1}{2f(t)} \frac{df(t)}{dt} \tag{5.162}$$

where we have $f(t) > 0$ because of the facts that $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}, \boldsymbol{\Delta} \succeq \mathbf{0}$, and $0 \leq t \leq 1$. Moreover, $f(t)$ is monotonically decreasing in t, which can be deduced from (5.107), implying $df(t)/dt \leq 0$. Thus, we have $dr(t)/dt \leq 0$, completing the proof. $\square$

After this digression, we are ready to investigate the implications of (5.153). For that purpose, let us select $\mathbf{A}, \mathbf{B}, \mathbf{\Delta}$ in $r(t)$ in Lemma 5.10 as follows

$$\mathbf{A} = \mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} \tag{5.163}$$

$$\mathbf{B} = \mathbf{\Sigma}_Z - \mathbf{\Sigma}_2 \tag{5.164}$$

$$\mathbf{\Delta} = \mathbf{J}(\mathbf{X} + \mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_Z - \mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} \tag{5.165}$$

where clearly $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}$, and also $\mathbf{\Delta} \succeq \mathbf{0}$ due to Lemma 5.6. With these selections, we have

$$r(0) = \frac{1}{2} \log \frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_2|}{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1}|} \tag{5.166}$$

$$r(1) = \frac{1}{2} \log \frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_Z)^{-1}|}{|\mathbf{J}(\mathbf{X} + \mathbf{N}_Z)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_Z|} \tag{5.167}$$

Thus, (5.153) can be expressed as

$$r(1) \leq \alpha \leq r(0) \tag{5.168}$$

We know from Lemma 5.10 that $r(t)$ is continuous in t. Then, from the intermediate value theorem, there exists a t^* such that $r(t^*) = \alpha$. Thus, we have

$$\alpha = r(t^*) = \frac{1}{2} \log \frac{|\mathbf{A} + t^*\mathbf{\Delta} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_2|}{|\mathbf{A} + t^*\mathbf{\Delta}|} \tag{5.169}$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} \tag{5.170}$$

where $\mathbf{K}^* = \mathbf{A} + t^*\mathbf{\Delta} - \mathbf{\Sigma}_2$. Since $0 \leq t^* \leq 1$, $\mathbf{K}^*$ satisfies the following orderings,

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} - \mathbf{\Sigma}_2 \preceq \mathbf{K}^* \preceq \mathbf{J}(\mathbf{X} + \mathbf{N}_Z)^{-1} - \mathbf{\Sigma}_Z \tag{5.171}$$

which in turn, by using Lemma 5.5 and Corollary 5.2, imply the following orderings,

$$\mathbf{K}^* \succeq \mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} - \mathbf{\Sigma}_2 \succeq \mathbf{J}(\mathbf{N}_2)^{-1} - \mathbf{\Sigma}_2 = \mathbf{\Sigma}_2 - \mathbf{\Sigma}_2 = \mathbf{0} \tag{5.172}$$

$$\mathbf{K}^\star \preceq \mathbf{J}(\mathbf{X} + \mathbf{N}_Z)^{-1} - \mathbf{\Sigma}_Z \preceq \mathrm{Cov}(\mathbf{X}) + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_Z = \mathrm{Cov}(\mathbf{X}) \preceq \mathbf{S} \tag{5.173}$$

which can be summarized as follows,

$$\mathbf{0} \preceq \mathbf{K}^\star \preceq \mathbf{S} \tag{5.174}$$

In addition, using Lemma 5.6 in (5.171), we get

$$\mathbf{K}^* \succeq \mathbf{J}(\mathbf{X} + \mathbf{N})^{-1} - \mathbf{\Sigma}_N \tag{5.175}$$

for any Gaussian random vector $\mathbf{N}$ such that its covariance matrix satisfies $\mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2$. The inequality in (5.175) is equivalent to

$$\mathbf{J}(\mathbf{X} + \mathbf{N}) \succeq (\mathbf{K}^* + \mathbf{\Sigma}_N)^{-1}, \quad \text{for} \quad \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2 \tag{5.176}$$

where $\mathbf{N}$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N$.

Returning to the proof of Theorem 5.6, we now lower bound

$$h(\mathbf{X}+\mathbf{N}_Z)-(\mathbf{X}+\mathbf{N}_1) \tag{5.177}$$

while keeping

$$h(\mathbf{X}+\mathbf{N}_Z)-(\mathbf{X}+\mathbf{N}_2)=\alpha=\frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{5.178}$$

The lower bound on (5.177) can be obtained as follows

$$\begin{aligned}
h(\mathbf{X}+\mathbf{N}_Z)-h(\mathbf{X}+\mathbf{N}_1) &= \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_Z}\mathbf{J}(\mathbf{X}+\mathbf{N})d\mathbf{\Sigma}_N && (5.179)\\
&= \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2}\mathbf{J}(\mathbf{X}+\mathbf{N})d\mathbf{\Sigma}_N+\frac{1}{2}\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z}\mathbf{J}(\mathbf{X}+\mathbf{N})d\mathbf{\Sigma}_N && (5.180)\\
&= \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2}\mathbf{J}(\mathbf{X}+\mathbf{N})d\mathbf{\Sigma}_N+\frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} && (5.181)\\
&\geq \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2}(\mathbf{K}^*+\mathbf{\Sigma}_N)^{-1}d\mathbf{\Sigma}_N+\frac{1}{2}\log\frac{|\mathbf{K}^\star+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} && (5.182)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_2|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|}+\frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} && (5.183)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^\star+\mathbf{\Sigma}_1|} && (5.184)
\end{aligned}$$

where (5.180) follows from the fact that the integral in (5.179) is path-independent, and (5.182) is due to Lemma 5.8 and (5.176).

Thus, we have shown the following: For any admissible random vector $\mathbf{X}$, we can find a positive semi-definite matrix $\mathbf{K}^*$ such that $\mathbf{0} \preceq \mathbf{K}^* \preceq \mathbf{S}$, and

$$h(\mathbf{X}+\mathbf{N}_Z) - (\mathbf{X}+\mathbf{N}_2) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{5.185}$$

and

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_1) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{5.186}$$

which completes the proof of Theorem 5.6.

5.5.4 Proof of Theorem 5.7

We now adapt the proof of Theorem 5.6 to the setting of Theorem 5.7 by providing the conditional versions of the tools we have used in the proof of Theorem 5.6. Main ingredients of the proof of Theorem 5.6 are: the relationship between the differential entropy and the Fisher information matrix given in Lemma 5.7, and the properties of the Fisher information matrix given in Lemmas 5.5, 5.6 and Corollary 5.2. Thus, in this section, we basically provide the extensions of Lemmas 5.5, 5.6, 5.7 and Corollary 5.2 to the conditional setting. From another point of view, the material that we present in this section can be regarded as extending some well-known results on the Fisher information matrix [50, 51] to a conditional setting.

We start with the definition of the conditional Fisher information matrix.

Definition 5.3 *Let* $(\mathbf{U},\mathbf{X})$ *be an arbitrarily correlated length-n random vector pair*

with well-defined densities. The conditional Fisher information matrix of $\mathbf{X}$ *given* $\mathbf{U}$ *is defined as*

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] \tag{5.187}$$

where the expectation is over the joint density $f(\mathbf{u}, \mathbf{x})$*, and the conditional score function* $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$ *is*

$$\boldsymbol{\rho}(\mathbf{x}|\mathbf{u}) = \nabla \log f(\mathbf{x}|\mathbf{u}) = \left[\begin{array}{ccc} \dfrac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_1} & \ldots & \dfrac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_n} \end{array}\right]^\top \tag{5.188}$$

The following lemma extends Stein identity [50, 51] to a conditional setting. We provide its proof in Appendix 5.9.1.

Lemma 5.11 (Conditional Stein Identity) *Let* $\mathbf{U}, \mathbf{X}$ *be as specified above. Consider a smooth scalar-valued function of* $\mathbf{x}$*,* $g(\mathbf{x})$*, which well-behaves at infinity in the sense that*

$$\lim_{x_i \to \pm\infty} g(\mathbf{x}) f(\mathbf{x}|\mathbf{u}) = 0, \qquad i = 1, \ldots, n \tag{5.189}$$

For such a $g(\mathbf{x})$*, we have*

$$E\left[g(\mathbf{X})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = -E\left[\nabla g(\mathbf{X})\right] \tag{5.190}$$

The following implications of this lemma are important for the upcoming proofs.

Corollary 5.3 *Let* $\mathbf{U}, \mathbf{X}$ *be as specified above.*

1. $E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = \mathbf{0}$

2. $E\left[\mathbf{X}\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right] = -\mathbf{I}$

Proof: The first and the second parts of the corollary follow from the previous lemma by selecting $g(\mathbf{x}) = 1$ and $g(\mathbf{x}) = x_i$, respectively. □

We also need the following variation of this corollary whose proof is given in Appendix 5.9.2.

Lemma 5.12 *Let* $\mathbf{U}, \mathbf{X}$ *be as specified above. Then, we have*

1. $E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})|\mathbf{U}\right] = \mathbf{0}$.

2. *Let* $g(\mathbf{u})$ *be a finite, scalar-valued function of* $\mathbf{u}$. *For such a* $g(\mathbf{u})$, *we have*

$$E\left[g(\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = \mathbf{0} \tag{5.191}$$

3. *Let* $E\left[\mathbf{X}|\mathbf{U}\right]$ *be finite, then we have*

$$E\left[E\left[\mathbf{X}|\mathbf{U}\right]\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right] = \mathbf{0} \tag{5.192}$$

We are now ready to prove the conditional version of the Cramer-Rao inequality, i.e., the generalization of the first part of Lemma 5.5 to a conditional setting.

Lemma 5.13 (Conditional Cramer-Rao Inequality) *Let* $\mathbf{U}, \mathbf{X}$ *be arbitrarily correlated random vectors with well-defined densities. Let the conditional covariance*

matrix of $\mathbf{X}$ *be* $\mathrm{Cov}(\mathbf{X}|\mathbf{U}) \succ \mathbf{0}$*, then we have*

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \tag{5.193}$$

which is satisfied with equality if $(\mathbf{U}, \mathbf{X})$ *is jointly Gaussian with conditional covariance matrix* $\mathrm{Cov}(\mathbf{X}|\mathbf{U})$*.*

Proof: We first prove the inequality in (5.193), and next show that jointly Gaussian $(\mathbf{U}, \mathbf{X})$ with conditional covariance matrix $\mathrm{Cov}(\mathbf{X}|\mathbf{U})$ satisfies the inequality in (5.193) with equality. To this end, we consider

$$\begin{aligned}
\mathbf{0} \preceq\ & E\Bigg[\Big(\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\Big) \\
& \qquad \Big(\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\Big)^{\top}\Bigg] \qquad (5.194) \\
=\ & E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right] + E\Big[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)^{\top}\Big]\,\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \\
& + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}E\left[\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right] \\
& + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}E\Big[\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)^{\top}\Big]\,\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \qquad (5.195) \\
=\ & \mathbf{J}(\mathbf{X}|\mathbf{U}) + E\Big[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)^{\top}\Big]\,\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \\
& + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}E\left[\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right] + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \qquad (5.196)
\end{aligned}$$

where for the second equality, we used the definition of the conditional Fisher infor-

mation matrix, and the conditional covariance matrix. We note that

$$\big(E\left[\big(\mathbf{X}-E\left[\mathbf{X}|\mathbf{U}\right]\big)\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right]\big)^\top = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\big(\mathbf{X}-E\left[\mathbf{X}|\mathbf{U}\right]\big)^\top\right] \tag{5.197}$$

$$= E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\mathbf{X}^\top\right] - E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})E\left[\mathbf{X}|\mathbf{U}\right]^\top\right] \tag{5.198}$$

$$= E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\mathbf{X}^\top\right] \tag{5.199}$$

$$= -\mathbf{I} \tag{5.200}$$

where (5.199) is due to the third part of Lemma 5.12, and (5.200) is a result of the second part of Corollary 5.3. Using (5.200) in (5.196) gives

$$\mathbf{0} \preceq \mathbf{J}(\mathbf{X}|\mathbf{U}) - \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} - \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \tag{5.201}$$

which concludes the proof.

For the equality case, consider the conditional Gaussian distribution

$$f(\mathbf{x}|\mathbf{u}) = C\exp\left(-\frac{1}{2}\big(\mathbf{x}-E\left[\mathbf{X}|\mathbf{U}=\mathbf{u}\right]\big)^\top \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\big(\mathbf{x}-E\left[\mathbf{X}|\mathbf{U}=\mathbf{u}\right]\big)\right) \tag{5.202}$$

where C is the normalizing factor. The conditional score function is

$$\boldsymbol{\rho}(\mathbf{x}|\mathbf{u}) = -\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\big(\mathbf{x}-E\left[\mathbf{X}|\mathbf{U}=\mathbf{u}\right]\big) \tag{5.203}$$

which implies $\mathbf{J}(\mathbf{X}|\mathbf{U}) = \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}$. $\square$

We now present the conditional convolution identity which is crucial to extend the second part of Lemma 5.5 to a conditional setting.

Lemma 5.14 (Conditional Convolution Identity) *Let* $\mathbf{X}, \mathbf{Y}, \mathbf{U}$ *be length-n random vectors and let the density for any combination of these random vectors exist. Moreover, let* $\mathbf{X}$ *and* $\mathbf{Y}$ *be conditionally independent given* $\mathbf{U}$*, and let* $\mathbf{W}$ *be defined as* $\mathbf{W} = \mathbf{X} + \mathbf{Y}$*. Then, we have*

$$\boldsymbol{\rho}(\mathbf{w}|\mathbf{u}) = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}=\mathbf{u})|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right] = E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U}=\mathbf{u})|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right] \tag{5.204}$$

The proof of this lemma is given in Appendix 5.9.3. We will use this lemma to prove the conditional Fisher information matrix inequality, i.e., the generalization of the second part of Lemma 5.5.

Lemma 5.15 (Conditional Fisher Information Matrix Inequality) *Let* $\mathbf{X}$, $\mathbf{Y}, \mathbf{U}$ *be as specified in the previous lemma. For any square matrix* $\mathbf{A}$*, we have*

$$\mathbf{J}(\mathbf{X}+\mathbf{Y}|\mathbf{U}) \preceq \mathbf{A}\mathbf{J}(\mathbf{X}|\mathbf{U})\mathbf{A}^{\top} + (\mathbf{I}-\mathbf{A})\,\mathbf{J}(\mathbf{Y}|\mathbf{U})\,(\mathbf{I}-\mathbf{A})^{\top} \tag{5.205}$$

The proof of this lemma is given in Appendix 5.9.4. The following implications of Lemma 5.15 correspond to the conditional version of Corollary 5.2.

Corollary 5.4 *Let* $\mathbf{X}, \mathbf{Y}, \mathbf{U}$ *be as specified in the previous lemma. Then, we have*

1. $\mathbf{J}(\mathbf{X}+\mathbf{Y}|\mathbf{U}) \preceq \mathbf{J}(\mathbf{X}|\mathbf{U})$

2. $\mathbf{J}(\mathbf{X}+\mathbf{Y}|\mathbf{U}) \preceq [\mathbf{J}(\mathbf{X}|\mathbf{U})^{-1}+\mathbf{J}(\mathbf{Y}|\mathbf{U})^{-1}]^{-1}$

Proof: The first part of the corollary can be obtained by setting $\mathbf{A}=\mathbf{I}$ in the previous lemma. For the second part, the selection

$$\mathbf{A} = \left[\mathbf{J}(\mathbf{X}|\mathbf{U})^{-1}+\mathbf{J}(\mathbf{Y}|\mathbf{U})^{-1}\right]^{-1}\mathbf{J}(\mathbf{X}|\mathbf{U})^{-1} \tag{5.206}$$

yields the desired result. □

Using this corollary, one can prove the conditional version of Lemma 5.6 as well:

Lemma 5.16 *Let* $\mathbf{T},\mathbf{U},\mathbf{V}_1,\mathbf{V}_2$ *be random vectors such that* $(\mathbf{T},\mathbf{U})$ *and* $(\mathbf{V}_1,\mathbf{V}_2)$ *are independent. Moreover, let* $\mathbf{V}_1,\mathbf{V}_2$ *be Gaussian random vectors with covariance matrices* $\mathbf{\Sigma}_1,\mathbf{\Sigma}_2$ *such that* $\mathbf{0}\prec\mathbf{\Sigma}_1\preceq\mathbf{\Sigma}_2$*. Then, we have*

$$\mathbf{J}^{-1}(\mathbf{U}+\mathbf{V}_2|\mathbf{T})-\mathbf{\Sigma}_2 \succeq \mathbf{J}^{-1}(\mathbf{U}+\mathbf{V}_1|\mathbf{T})-\mathbf{\Sigma}_1 \tag{5.207}$$

So far, we have proved the conditional versions of the inequalities related to the Fisher information matrix, that were used in the proof of Theorem 5.6. To claim that the proof of Theorem 5.6 can be adapted for Theorem 5.7, we only need the conditional version of Lemma 5.7. In [52], the following result is implicity present.

Lemma 5.17 *Let* $(\mathbf{U},\mathbf{X})$ *be an arbitrarily correlated random vector pair with finite second order moments, and be independent of the random vector* $\mathbf{N}$ *which is zero-*

mean Gaussian with covariance matrix $\mathbf{\Sigma}_N \succ \mathbf{0}$. *Then, we have*

$$\nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}|\mathbf{U}) = \frac{1}{2}\mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U}) \tag{5.208}$$

Proof: Let $F_U(\mathbf{u})$ be the cumulative distribution function of $\mathbf{U}$, and $f(\mathbf{x}+\mathbf{n}|\mathbf{U}=\mathbf{u})$ be the conditional density of $\mathbf{X}+\mathbf{N}$ which is guaranteed to exist because $\mathbf{N}$ is Gaussian. We have

$$\begin{aligned}
&\nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}|\mathbf{U}) \\
&\quad = \nabla_{\mathbf{\Sigma}_N} \int h(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u}) dF_U(\mathbf{u}) && (5.209)\\
&\quad = \int \nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u}) dF_U(\mathbf{u}) && (5.210)\\
&\quad = \frac{1}{2}\int E\left[\nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u}) \nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u})^\top\right] dF_U(\mathbf{u}) && (5.211)\\
&\quad = \frac{1}{2} E\left[\nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U}) \nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U})^\top\right] && (5.212)\\
&\quad = \frac{1}{2}\mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U}) && (5.213)
\end{aligned}$$

where in (5.210), we changed the order of integration and differentiation, which can be done due to the finiteness of the conditional differential entropy, which in turn is ensured by the finite second-order moments of $(\mathbf{U},\mathbf{X})$, (5.211) is a consequence of Lemma 5.7, and (5.213) follows from the definition of the conditional Fisher information matrix. □

Since we have derived all necessary tools, namely conditional counterparts of Lemmas 5.5, 5.6, 5.7 and Corollary 5.2, the proof Theorem 5.6 can be adapted to

prove Theorem 5.7.

5.5.5 Proof of Theorem 5.2 for Arbitrary K

We now prove Theorem 5.2 for arbitrary K. To this end, we will mainly use the intuition gained in the proof of Theorem 5.6 and the tools developed in the previous section. The only new ingredient that is needed is the following lemma whose proof is given in Appendix 5.9.5.

Lemma 5.18 *Let* $(\mathbf{V}, \mathbf{U}, \mathbf{X})$ *be length-n random vectors with well-defined densities. Moreover, assume that the partial derivatives of* $f(\mathbf{u}|\mathbf{v}, \mathbf{x})$ *with respect to* x_i, $i = 1, \ldots, n$, *exist and satisfy*

$$\max_{1 \leq i \leq n} \left| \frac{\partial f(\mathbf{u}|\mathbf{x}, \mathbf{v})}{\partial x_i} \right| \leq g(\mathbf{u}) \tag{5.214}$$

for some integrable function $g(\mathbf{u})$. *Then, if* $(\mathbf{V}, \mathbf{U}, \mathbf{X})$ *satisfy the Markov chain* $\mathbf{V} \to \mathbf{U} \to \mathbf{X}$, *we have*

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathbf{J}(\mathbf{X}|\mathbf{V}) \tag{5.215}$$

We now start the proof of Theorem 5.2 for arbitrary K. First, we rewrite the bound given in Theorem 5.1 for the Kth user's secrecy rate as follows

$$
\begin{aligned}
&I(U_K;\mathbf{Y}_K) - I(U_K;\mathbf{Z}) \\
&\quad = I(\mathbf{X};\mathbf{Y}_K) - I(\mathbf{X};\mathbf{Z}) - [I(\mathbf{X};\mathbf{Y}_K|U_K) - I(\mathbf{X};\mathbf{Z}|U_K)] && (5.216)\\
&\quad \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_K|}{|\mathbf{\Sigma}_K|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} - [I(\mathbf{X};\mathbf{Y}_K|U_K) - I(\mathbf{X};\mathbf{Z}|U_K)] && (5.217)
\end{aligned}
$$

where in (5.216), we used the Markov chain $U_K \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}_K, \mathbf{Z})$, and obtained (5.217) using the worst additive noise lemma given in Lemma 5.4. Moreover, using the Markov chain $U_K \rightarrow \mathbf{X} \rightarrow \mathbf{Y}_K \rightarrow \mathbf{Z}$, the other difference term in (5.217) can be bounded as follows.

$$
\begin{aligned}
0 \leq I(\mathbf{X};\mathbf{Y}_K|U_K) - I(\mathbf{X};\mathbf{Z}|U_K) &\leq I(\mathbf{X};\mathbf{Y}_K) - I(\mathbf{X};\mathbf{Z}) && (5.218)\\
&\leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_K|}{|\mathbf{\Sigma}_K|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (5.219)
\end{aligned}
$$

The proofs of Theorems 5.6 and 5.7 reveal that for any value of $I(\mathbf{X};\mathbf{Y}_K|U_K) - I(\mathbf{X};\mathbf{Z}|U_K)$ in the range given in (5.219), there exists positive semi-definite matrix $\tilde{\mathbf{K}}_K$ such that

$$
\mathbf{J}(\mathbf{X}+\mathbf{N}_K|U_K)^{-1} - \mathbf{\Sigma}_K \preceq \tilde{\mathbf{K}}_K \preceq \mathbf{S} \tag{5.220}
$$

and

$$I(\mathbf{X};\mathbf{Y}_K|U_K) - I(\mathbf{X};\mathbf{Z}|U_K) = \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_K|}{|\mathbf{\Sigma}_K|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (5.221)$$

$$I(\mathbf{X};\mathbf{Y}_{K-1}|U_K) - I(\mathbf{X};\mathbf{Z}|U_K) \leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (5.222)$$

Using (5.221) in (5.217) yields the desired bound on the Kth user's secrecy rate as follows

$$R_K \leq \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_K|}{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_K|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|} \quad (5.223)$$

We now bound the $(K-1)$th user's secrecy rate. To this end, first note that

$$R_{K-1} \leq I(U_{K-1};\mathbf{Y}_{K-1}|U_K) - I(U_{K-1};\mathbf{Z}|U_K) \quad (5.224)$$

$$= I(\mathbf{X};\mathbf{Y}_{K-1}|U_K) - I(\mathbf{X};\mathbf{Z}|U_K) - [I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1})] \quad (5.225)$$

$$\leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} - [I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1})] \quad (5.226)$$

where in order to obtain (5.225), we used the Markov chain $U_K \to U_{K-1} \to \mathbf{X} \to (\mathbf{Y}_{K-1}, \mathbf{Z})$, and (5.226) comes from (5.222). Using the Markov chain $U_K \to U_{K-1} \to$

$\mathbf{X} \to \mathbf{Y}_{K-1} \to \mathbf{Z}$, the mutual information difference in (5.226) is bounded as

$$0 \leq I(\mathbf{X}; \mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) \tag{5.227}$$

$$\leq I(\mathbf{X}; \mathbf{Y}_{K-1}|U_K) - I(\mathbf{X}; \mathbf{Z}|U_K) \tag{5.228}$$

$$\leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{5.229}$$

Using the analysis carried out in the proof of Theorem 5.6, we can get a more refined lower bound as follows

$$\begin{aligned} &I(\mathbf{X}; \mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) \\ &\geq \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1}|}{|\mathbf{\Sigma}_{K-1}|} - \frac{1}{2}\log\ \frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{5.230}$$

Combining (5.229) and (5.230) yields

$$\begin{aligned} &\frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1}|}{|\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_{K-1}|} \\ &\qquad \leq I(\mathbf{X}; \mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) + \frac{1}{2}\log\frac{|\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|} \\ &\qquad \leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_{K-1}|}{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|} \end{aligned} \tag{5.231}$$

Now, using the lower bound on $\tilde{\mathbf{K}}_K$ given in (5.220), we get

$$\tilde{\mathbf{K}}_K \succeq \mathbf{J}(\mathbf{X} + \mathbf{N}_K|U_K)^{-1} - \mathbf{\Sigma}_K \tag{5.232}$$

$$\succeq \mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_K)^{-1} - \mathbf{\Sigma}_{K-1} \tag{5.233}$$

where (5.233) is obtained using Lemma 5.6. Moreover, since we have $U_K \to U_{K-1} \to \mathbf{X} + \mathbf{N}_{K-1}$, the following order exists

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1}) \succeq \mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_K) \tag{5.234}$$

due to Lemma 5.18. Equation (5.234) is equivalent to

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} \preceq \mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_K)^{-1} \tag{5.235}$$

using which in (5.233), we get

$$\tilde{\mathbf{K}}_K \succeq \mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} - \mathbf{\Sigma}_{K-1} \tag{5.236}$$

We now consider the function

$$r(t) = \frac{1}{2} \log \frac{|\mathbf{A} + \mathbf{B} + t\mathbf{\Delta}|}{|\mathbf{A} + t\mathbf{\Delta}|}, \quad 0 \leq t \leq 1 \tag{5.237}$$

with the following parameters

$$\mathbf{A} = \mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} \tag{5.238}$$

$$\mathbf{B} = \mathbf{\Sigma}_Z - \mathbf{\Sigma}_{K-1} \tag{5.239}$$

$$\mathbf{\Delta} = \tilde{\mathbf{K}}_K + \mathbf{\Sigma}_{K-1} - \mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} \tag{5.240}$$

where $\mathbf{\Delta} \succeq \mathbf{0}$ due to (5.236). Using this function, we can paraphrase the bound in (5.231) as

$$-r(0) \leq I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1}) + \frac{1}{2}\log\frac{|\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|} \leq -r(1) \tag{5.241}$$

As shown in Lemma 5.10, $r(t)$ is continuous and monotonically decreasing in t. Thus, there exists a t^* such that

$$-r(t^*) = I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1}) + \frac{1}{2}\log\frac{|\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|} \tag{5.242}$$

due to the intermediate value theorem. Let $\tilde{\mathbf{K}}_{K-1} = \mathbf{A} + t^*\mathbf{\Delta} - \mathbf{\Sigma}_{K-1}$, then we get

$$I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1}) = \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{5.243}$$

We note that using (5.243) in (5.226) yields the desired bound on the $(K-1)$th user's secrecy rate as follows

$$R_{K-1} \leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_{K-1}|}{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_{K-1}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|}{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_Z|} \tag{5.244}$$

Moreover, since $\mathbf{\Delta} \succeq \mathbf{0}$ and $0 \leq t \leq 1$, $\tilde{\mathbf{K}}_{K-1} = \mathbf{A} + t^*\mathbf{\Delta} - \mathbf{\Sigma}_{K-1}$ satisfies the following orderings

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} - \mathbf{\Sigma}_{K-1} \preceq \tilde{\mathbf{K}}_{K-1} \preceq \tilde{\mathbf{K}}_K \tag{5.245}$$

Furthermore, the lower bound in (5.245) implies the following order

$$\tilde{\mathbf{K}}_{K-1} \succeq \mathbf{J}(\mathbf{X}+\mathbf{N}|U_{K-1})^{-1} - \boldsymbol{\Sigma}_N \tag{5.246}$$

for any Gaussian random vector $\mathbf{N}$ such that $\boldsymbol{\Sigma}_N \preceq \boldsymbol{\Sigma}_{K-1}$, and is independent of $U_{K-1}, \mathbf{X}$, which is a consequence of Lemma 5.6. Using (5.246), and following the proof of Theorem 5.6, we can show that

$$I(\mathbf{X};\mathbf{Y}_{K-2}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1}) \leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1}+\boldsymbol{\Sigma}_{K-2}|}{|\boldsymbol{\Sigma}_{K-2}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1}+\boldsymbol{\Sigma}_{Z}|}{|\boldsymbol{\Sigma}_{Z}|} \tag{5.247}$$

Thus, as a recap, we have showed that there exists $\tilde{\mathbf{K}}_{K-1}$ such that

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1} - \boldsymbol{\Sigma}_{K-1} \preceq \tilde{\mathbf{K}}_{K-1} \preceq \tilde{\mathbf{K}}_{K} \tag{5.248}$$

and

$$I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1}) = \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1}+\boldsymbol{\Sigma}_{K-1}|}{|\boldsymbol{\Sigma}_{K-1}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1}+\boldsymbol{\Sigma}_{Z}|}{|\boldsymbol{\Sigma}_{Z}|} \tag{5.249}$$

$$I(\mathbf{X};\mathbf{Y}_{K-2}|U_{K-1}) - I(\mathbf{X};\mathbf{Z}|U_{K-1}) \leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1}+\boldsymbol{\Sigma}_{K-2}|}{|\boldsymbol{\Sigma}_{K-2}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_{K-1}+\boldsymbol{\Sigma}_{Z}|}{|\boldsymbol{\Sigma}_{Z}|} \tag{5.250}$$

which are analogous to (5.220), (5.221), (5.222). Thus, proceeding in the same manner, for any selection of the joint distribution $p(u_K)p(u_{K-1}|u_K)\ldots p(\mathbf{x}|u_2)$, we

can show the existence of matrices $\left\{\tilde{\mathbf{K}}_k\right\}_{k=1}^{K+1}$ such that

$$\mathbf{0} = \tilde{\mathbf{K}}_1 \preceq \tilde{\mathbf{K}}_2 \preceq \quad \ldots \quad \preceq \tilde{\mathbf{K}}_K \preceq \tilde{\mathbf{K}}_{K+1} = \mathbf{S} \tag{5.251}$$

and

$$I(\mathbf{X};\mathbf{Y}_k|U_k) - I(\mathbf{X};\mathbf{Z}|U_k) = \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_k|}{|\mathbf{\Sigma}_k|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}, \quad k = 2,\ldots,K \tag{5.252}$$

$$\begin{aligned} I(\mathbf{X};\mathbf{Y}_{k-1}|U_k) - I(\mathbf{X};\mathbf{Z}|U_k) \leq{}& \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_{k-1}|}{|\mathbf{\Sigma}_{k-1}|} \\ & - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}, \quad k = 2,\ldots,K+1 \end{aligned} \tag{5.253}$$

where $U_{K+1} = \phi$. We now define $\mathbf{K}_k = \tilde{\mathbf{K}}_{k+1} - \tilde{\mathbf{K}}_k,\ k = 1,\ldots,K$, which yields $\tilde{\mathbf{K}}_{k+1} = \sum_{i=1}^{k}\mathbf{K}_i$, and in particular, $\mathbf{S} = \sum_{i=1}^{K}\mathbf{K}_i$. Using these new variables in conjunction with (5.252) and (5.253) results in

$$R_k \leq I(U_k;\mathbf{Y}_k|U_{k+1}) - I(U_k;\mathbf{Z}|U_{k+1}) \tag{5.254}$$

$$= I(\mathbf{X};\mathbf{Y}_k|U_{k+1}) - I(\mathbf{X};\mathbf{Z}|U_{k+1}) - [I(\mathbf{X};\mathbf{Y}_k|U_k) - I(\mathbf{X};\mathbf{Z}|U_k)] \tag{5.255}$$

$$\begin{aligned} \leq{}& \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_k\right|}{|\mathbf{\Sigma}_k|} - \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|} \\ & - \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_k\right|}{|\mathbf{\Sigma}_k|} + \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{5.256}$$

$$= \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_k\right|}{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_k\right|} - \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_Z\right|}{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z\right|} \tag{5.257}$$

$$= \frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i + \mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1}\mathbf{K}_i + \mathbf{\Sigma}_k\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right|} \tag{5.258}$$

for $k = 2, \ldots, K$. For $k = 1$, the bound in (5.253), by setting $k = 2$ in the corresponding expression, yields the desired bound on the first user's secrecy rate

$$R_1 \leq I(\mathbf{X}; \mathbf{Y}_1|U_2) - I(\mathbf{X}; \mathbf{Z}|U_2) \tag{5.259}$$

$$\leq \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{5.260}$$

Since for any selection of the joint distribution $p(u_K)p(u_{K-1}|u_K) \ldots p(\mathbf{x}|u_2)$, we can establish the bounds in (5.258) and (5.260) with positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^K$ such that $\mathbf{S} = \sum_{i=1}^K \mathbf{K}_i$, the union of these bounds over such matrices would be an outer bound for the secrecy capacity region, completing the converse proof of Theorem 5.2 for an arbitrary K.

5.6 Aligned Gaussian MIMO Multi-receiver Wiretap Channel

We now consider the aligned Gaussian MIMO multi-receiver wiretap channel, and obtain its secrecy capacity region given in Theorem 5.3. First, we will show the achievability of the secrecy rates in Theorem 5.3 by extending Marton's achievable scheme for broadcast channels [11] to multi-receiver wiretap channels. For that purpose, we will use Theorem 1 of [12], where the authors provided an achievable rate region for Gaussian vector broadcast channels using Marton's achievable scheme in [11]. While using this result, we will combine it with a stochastic encoding scheme for secrecy purposes.

Next, we will provide a converse proof for Theorem 5.3 by using our capacity result for the degraded Gaussian MIMO multi-receiver wiretap channel in Section 5.5

in conjunction with the channel enhancement technique [4]. In particular, to provide a converse proof for Theorem 5.3, we will show that for any point on the boundary of the secrecy capacity region, there exists a degraded channel such that its secrecy capacity region includes the secrecy capacity region of the original channel, and furthermore, the boundaries of these two regions intersect at this specific point. The channel enhancement technique comes into the picture to show the existence of such a degraded channel by explicitly constructing it, and our capacity result for the degraded case is used to obtain the secrecy capacity region of this constructed degraded channel.

5.6.1 Achievability

To show the achievability of the secrecy rates in Theorem 5.3, we mostly rely on the derivation of the dirty-paper coding region for the Gaussian MIMO broadcast channel in [12, Theorem 1]. We employ the achievable scheme in [12] in conjunction with a stochastic encoding scheme due to secrecy concerns. Without loss of generality, we consider the identity permutation, i.e., $\pi(k) = k,\ k = 1, \ldots, K$. Let $(\mathbf{V}_1, \ldots, \mathbf{V}_K)$ be arbitrarily correlated random vectors such that

$$(\mathbf{V}_1, \ldots, \mathbf{V}_K) \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}_1, \ldots, \mathbf{Y}_K, \mathbf{Z}) \tag{5.261}$$

Using these correlated random vectors, we can construct codebooks

$$\left\{ \mathbf{V}_{k,1}^n(W_k, \tilde{W}_k) \right\}_{k=1}^K \tag{5.262}$$

where $W_k \in \left\{1, \ldots, 2^{nR_k}\right\}$, $\tilde{W}_k \in \left\{1, \ldots, 2^{n\tilde{R}_k}\right\}$, $k = 1, \ldots, K$, such that each legitimate receiver can decode the following rates

$$R_k + \tilde{R}_k = \frac{1}{2} \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_k \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k \right|}, \quad k = 1, \ldots, K \tag{5.263}$$

for some positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^{K}$ such that $\sum_{k=1}^{K} \mathbf{K}_k \preceq \mathbf{S}$ [12]. The messages $\left\{\tilde{W}_k\right\}_{k=1}^{K}$ do not carry any information, and their sole purpose is to confuse the eavesdropper. In other words, the purpose of these messages is to make the eavesdropper spend its decoding capability on them, preventing the eavesdropper to decode the confidential messages $\{W_k\}_{k=1}^{K}$. Thus, we need to select the rates of these dummy messages $\left\{\tilde{R}_k\right\}_{k=1}^{K}$ as follows

$$\tilde{R}_k = \frac{1}{2} \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}, \quad k = 1, \ldots, K \tag{5.264}$$

To achieve the rates given in (5.263), $\{\mathbf{V}_k\}_{k=1}^{K}$ should be taken as jointly Gaussian with appropriate covariance matrices. Moreover, it is sufficient to choose $\mathbf{X}$ as a deterministic function of $\{\mathbf{V}_k\}_{k=1}^{K}$, and the resulting unconditional distribution of $\mathbf{X}$ is also Gaussian with covariance matrix $\sum_{k=1}^{K} \mathbf{K}_k$ [12].

To complete the proof, we need to show that the above codebook structure fulfills all of the secrecy constraints in (5.1). To this end, we take a shortcut, by

using the fact that, if a codebook satisfies

$$\lim_{n\to\infty}\frac{1}{n}H(W_1,\ldots,W_K|\mathbf{Z}^n)\geq\sum_{k=1}^{K}R_k \tag{5.265}$$

then it also satisfies all of the remaining secrecy constraints in (5.1) [54]. Thus, we only check (5.265)

$$\begin{aligned}
&\frac{1}{n}H(W_1,\ldots,W_K|\mathbf{Z}^n)=\frac{1}{n}H(W_1,\ldots,W_K,\mathbf{Z}^n)-\frac{1}{n}H(\mathbf{Z}^n) && (5.266)\\
&=\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n,W_1,\ldots,W_K,\mathbf{Z}^n)-\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n|W_1,\ldots,W_K,\mathbf{Z}^n)\\
&\quad-\frac{1}{n}H(\mathbf{Z}^n) && (5.267)\\
&=\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n)+\frac{1}{n}H(W_1,\ldots,W_K,\mathbf{Z}^n|\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n)\\
&\quad-\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n|W_1,\ldots,W_K,\mathbf{Z}^n)-\frac{1}{n}H(\mathbf{Z}^n) && (5.268)\\
&\geq\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n)-\frac{1}{n}I(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n;\mathbf{Z}^n)\\
&\quad-\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n|W_1,\ldots,W_K,\mathbf{Z}^n) && (5.269)
\end{aligned}$$

We will treat each of the three terms in (5.269) separately. Since $(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n)$ can take $2^{n\sum_{k=1}^{K}\left(R_k+\tilde{R}_k\right)}$ values uniformly, for the first term in (5.269), we have

$$\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n)=\sum_{k=1}^{K}R_k+\sum_{k=1}^{K}\tilde{R}_k \tag{5.270}$$

The second term in (5.269) can be bounded as

$$\frac{1}{n} I(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n; \mathbf{Z}^n) \leq I(\mathbf{V}_{1,1}, \ldots, \mathbf{V}_{K,1}; \mathbf{Z}) + \epsilon_n \tag{5.271}$$

$$\leq I(\mathbf{X}; \mathbf{Z}) + \epsilon_n \tag{5.272}$$

$$= \frac{1}{2} \log \frac{\left| \sum_{k=1}^K \mathbf{K}_k + \mathbf{\Sigma}_Z \right|}{|\mathbf{\Sigma}_Z|} + \epsilon_n \tag{5.273}$$

where $\epsilon_n \to 0$ as $n \to \infty$. The first inequality can be shown following [2, Lemma 8], the second inequality follows from the Markov chain in (5.261), and the equality in (5.273) comes from our choice of $\mathbf{X}$, which is Gaussian with covariance matrix $\sum_{k=1}^K \mathbf{K}_k$. We now consider the third term in (5.269). First, we note that given $(W_1 = w_1, \ldots, W_K = w_K)$, $\left(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n\right)$ can take $2^{n \sum_{k=1}^K \tilde{R}_k}$ values, where $\sum_{k=1}^K \tilde{R}_k$ is given by

$$\sum_{k=1}^K \tilde{R}_k = \frac{1}{2} \log \frac{\left| \sum_{k=1}^K \mathbf{K}_k + \mathbf{\Sigma}_Z \right|}{|\mathbf{\Sigma}_Z|} \tag{5.274}$$

using our selection in (5.264). Thus, (5.274) implies that given $(W_1 = w_1, \ldots, W_K = w_K)$, the eavesdropper can decode $\left(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n\right)$ with vanishingly small probability of error. Hence, using Fano's lemma, we get

$$\frac{1}{n} H(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n | W_1, \ldots, W_K, \mathbf{Z}^n) \leq \frac{1}{n} \left[1 + \gamma_n \left(\sum_{k=1}^K \tilde{R}_k \right) \right] \tag{5.275}$$

where $\gamma_n \to 0$ as $n \to \infty$. Thus, plugging (5.270), (5.273) and (5.275) into (5.269)

yields

$$\lim_{n\to\infty}\frac{1}{n}H(W_1,\ldots,W_K|\mathbf{Z}^n)\geq\sum_{k=1}^{K}R_k \tag{5.276}$$

which ensures that the rates

$$R_k=\frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1}\mathbf{K}_i+\mathbf{\Sigma}_k\right|}-\frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|},\quad k=1,\ldots,K \tag{5.277}$$

can be transmitted in perfect secrecy.

5.6.2 Converse

To show the converse, we consider the maximization of the following expression

$$\sum_{k=1}^{K}\mu_k R_k \tag{5.278}$$

where $\mu_k\geq 0,\ k=1,\ldots,K$. We note that the maximum value of (5.278) traces the boundary of the secrecy capacity region, i.e., its maximum value for any non-negative vector $[\mu_1\ \ldots\ \mu_K]$ will give us a point on the boundary of the secrecy capacity region. Let us define $\pi(\cdot)$ to be a one-to-one permutation on $\{1,\ldots,K\}$ such that

$$0\leq\mu_{\pi(1)}\leq\ldots\leq\mu_{\pi(K)} \tag{5.279}$$

Furthermore, let $0 < m \leq K$ of $\{\mu_k\}_{k=1}^K$ be strictly positive, i.e., $\mu_{\pi(1)} = \ldots = \mu_{\pi(K-m)} = 0$, and $\mu_{\pi(K-m+1)} > 0$. We now define another permutation $\pi'(\cdot)$ on the strictly positive elements of $\{\mu_k\}_{k=1}^K$ such that $\pi'(l) = \pi(K-m+l),\ l = 1, \ldots, m$. Then, (5.278) can be expressed as

$$\sum_{k=1}^{K} \mu_k R_k = \sum_{k=1}^{K} \mu_{\pi(k)} R_{\pi(k)} = \sum_{k=1}^{m} \mu_{\pi'(k)} R_{\pi'(k)} \tag{5.280}$$

We will show that

$$\max \sum_{k=1}^{K} \mu_k R_k = \max \sum_{k=1}^{m} \mu_{\pi'(k)} R_{\pi'(k)} \tag{5.281}$$

$$\leq \max \sum_{k=1}^{m} \frac{\mu_{\pi'(k)}}{2} \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_{\pi'(i)} + \mathbf{\Sigma}_{\pi'(k)} \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_{\pi'(i)} + \mathbf{\Sigma}_{\pi'(k)} \right|} - \sum_{k=1}^{m} \frac{\mu_{\pi'(k)}}{2} \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_{\pi'(i)} + \mathbf{\Sigma}_{Z} \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_{\pi'(i)} + \mathbf{\Sigma}_{Z} \right|} \tag{5.282}$$

where the last maximization is over all positive semi-definite matrices $\left\{\mathbf{K}_{\pi'(k)}\right\}_{k=1}^m$ such that $\sum_{k=1}^m \mathbf{K}_{\pi'(k)} \preceq \mathbf{S}$. Since the right hand side of (5.282) is achievable, if we can show that (5.282) holds for any non-negative vector $[\mu_1 \ \ldots \ \mu_K]$, this will complete the proof of Theorem 5.3. To simplify the notation, without loss of generality, we assume that $\pi'(k) = k,\ k = 1, \ldots, m$. This assumption is equivalent to the assumption that $0 < \mu_1 \leq \ldots \leq \mu_m,$ and $\mu_k = 0,\ k = m+1, \ldots, K$.

We now investigate the maximization in (5.282). The objective function in (5.282) is generally non-convex in the covariance matrices $\left\{\mathbf{K}_{\pi'(k)}\right\}_{k=1}^m$ implying that the KKT conditions for this problem are necessary, but not sufficient. Let us

construct the Lagrangian for this optimization problem

$$L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = \sum_{k=1}^m \mu_k R_k^G + \sum_{k=1}^m \mathrm{tr}(\mathbf{K}_k \mathbf{M}_k) + \mathrm{tr}\left(\left(\mathbf{S} - \sum_{k=1}^m \mathbf{K}_k\right)\mathbf{M}_Z\right) \tag{5.283}$$

where the Lagrange multipliers $\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z$ are positive semi-definite matrices, and we defined $\left\{R_k^G\right\}_{k=1}^m$ as follows,

$$R_k^G = \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \ldots, m \tag{5.284}$$

The gradient of $L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right)$ with respect to $\mathbf{K}_j$ for any $j = 1, \ldots, m-1$, is given by

$$\begin{aligned}\nabla_{\mathbf{K}_j} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = &\sum_{k=j}^m \frac{\mu_k}{2}\left(\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_k\right)^{-1} - \sum_{k=j+1}^m \frac{\mu_k}{2}\left(\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k\right)^{-1} \\ &- \sum_{k=j}^m \frac{\mu_k}{2}\left(\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} + \sum_{k=j+1}^m \frac{\mu_k}{2}\left(\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} \\ &+ \mathbf{M}_j - \mathbf{M}_Z\end{aligned} \tag{5.285}$$

and the gradient of $L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right)$ with respect to $\mathbf{K}_m$ is given by

$$\begin{aligned}\nabla_{\mathbf{K}_m} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = &\frac{\mu_m}{2}\left(\sum_{i=1}^m \mathbf{K}_i + \mathbf{\Sigma}_m\right)^{-1} - \frac{\mu_m}{2}\left(\sum_{i=1}^m \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} \\ &+ \mathbf{M}_m - \mathbf{M}_Z\end{aligned} \tag{5.286}$$

The KKT conditions are given by

$$\nabla_{\mathbf{K}_j} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = \mathbf{0}, \quad j = 1, \ldots, m \tag{5.287}$$

$$\operatorname{tr}(\mathbf{K}_j \mathbf{M}_j) = 0, \quad j = 1, \ldots, m \tag{5.288}$$

$$\operatorname{tr}\left(\left(\mathbf{S} - \sum_{k=1}^m \mathbf{K}_k\right)\mathbf{M}_Z\right) = 0 \tag{5.289}$$

We note that since $\operatorname{tr}(\mathbf{K}_j\mathbf{M}_j) = \operatorname{tr}(\mathbf{M}_j\mathbf{K}_j)$, and $\mathbf{M}_j \succeq \mathbf{0}, \mathbf{K}_j \succeq \mathbf{0}$, we have $\mathbf{M}_j\mathbf{K}_j = \mathbf{K}_j\mathbf{M}_j = \mathbf{0}$. Thus, the KKT conditions in (5.288) are equivalent to

$$\mathbf{M}_j\mathbf{K}_j = \mathbf{K}_j\mathbf{M}_j = \mathbf{0}, \quad j = 1, \ldots, m \tag{5.290}$$

Similarly, we also have

$$\mathbf{M}_Z\left(\mathbf{S} - \sum_{k=1}^m \mathbf{K}_k\right) = \left(\mathbf{S} - \sum_{k=1}^m \mathbf{K}_k\right)\mathbf{M}_Z = \mathbf{0} \tag{5.291}$$

Subtracting the gradient of the Lagrangian with respect to $\mathbf{K}_{j+1}$ from the one with respect to $\mathbf{K}_j$, for $j = 1, \ldots, m-1$, we get

$$\begin{aligned}
&\nabla_{\mathbf{K}_j} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) - \nabla_{\mathbf{K}_{j+1}} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) \\
&= \frac{\mu_j}{2}\left(\sum_{i=1}^j \mathbf{K}_i + \mathbf{\Sigma}_j\right)^{-1} - \frac{\mu_{j+1}}{2}\left(\sum_{i=1}^j \mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} \\
&\quad - \frac{\mu_j}{2}\left(\sum_{i=1}^j \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} + \frac{\mu_{j+1}}{2}\left(\sum_{i=1}^j \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} + \mathbf{M}_j - \mathbf{M}_{j+1}
\end{aligned} \tag{5.292}$$

Thus, using (5.290), (5.291), (5.292), we can express the KKT conditions in (5.287),

(5.288), (5.289) as follows

$$\mu_j \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_j \right)^{-1} + (\mu_{j+1} - \mu_j) \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_Z \right)^{-1} + \mathbf{M}_j$$
$$= \mu_{j+1} \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \mathbf{M}_{j+1}, \quad j = 1, \ldots, m-1 \tag{5.293}$$

and

$$\mu_m \left(\sum_{i=1}^{m} \mathbf{K}_i + \mathbf{\Sigma}_m \right)^{-1} + \mathbf{M}_m = \mu_m \left(\sum_{i=1}^{m} \mathbf{K}_i + \mathbf{\Sigma}_Z \right)^{-1} + \mathbf{M}_Z \tag{5.294}$$

$$\mathbf{K}_j \mathbf{M}_j = \mathbf{M}_j \mathbf{K}_j = \mathbf{0}, \qquad j = 1, \ldots, m \tag{5.295}$$

$$\mathbf{M}_Z \left(\mathbf{S} - \sum_{k=1}^{m} \mathbf{K}_k \right) = \left(\mathbf{S} - \sum_{k=1}^{m} \mathbf{K}_k \right) \mathbf{M}_Z = \mathbf{0} \tag{5.296}$$

where we also embed the multiplications by 2 into the Lagrange multipliers.

We now present a lemma which will be instrumental in constructing a degraded Gaussian MIMO multi-receiver wiretap channel, such that the secrecy capacity region of the constructed channel includes the secrecy capacity region of the original channel, and the boundary of the secrecy capacity region of this constructed channel coincides with the boundary of the secrecy capacity region of the original channel at a certain point for a given non-negative vector $[\mu_1 \ \ldots \ \mu_K]$.

Lemma 5.19 *Given the covariance matrices $\{\mathbf{K}_j\}_{j=1}^m$ satisfying the KKT conditions given in (5.293)-(5.296), there exist noise covariance matrices $\left\{\tilde{\mathbf{\Sigma}}_j\right\}_{j=1}^m$ such that*

1. $\tilde{\mathbf{\Sigma}}_j \preceq \mathbf{\Sigma}_j, \ j = 1, \ldots, m.$

2. $\mathbf{0} \prec \tilde{\mathbf{\Sigma}}_1 \preceq \ldots \preceq \tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$

3. $\mu_j \left(\sum_{i=1}^{j} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_j\right)^{-1} + (\mu_{j+1} - \mu_j) \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1}$

$$= \mu_{j+1} \left(\sum_{i=1}^{j} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1}, \quad \textit{for } j = 1, \ldots, m-1,$$

and

$$\mu_m \left(\sum_{i=1}^{m} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} = \mu_m \big(\sum_{i=1}^{m} \mathbf{K}_i + \mathbf{\Sigma}_Z\big)^{-1} + \mathbf{M}_Z$$

4. $\left(\sum_{i=1}^{j} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_j\right)^{-1} \left(\sum_{i=1}^{j-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_j\right) = \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_j\right)^{-1} \left(\sum_{i=1}^{j-1} \mathbf{K}_i + \mathbf{\Sigma}_j\right)$

for $j = 1, \ldots, m$

5. $\left(\mathbf{S} + \tilde{\mathbf{\Sigma}}_m\right) \left(\sum_{i=1}^{m} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} = \left(\mathbf{S} + \mathbf{\Sigma}_Z\right) \left(\sum_{i=1}^{m} \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1}$

The proof of this lemma is given in Appendix 5.9.6.

Without loss of generality, we have already fixed $[\mu_1 \ \ldots \ \mu_K]$ such that $0 < \mu_1 \leq \ldots \leq \mu_m$, and $\mu_k = 0, \ k = m+1, \ldots, K$ for some $0 < m \leq K$. For this fixed $[\mu_1 \ \ldots \ \mu_K]$, assume that $\{\mathbf{K}_k^*\}_{k=1}^m$ achieves the maximum of (5.282). Since these covariance matrices need to satisfy the KKT conditions given in (5.293)-(5.296), Lemma 5.19 ensures the existence of the covariance matrices $\left\{\tilde{\mathbf{\Sigma}}_j\right\}_{j=1}^m$ that have the properties listed in Lemma 5.19. Thus, we can define a degraded Gaussian MIMO multi-receiver wiretap channel that has the following noise covariance matrices

$$\hat{\mathbf{\Sigma}}_k = \begin{cases} \tilde{\mathbf{\Sigma}}_k, & 1 \leq k \leq m \\ \alpha_{k-m} \tilde{\mathbf{\Sigma}}_1, & m+1 \leq k \leq K \end{cases} \tag{5.297}$$

where $0 < \alpha_{k-m} \leq 1$ are chosen to satisfy $\alpha_{k-m} \tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_k$ for $k = m+1, \ldots, K$, where the existence of such $\{\alpha_{k-m}\}_{k=m+1}^K$ are ensured by the positive definiteness

of $\{\mathbf{\Sigma}_k\}_{k=1}^K$. The noise covariance matrix of the eavesdropper is the same as in the original channel, i.e., $\mathbf{\Sigma}_Z$. Since this channel is degraded, its secrecy capacity region is given by Theorem 5.2. Moreover, since $\hat{\mathbf{\Sigma}}_k \preceq \mathbf{\Sigma}_k,\ k = 1, \ldots, K$, and the noise covariance matrices in the constructed degraded channel and the original channel are the same, the secrecy capacity region of this degraded channel outer bounds that of the original channel. Next, we show that for the so-far fixed $[\mu_1\ \ldots\ \mu_K]$, the boundaries of these two regions intersect at this point. For this purpose, reconsider the maximization problem in (5.278)

$$\max \sum_{k=1}^{K} \mu_k R_k = \max \sum_{k=1}^{m} \mu_k R_k \tag{5.298}$$

$$\leq \max_{\substack{\mathbf{K}_i \succeq 0,\ i=1,\ldots,K \\ \sum_{i=1}^K \mathbf{K}_i \preceq \mathbf{S}}} \sum_{k=1}^{m} \frac{\mu_k}{2} \left[\log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k \right|} - \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|} \right] \tag{5.299}$$

$$= \max_{\substack{\mathbf{K}_i \succeq 0,\ i=1,\ldots,m \\ \sum_{i=1}^m \mathbf{K}_i \preceq \mathbf{S}}} \sum_{k=1}^{m} \frac{\mu_k}{2} \left[\log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k \right|} - \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|} \right] \tag{5.300}$$

where (5.298) is implied by the fact that for the fixed $[\mu_1\ \ldots\ \mu_K]$, we assumed that $\mu_k = 0,\ k = m+1, \ldots, K$ and $0 < \mu_1 \leq \ldots \leq \mu_m$, (5.299) follows from the facts that the constructed degraded channel includes the secrecy capacity region of the original channel, and the secrecy capacity region of the degraded channel is given by Theorem 5.2. The last equation, i.e., (5.300), comes from the fact

that, since $\mu_k = 0,\ k = m+1, \ldots, K$, there is no loss of optimality in choosing $\mathbf{K}_k = \mathbf{0},\ k = m+1, \ldots, K$. We now claim that the maximum in (5.300) is achieved by $\{\mathbf{K}_k^*\}_{k=1}^m$. To prove this claim, we first define

$$R_k^* = \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \ldots, m \tag{5.301}$$

and

$$\hat{R}_k = \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \ldots, m \tag{5.302}$$

for some arbitrary positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^m$ such that $\sum_{i=1}^m \mathbf{K}_i \preceq \mathbf{S}$. To prove that the maximum in (5.300) is achieved by $\{\mathbf{K}_k^*\}_{k=1}^m$, we will show that

$$\sum_{k=1}^m \mu_k R_k^* - \sum_{k=1}^m \mu_k \hat{R}_k \geq 0 \tag{5.303}$$

To this end, consider the first summation in (5.303)

$$\begin{aligned}
\sum_{k=1}^{m}\mu_k R_k^* &= \sum_{k=1}^{m}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\sum_{k=2}^{m}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k-1}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k-1}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} \qquad (5.304)\\
&=\sum_{k=1}^{m}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} \qquad (5.305)\\
&=\frac{\mu_m}{2}\log\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|}\\
&\quad+\sum_{k=1}^{m-1}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} \qquad (5.306)\\
&=\frac{\mu_m}{2}\log\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|}+\sum_{k=1}^{m-1}\frac{\mu_k}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|\\
&\quad+\sum_{k=1}^{m-1}\frac{\mu_{k+1}-\mu_k}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|-\sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right|\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} \qquad (5.307)
\end{aligned}$$

Similarly, we have

$$\sum_{k=1}^{m}\mu_k\hat{R}_k = \frac{\mu_m}{2}\log\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|}+\sum_{k=1}^{m-1}\frac{\mu_k}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_k\right| + \sum_{k=1}^{m-1}\frac{\mu_{k+1}-\mu_k}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right| - \sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{k+1}\right| - \frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} \tag{5.308}$$

We define the following matrices

$$\mathbf{\Delta}_k = \sum_{i=1}^{k}\mathbf{K}_i - \sum_{i=1}^{k}\mathbf{K}_i^*, \quad k=1,\ldots,m \tag{5.309}$$

Using (5.307), (5.308) and (5.309), the difference in (5.303) can be expressed as

$$\begin{aligned}\sum_{k=1}^{m}\mu_k R_k^* - \sum_{k=1}^{m}\mu_k\hat{R}_k = {}& \frac{\mu_m}{2}\log\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|} - \frac{\mu_m}{2}\log\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|} \\ & - \sum_{k=1}^{m-1}\frac{\mu_k}{2}\log\left|\mathbf{I}+\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right)^{-1}\mathbf{\Delta}_k\right| \\ & - \sum_{k=1}^{m-1}\frac{\mu_{k+1}-\mu_k}{2}\log\left|\mathbf{I}+\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right)^{-1}\mathbf{\Delta}_k\right| \\ & + \sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\log\left|\mathbf{I}+\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right)^{-1}\mathbf{\Delta}_k\right|\end{aligned} \tag{5.310}$$

We first note that

$$\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|} = \frac{\left|\mathbf{S}+\tilde{\mathbf{\Sigma}}_m\right|}{|\mathbf{S}+\mathbf{\Sigma}_Z|} \geq \frac{\left|\sum_{i=1}^{m}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right|} \tag{5.311}$$

where the equality is due to the fifth part of Lemma 5.19, and the inequality follows from the fact that the function

$$\frac{\left|\mathbf{A}+\tilde{\mathbf{\Sigma}}_m\right|}{|\mathbf{A}+\mathbf{\Sigma}_Z|} \tag{5.312}$$

is monotonically increasing in the positive semi-definite matrix $\mathbf{A}$ as can be deduced from (5.107), and that $\sum_{i=1}^{m}\mathbf{K}_i \preceq \mathbf{S}$. Furthermore, we have

$$\begin{aligned}
&\frac{\mu_k}{\mu_{k+1}}\log\left|\mathbf{I}+\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right)^{-1}\mathbf{\Delta}_k\right|+\frac{\mu_{k+1}-\mu_k}{\mu_{k+1}}\log\left|\mathbf{I}+\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right)^{-1}\mathbf{\Delta}_k\right| \\
&\leq \log\left|\mathbf{I}+\frac{\mu_k}{\mu_{k+1}}\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right)^{-1}\mathbf{\Delta}_k+\frac{\mu_{k+1}-\mu_k}{\mu_{k+1}}\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right)^{-1}\mathbf{\Delta}_k\right| \qquad (5.313) \\
&= \log\left|\mathbf{I}+\left(\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right)^{-1}\mathbf{\Delta}_k\right| \qquad (5.314)
\end{aligned}$$

where the inequality in (5.313) follows from the concavity of $\log|\cdot|$ in positive semi-definite matrices, and (5.314) follows from the third part of Lemma 5.19. Using (5.311) and (5.314) in (5.310) yields

$$\sum_{k=1}^{m}\mu_k R_k^* - \sum_{k=1}^{m}\mu_k\hat{R}_k \geq 0 \tag{5.315}$$

which implies that the maximum in (5.300) is achieved by $\{\mathbf{K}_k^*\}_{k=1}^{m}$. Thus, using

this fact in (5.300), we get

$$\max \sum_{k=1}^{K} \mu_k R_k \leq \sum_{k=1}^{m} \frac{\mu_k}{2} \left[\log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k \right|} - \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i^* + \mathbf{\Sigma}_Z \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_Z \right|} \right] \tag{5.316}$$

$$= \sum_{k=1}^{m} \frac{\mu_k}{2} \left[\log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i^* + \mathbf{\Sigma}_k \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_k \right|} - \log \frac{\left| \sum_{i=1}^{k} \mathbf{K}_i^* + \mathbf{\Sigma}_Z \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_Z \right|} \right] \tag{5.317}$$

where the equality follows from the fourth part of Lemma 5.19. Since the right hand side of (5.317) is achievable, and we can get a similar outer bound for any non-negative vector $[\mu_1 \ \dots \ \mu_K]$, this completes the converse proof for the aligned Gaussian MIMO channel.

5.7 General Gaussian MIMO Multi-receiver Wiretap Channel

In this final part of the chapter, we consider the general Gaussian multi-receiver wiretap channel and obtain its secrecy capacity region given in Theorem 5.4. The main idea in this section is to construct an aligned channel that is indexed by a scalar variable, and then show that this aligned channel has the same secrecy capacity region as the original channel in the limit of this indexing parameter on the constructed aligned channel. This argument was previously used in [4, 21]. The way we use this argument here is different from [4] because there are no secrecy constraints in [4], and it is different from [21] because there are multiple legitimate receivers here.

Achievability of the region given in Theorem 5.4 can be shown by following the achievability proof of Theorem 5.3 given in Section 5.6.1, hence it is omitted. For

the converse, we basically use the ideas presented in [4, 21]. Following Section V-B of [4], we can construct an equivalent channel which has the same secrecy capacity region as the original channel defined in (5.19)-(5.20). In this constructed equivalent channel, all receivers, including the eavesdropper, and the transmitter have the same number of antennas, which is t,

$$\hat{\mathbf{Y}}_k = \hat{\mathbf{H}}_k \mathbf{X} + \hat{\mathbf{N}}_k, \quad k = 1, \ldots, K \tag{5.318}$$

$$\hat{\mathbf{Z}} = \hat{\mathbf{H}}_Z \mathbf{X} + \hat{\mathbf{N}}_Z \tag{5.319}$$

where $\hat{\mathbf{H}}_k = \hat{\mathbf{\Lambda}}_k \mathbf{V}_k$, $\mathbf{V}_k$ is a $t \times t$ orthonormal matrix, and $\hat{\mathbf{\Lambda}}_k$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_k)$ diagonal entries are zero, and the rest of the diagonal entries are strictly positive. Here, $\hat{r}_k$ is the rank of the original channel gain matrix, $\mathbf{H}_k$. The noise covariance matrix of the Gaussian random vector $\hat{\mathbf{N}}_k$ is given by $\hat{\mathbf{\Sigma}}_k$ which has the following block diagonal form

$$\hat{\mathbf{\Sigma}}_k = \begin{bmatrix} \hat{\mathbf{\Sigma}}_k^A & \mathbf{0} \\ \mathbf{0} & \hat{\mathbf{\Sigma}}_k^B \end{bmatrix} \tag{5.320}$$

where $\hat{\mathbf{\Sigma}}_k^A$ is of size $(t - \hat{r}_k) \times (t - \hat{r}_k)$, and $\hat{\mathbf{\Sigma}}_k^B$ is of size $\hat{r}_k \times \hat{r}_k$.

Similar notations hold for the eavesdropper's observation $\hat{\mathbf{Z}}$ as well. In particular, $\hat{\mathbf{H}}_Z = \hat{\mathbf{\Lambda}}_Z \mathbf{V}_Z$ where $\mathbf{V}_Z$ is a $t \times t$ orthonormal matrix, and $\hat{\mathbf{\Lambda}}_Z$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_Z)$ diagonal entries are zero, and the rest of the diagonal entries are strictly positive. Here, $\hat{r}_Z$ is the rank of the original channel gain matrix of the eavesdropper, $\mathbf{H}_Z$. The covariance matrix of the Gaussian random vector $\hat{\mathbf{N}}_Z$

is given by $\hat{\mathbf{\Sigma}}_Z$ which has the following block diagonal form

$$\hat{\mathbf{\Sigma}}_Z = \begin{bmatrix} \hat{\mathbf{\Sigma}}_Z^A & \mathbf{0} \\ \mathbf{0} & \hat{\mathbf{\Sigma}}_Z^B \end{bmatrix} \tag{5.321}$$

where $\hat{\mathbf{\Sigma}}_Z^A$ is of size $(t-\hat{r}_Z)\times(t-\hat{r}_Z)$ and $\hat{\mathbf{\Sigma}}_Z^B$ is of size $\hat{r}_Z \times \hat{r}_Z$. Since this new channel in (5.318)-(5.319) can be constructed from the original channel in (5.19)-(5.20) through invertible transformations [4], both have the same secrecy capacity region. Moreover, these transformations preserve the dirty-paper coding region as well, i.e.,

$$\begin{aligned}
&R_k^{\mathrm{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right) \\
&= \frac{1}{2}\log\frac{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|}{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\mathbf{H}_Z\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|}{\left|\mathbf{H}_Z\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|} \\
&= \frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^\top + \hat{\mathbf{\Sigma}}_{\pi(k)}\right|}{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^\top + \hat{\mathbf{\Sigma}}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_Z\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_Z^\top + \hat{\mathbf{\Sigma}}_Z\right|}{\left|\hat{\mathbf{H}}_Z\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_Z^\top + \hat{\mathbf{\Sigma}}_Z\right|}, \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad k = 1,\ldots,K
\end{aligned} \tag{5.322}$$

We now define another channel which does not have the same secrecy capacity region or the dirty paper coding region as the original channel:

$$\bar{\mathbf{Y}}_k = \bar{\mathbf{H}}_k\mathbf{X} + \hat{\mathbf{N}}_k, \quad k = 1,\ldots,K \tag{5.323}$$

$$\bar{\mathbf{Z}} = \bar{\mathbf{H}}_Z\mathbf{X} + \hat{\mathbf{N}}_Z \tag{5.324}$$

where $\bar{\mathbf{H}}_k = \left(\hat{\mathbf{\Lambda}}_k + \alpha\hat{\mathbf{I}}_k\right)\mathbf{V}_k$ and $\alpha > 0$, and $\hat{\mathbf{I}}_k$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_k)$ diagonal entries are 1, and the rest of the diagonal entries are zero. Similarly, $\bar{\mathbf{H}}_Z = \left(\hat{\mathbf{\Lambda}}_Z + \alpha\hat{\mathbf{I}}_Z\right)\mathbf{V}_Z$, where $\hat{\mathbf{I}}_Z$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_Z)$ diagonal entries are 1, and the rest are zero. We note that $\{\bar{\mathbf{H}}_k\}_{k=1}^K, \bar{\mathbf{H}}_Z$ are invertible, hence the channel defined by (5.323)-(5.324) can be considered as an aligned Gaussian MIMO multi-receiver wiretap channel. Thus, since it is an aligned Gaussian MIMO multi-receiver wiretap channel, its secrecy capacity region is given by Theorem 5.3.

We now show that as $\alpha \to 0$, the secrecy capacity region of the channel described by (5.323)-(5.324) converges to a region that includes the secrecy capacity region of the original channel in (5.19)-(5.20). Since the original channel in (5.19)-(5.20) and the channel in (5.318)-(5.319) have the same secrecy capacity region and the dirty-paper coding region, checking that the secrecy capacity region of the channel described by (5.323)-(5.324) converges, as $\alpha \to 0$, to a region that includes the secrecy capacity region of the channel described by (5.318)-(5.319), is sufficient. To this end, consider an arbitrary $(2^{nR_1}, \ldots, 2^{nR_K}, n)$ code which can be transmitted with vanishingly small probability of error and in perfect secrecy when it is used in the channel given in (5.318)-(5.319). We will show that the same code can also be transmitted with vanishingly small probability of error and in perfect secrecy when it is used in the channel given in (5.323)-(5.324) as $\alpha \to 0$. This will imply that the secrecy capacity region of the channel given in (5.323)-(5.324) converges to a region that includes the secrecy capacity region of the channel given in (5.318)-(5.319). We

first note that

$$\bar{\mathbf{Y}}_k = \left(\hat{\mathbf{\Lambda}}_k + \alpha\hat{\mathbf{I}}_k\right)\mathbf{V}_k\mathbf{X} + \hat{\mathbf{N}}_k \tag{5.325}$$

$$= \begin{bmatrix} \alpha\hat{\mathbf{I}}_k^A\mathbf{V}_k\mathbf{X} \\ \\ \hat{\mathbf{\Lambda}}_k^B\mathbf{V}_k\mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_k^A \\ \\ \hat{\mathbf{N}}_k^B \end{bmatrix} \tag{5.326}$$

$$= \begin{bmatrix} \bar{\mathbf{Y}}_k^A \\ \\ \bar{\mathbf{Y}}_k^B \end{bmatrix}, \qquad k = 1, \ldots, K \tag{5.327}$$

where $\hat{\mathbf{I}}_k^A$ contains the first $(t - \hat{r}_k)$ rows of $\hat{\mathbf{I}}_k$, and $\hat{\mathbf{\Lambda}}_k^B$ contains the last $\hat{r}_k$ rows of $\hat{\mathbf{\Lambda}}_k$. $\hat{\mathbf{N}}_k^A$ is a Gaussian random vector that contains the first $(t - \hat{r}_k)$ entries of $\hat{\mathbf{N}}_k$, and $\hat{\mathbf{N}}_k^B$ is a vector that contains the last $\hat{r}_k$ entries. The covariance matrices of $\hat{\mathbf{N}}_k^A, \hat{\mathbf{N}}_k^B$ are $\hat{\mathbf{\Sigma}}_k^A, \hat{\mathbf{\Sigma}}_k^B$, respectively, and $\hat{\mathbf{N}}_k^A$ and $\hat{\mathbf{N}}_k^B$ are independent as can be observed through (5.320). Similarly, we can write

$$\hat{\mathbf{Y}}_k = \hat{\mathbf{\Lambda}}_k\mathbf{V}_k\mathbf{X} + \hat{\mathbf{N}}_k \tag{5.328}$$

$$= \begin{bmatrix} \mathbf{0} \\ \\ \hat{\mathbf{\Lambda}}_k^B\mathbf{V}_k\mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_k^A \\ \\ \hat{\mathbf{N}}_k^B \end{bmatrix} \tag{5.329}$$

$$= \begin{bmatrix} \hat{\mathbf{Y}}_k^A \\ \\ \hat{\mathbf{Y}}_k^B \end{bmatrix}, \qquad k = 1, \ldots, K \tag{5.330}$$

We note that $\bar{\mathbf{Y}}_k^B = \hat{\mathbf{Y}}_k^B,\ k = 1, \ldots, K$, thus we have

$$\mathbf{X} \to \bar{\mathbf{Y}}_k \to \hat{\mathbf{Y}}_k, \quad k = 1, \ldots, K \tag{5.331}$$

which ensures the any message rate that is decodable by the kth user of the channel given in (5.318)-(5.319) is also decodable by the kth user of the channel given in (5.323)-(5.324). Thus, any $(2^{nR_1}, \ldots, 2^{nR_K}, n)$ code which can be transmitted with vanishingly small probability of error in the channel defined by (5.318)-(5.319) can be transmitted with vanishingly small probability of error in the channel defined by (5.323)-(5.324) as well.

We now check the secrecy constraints. To this end, we note that

$$\bar{\mathbf{Z}} = \left(\hat{\mathbf{\Lambda}}_Z + \alpha \hat{\mathbf{I}}_Z\right) \mathbf{V}_Z \mathbf{X} + \hat{\mathbf{N}}_Z \tag{5.332}$$

$$= \begin{bmatrix} \alpha \hat{\mathbf{I}}_Z^A \mathbf{V}_Z \mathbf{X} \\ \hat{\mathbf{\Lambda}}_Z^B \mathbf{V}_Z \mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_Z^A \\ \hat{\mathbf{N}}_Z^B \end{bmatrix} \tag{5.333}$$

$$= \begin{bmatrix} \bar{\mathbf{Z}}^A \\ \bar{\mathbf{Z}}^B \end{bmatrix} \tag{5.334}$$

where $\hat{\mathbf{I}}_Z^A$ contains the first $(t - \hat{r}_Z)$ rows of $\hat{\mathbf{I}}_Z$, and $\hat{\mathbf{\Lambda}}_Z^B$ contains the last $\hat{r}_Z$ rows of $\hat{\mathbf{\Lambda}}_Z$. $\hat{\mathbf{N}}_Z^A$ is a Gaussian random vector that contains the first $t - \hat{r}_Z$ entries of $\hat{\mathbf{N}}_Z$, and $\hat{\mathbf{N}}_Z^B$ is a vector that contains the last $\hat{r}_Z$ entries. The covariance matrices of $\hat{\mathbf{N}}_Z^A, \hat{\mathbf{N}}_Z^B$ are $\hat{\mathbf{\Sigma}}_Z^A, \hat{\mathbf{\Sigma}}_Z^B$, respectively, and $\hat{\mathbf{N}}_Z^A$ and $\hat{\mathbf{N}}_Z^B$ are independent as can be

observed through (5.321). Similarly, we can write

$$\hat{\mathbf{Z}} = \hat{\mathbf{\Lambda}}_Z \mathbf{V}_Z \mathbf{X} + \hat{\mathbf{N}}_Z \tag{5.335}$$

$$= \begin{bmatrix} \mathbf{0} \\ \hat{\mathbf{\Lambda}}_Z^B \mathbf{V}_Z \mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_Z^A \\ \hat{\mathbf{N}}_Z^B \end{bmatrix} \tag{5.336}$$

$$= \begin{bmatrix} \hat{\mathbf{Z}}^A \\ \hat{\mathbf{Z}}^B \end{bmatrix} \tag{5.337}$$

We note that $\bar{\mathbf{Z}}^B = \hat{\mathbf{Z}}^B$, and thus we have

$$\mathbf{X} \to \bar{\mathbf{Z}} \to \hat{\mathbf{Z}} \tag{5.338}$$

We now show that any $(2^{nR_1}, \ldots, 2^{nR_K})$ code that achieves the perfect secrecy rates $(R_1, \ldots,$

$R_K)$ in the channel given in (5.318)-(5.319) also achieves the same perfect secrecy rates in the channel given in (5.323)-(5.324) when $\alpha \to 0$. To this end, let $\mathcal{S}$ be a non-empty subset of $\{1, \ldots, K\}$. We consider the following equivocation

$$H(W_{\mathcal{S}}|\bar{\mathbf{Z}}^n) = H(W_{\mathcal{S}}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^n) \tag{5.339}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) + I(W_{\mathcal{S}}; \hat{\mathbf{Z}}^n) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^n) \tag{5.340}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) + I(W_{\mathcal{S}}; \hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^{A,n}, \bar{\mathbf{Z}}^{B,n}) \tag{5.341}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) + I(W_{\mathcal{S}}; \hat{\mathbf{Z}}^{B,n}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) \tag{5.342}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^{A,n}|\hat{\mathbf{Z}}^{B,n}) \tag{5.343}$$

where (5.342) follows from the facts that $W_{\mathcal{S}}$ and $\hat{\mathbf{Z}}^{A,n} = \hat{\mathbf{N}}^{A,n}$ are independent, and $\bar{\mathbf{Z}}^{B,n} = \hat{\mathbf{Z}}^{B,n}$. We now bound the mutual information term in (5.343)

$$
\begin{aligned}
I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^{A,n} | \hat{\mathbf{Z}}^{B,n}) &\leq I(\mathbf{X}^n; \bar{\mathbf{Z}}^{A,n} | \hat{\mathbf{Z}}^{B,n}) && (5.344)\\
&= h(\bar{\mathbf{Z}}^{A,n} | \hat{\mathbf{Z}}^{B,n}) - h(\bar{\mathbf{Z}}^{A,n} | \hat{\mathbf{Z}}^{B,n}, \mathbf{X}^n) && (5.345)\\
&= h(\bar{\mathbf{Z}}^{A,n} | \hat{\mathbf{Z}}^{B,n}) - h(\bar{\mathbf{Z}}^{A,n} | \mathbf{X}^n) && (5.346)\\
&\leq h(\bar{\mathbf{Z}}^{A,n}) - h(\bar{\mathbf{Z}}^{A,n} | \mathbf{X}^n) && (5.347)\\
&= I(\mathbf{X}^n; \bar{\mathbf{Z}}^{A,n}) && (5.348)\\
&\leq \sum_{i=1}^{n} I(\mathbf{X}_i; \bar{\mathbf{Z}}_i^A) && (5.349)\\
&\leq \sum_{i=1}^{n} \max_{E\left[\mathbf{X}_i \mathbf{X}_i^\top\right] \preceq \mathbf{S}} I(\mathbf{X}_i; \bar{\mathbf{Z}}_i^A) && (5.350)\\
&\leq \sum_{i=1}^{n} \frac{1}{2} \log \frac{\left| \alpha^2 \hat{\mathbf{I}}_Z^A \mathbf{V}_Z \mathbf{S} \mathbf{V}_Z^\top (\hat{\mathbf{I}}_Z^A)^\top + \hat{\mathbf{\Sigma}}_Z^A \right|}{\left| \hat{\mathbf{\Sigma}}_Z^A \right|} && (5.351)\\
&= \frac{n}{2} \log \frac{\left| \alpha^2 \hat{\mathbf{I}}_Z^A \mathbf{V}_Z \mathbf{S} \mathbf{V}_Z^\top (\hat{\mathbf{I}}_Z^A)^\top + \hat{\mathbf{\Sigma}}_Z^A \right|}{\left| \hat{\mathbf{\Sigma}}_Z^A \right|} && (5.352)
\end{aligned}
$$

where (5.344) follows from the Markov chain $W_{\mathcal{S}} \to \mathbf{X}^n \to (\bar{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n})$, (5.346) is due to the Markov chain $\bar{\mathbf{Z}}^{A,n} \to \mathbf{X}^n \to \hat{\mathbf{Z}}^{B,n}$, (5.347) comes from the fact that conditioning cannot increase entropy, (5.349) is a consequence of the fact that channel is memoryless, (5.351) is due to the fact that subject to a covariance constraint, Gaussian distribution maximizes the differential entropy. Thus, plugging (5.352)

into (5.343) yields

$$\frac{1}{n}H(W_{\mathcal{S}}|\bar{\mathbf{Z}}^n) \geq \frac{1}{n}H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) - \frac{1}{2}\log\frac{\left|\alpha^2\hat{\mathbf{I}}_Z^A\mathbf{V}_Z\mathbf{S}\mathbf{V}_Z^\top(\hat{\mathbf{I}}_Z^A)^\top + \hat{\mathbf{\Sigma}}_Z^A\right|}{\left|\hat{\mathbf{\Sigma}}_Z^A\right|} \tag{5.353}$$

which implies that

$$\lim_{n\to\infty}\frac{1}{n}H(W_{\mathcal{S}}|\bar{\mathbf{Z}}^n) \geq \lim_{n\to\infty}\frac{1}{n}H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) - \lim_{\alpha\to 0}\frac{1}{2}\log\frac{\left|\alpha^2\hat{\mathbf{I}}_Z^A\mathbf{V}_Z\mathbf{S}\mathbf{V}_Z^\top(\hat{\mathbf{I}}_Z^A)^\top + \hat{\mathbf{\Sigma}}_Z^A\right|}{\left|\hat{\mathbf{\Sigma}}_Z^A\right|} \tag{5.354}$$

$$= \lim_{n\to\infty}\frac{1}{n}H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) \tag{5.355}$$

$$\geq \sum_{k\in\mathcal{S}} R_k \tag{5.356}$$

where (5.355) follows from the fact that $\log|\alpha^2\mathbf{A}+\mathbf{B}|$ is continuous in α for positive definite matrices $\mathbf{A},\mathbf{B}$, and (5.356) comes from our assumption that the codebook under consideration achieves perfect secrecy in the channel given in (5.318)-(5.319). Thus, we have shown that if a codebook achieves the perfect secrecy rates $(R_1,\ldots,R_K)$ in the channel defined by (5.318)-(5.319), then it also achieves the same perfect secrecy rates in the channel defined by (5.323)-(5.324) as $\alpha\to 0$. Thus, the secrecy capacity region of the latter channel converges to a region that includes the secrecy capacity region of the channel in (5.318)-(5.319), and also the secrecy capacity region of the original channel in (5.19)-(5.20). Since the channel in (5.323)-(5.324) is an aligned channel, its secrecy capacity region is given by Theorem 5.3, and it is equal to the dirty-paper coding region. Thus, to find the region that the

secrecy capacity region of the channel in (5.323)-(5.324) converges to as $\alpha \to 0$, it is sufficient to consider the region which the dirty-paper coding region converges to as $\alpha \to 0$. For that purpose, pick the kth user, and the identity encoding order, i.e., $\pi(k) = k,\ k = 1, \ldots, K$. The corresponding secrecy rate is

$$\begin{aligned}
&\frac{1}{2}\log\frac{\left|\bar{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\mathbf{\Sigma}}_{\pi(k)}\right|}{\left|\bar{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\mathbf{\Sigma}}_{\pi(k)}\right|}-\frac{1}{2}\log\frac{\left|\bar{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{Z}^{\top}+\hat{\mathbf{\Sigma}}_{Z}\right|}{\left|\bar{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{Z}^{\top}+\hat{\mathbf{\Sigma}}_{Z}\right|}\\
&=\frac{1}{2}\log\frac{\left|\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)^{\top}+\hat{\mathbf{\Sigma}}_{\pi(k)}\right|}{\left|\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)^{\top}+\hat{\mathbf{\Sigma}}_{\pi(k)}\right|}\\
&\quad-\frac{1}{2}\log\frac{\left|\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)^{\top}+\hat{\mathbf{\Sigma}}_{Z}\right|}{\left|\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)^{\top}+\hat{\mathbf{\Sigma}}_{Z}\right|}
\end{aligned} \tag{5.357}$$

which converges to

$$\frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\mathbf{\Sigma}}_{\pi(k)}\right|}{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\mathbf{\Sigma}}_{\pi(k)}\right|}-\frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{Z}^{\top}+\hat{\mathbf{\Sigma}}_{Z}\right|}{\left|\hat{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{Z}^{\top}+\hat{\mathbf{\Sigma}}_{Z}\right|} \tag{5.358}$$

as $\alpha \to 0$ due to the continuity of $\log|\cdot|$ in positive semi-definite matrices. Moreover, (5.358) is equal to

$$\frac{1}{2}\log\frac{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^{\top}+\mathbf{\Sigma}_{\pi(k)}\right|}{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^{\top}+\mathbf{\Sigma}_{\pi(k)}\right|}-\frac{1}{2}\log\frac{\left|\mathbf{H}_{Z}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{Z}^{\top}+\mathbf{\Sigma}_{Z}\right|}{\left|\mathbf{H}_{Z}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{Z}^{\top}+\mathbf{\Sigma}_{Z}\right|} \tag{5.359}$$

which implies that the secrecy capacity region of the general Gaussian MIMO multi-

receiver wiretap channel is given by the dirty-paper coding region, completing the proof.

5.8 Conclusions

In this chapter, we study the Gaussian MIMO multi-receiver wiretap channel and obtain its secrecy capacity region. We show that the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel can be attained by a variant of dirty-paper coding with Gaussian signals. To able to prove this, we develop a new methodology to evaluate certain single-letter capacity expressions for (vector) Gaussian models, which we use to obtain the secrecy capacity region of the degraded case, which admits a single-letter description for its secrecy capacity region. Once we obtain the secrecy capacity region of the degraded MIMO channel, we generalize it to arbitrary, not necessarily degraded, channels by using the channel enhancement technique and some limiting arguments as in [4, 21].

Furthermore, we note that our new methodology to evaluate the single-letter descriptions for vector Gaussian models can be used in other network information theory problems. In particular, using this new methodology, we provide an alternative proof for the capacity region of the degraded Gaussian MIMO broadcast channel and an outer bound for rate-distortion region of the vector Gaussian CEO problem. A summary of how our new methodology can be applied to these problems can be found in Appendices 5.9.7 and 5.9.8.

5.9 Appendix

5.9.1 Proof of Lemma 5.11

Let $\rho_i(\mathbf{x}|\mathbf{u}) = \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_i}$, i.e., the ith component of $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$. Then, we have

$$E\left[g(\mathbf{X})\rho_i(\mathbf{X}|\mathbf{U})\right] = \int g(\mathbf{x}) \frac{\frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f(\mathbf{x}|\mathbf{u})} f(\mathbf{x},\mathbf{u})\ d\mathbf{x}\ d\mathbf{u} \tag{5.360}$$

$$= \int g(\mathbf{x}) \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} f(\mathbf{u})\ d\mathbf{x}\ d\mathbf{u} \tag{5.361}$$

$$= \int \left[\int_{-\infty}^{+\infty} g(\mathbf{x}) \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i \right] f(\mathbf{u})\ d\mathbf{x}^-\ d\mathbf{u} \tag{5.362}$$

where $d\mathbf{x}^- = dx_1 \dots dx_{i-1} dx_{i+1} \dots dx_n$. The inner integral can be evaluated using integration by parts as

$$\int_{-\infty}^{+\infty} g(\mathbf{x}) \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i = \left[g(\mathbf{x}) f(\mathbf{x}|\mathbf{u}) \right] \Big|_{x_i=-\infty}^{+\infty} - \int_{-\infty}^{+\infty} f(\mathbf{x}|\mathbf{u}) \frac{\partial g(\mathbf{x})}{\partial x_i} dx_i \tag{5.363}$$

$$= - \int_{-\infty}^{+\infty} f(\mathbf{x}|\mathbf{u}) \frac{\partial g(\mathbf{x})}{\partial x_i} dx_i \tag{5.364}$$

where (5.364) comes from the assumption in (5.189). Plugging (5.364) into (5.362) yields

$$E\left[g(\mathbf{X})\rho_i(\mathbf{X}|\mathbf{U})\right] = - \int \frac{\partial g(\mathbf{x})}{\partial x_i} f(\mathbf{x},\mathbf{u})\ d\mathbf{x}\ d\mathbf{u} \tag{5.365}$$

$$= -E\left[\frac{\partial g(\mathbf{x})}{\partial x_i} \right] \tag{5.366}$$

which concludes the proof.

5.9.2 Proof of Lemma 5.12

Let $\rho_i(\mathbf{x}|\mathbf{u}) = \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_i}$, i.e., the ith component of $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$. Then, we have

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})|\mathbf{U}=\mathbf{u}\right] = \int \frac{\frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f(\mathbf{x}|\mathbf{u})} f(\mathbf{x}|\mathbf{u}) d\mathbf{x} \tag{5.367}$$

$$= \int \left[\int_{-\infty}^{+\infty} \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i\right] d\mathbf{x}^{-} \tag{5.368}$$

where $d\mathbf{x}^{-} = dx_1 \ldots dx_{i-1} dx_{i+1} \ldots dx_n$. The inner integral is

$$\int_{-\infty}^{+\infty} \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i = f(\mathbf{x}|\mathbf{u})\Big|_{x_i=-\infty}^{+\infty} = 0 \tag{5.369}$$

since $f(\mathbf{x}|\mathbf{u})$ is a valid probability density function. This completes the proof of the first part. For the second part, we have

$$E\left[g(\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = E\left[g(\mathbf{U})E\big[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})|\mathbf{U}=\mathbf{u}\big]\right] = 0 \tag{5.370}$$

where the second equality follows from the fact that the inner expectation is zero as the first part of this lemma states. The last part of the lemma follows by selecting $g(\mathbf{U}) = E\left[\mathbf{X}|\mathbf{U}\right]$ in the second part of this lemma.

5.9.3 Proof of Lemma 5.14

Throughout this proof, the subscript of f will denote the random vector for which f is the density. For example, $f_X(\mathbf{x}|\mathbf{u})$ is the conditional density of $\mathbf{X}$. We first note

that

$$f_W(\mathbf{w}|\mathbf{u}) = \int f_{X,W}(\mathbf{x}, \mathbf{w}|\mathbf{u})d\mathbf{x} = \int f_X(\mathbf{x}|\mathbf{u})f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})d\mathbf{x} \tag{5.371}$$

where the second equality is due to the conditional independence of $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{U}$. Differentiating both sides of (5.371), we get

$$\frac{\partial f_W(\mathbf{w}|\mathbf{u})}{\partial w_i} = \int f_X(\mathbf{x}|\mathbf{u})\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial w_i}d\mathbf{x} \tag{5.372}$$

$$= -\int f_X(\mathbf{x}|\mathbf{u})\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial x_i}d\mathbf{x} \tag{5.373}$$

$$= \big[-f_X(\mathbf{x}|\mathbf{u})f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})\big]\Big|_{x_i=-\infty}^{\infty} + \int f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}d\mathbf{x} \tag{5.374}$$

$$= \int f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}d\mathbf{x} \tag{5.375}$$

where (5.373) is due to

$$\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial w_i} = \frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial(w_i-x_i)}\frac{\partial(w_i-x_i)}{\partial w_i} \tag{5.376}$$

$$= -\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial(w_i-x_i)}\frac{\partial(w_i-x_i)}{\partial x_i} \tag{5.377}$$

$$= -\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial x_i} \tag{5.378}$$

and (5.374) follows from the fact that $f_X(\mathbf{x}|\mathbf{u}), f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})$ vanish at infinity since they are probability density functions. Using (5.375), we get

$$\boldsymbol{\rho}_i(\mathbf{w}|\mathbf{u}) = \frac{\frac{\partial f_W(\mathbf{w}|\mathbf{u})}{\partial w_i}}{f_W(\mathbf{w}|\mathbf{u})} = \int \frac{f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})} \frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i} d\mathbf{x} \tag{5.379}$$

$$= \int \frac{f_X(\mathbf{x}|\mathbf{u}) f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})} \frac{\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f_X(\mathbf{x}|\mathbf{u})} d\mathbf{x} \tag{5.380}$$

$$= \int f_X(\mathbf{x}|\mathbf{u}, \mathbf{w}) \frac{\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f_X(\mathbf{x}|\mathbf{u})} d\mathbf{x} \tag{5.381}$$

$$= E\left[\frac{1}{f_X(\mathbf{x}|\mathbf{u})} \left. \frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i} \right| \mathbf{W} = \mathbf{w}, \mathbf{U} = \mathbf{u} \right] \tag{5.382}$$

where (5.381) follows from the fact that

$$f_X(\mathbf{x}|\mathbf{u}, \mathbf{w}) = \frac{f_{X,W}(\mathbf{x}, \mathbf{w}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})} = \frac{f_X(\mathbf{x}|\mathbf{u}) f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})} \tag{5.383}$$

Equation (5.382) implies

$$\boldsymbol{\rho}(\mathbf{w}|\mathbf{u}) = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U} = \mathbf{u}) | \mathbf{W} = \mathbf{w}, \mathbf{U} = \mathbf{u} \right] \tag{5.384}$$

and due to symmetry, we also have

$$\boldsymbol{\rho}(\mathbf{w}|\mathbf{u}) = E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U} = \mathbf{u}) | \mathbf{W} = \mathbf{w}, \mathbf{U} = \mathbf{u} \right] \tag{5.385}$$

which completes the proof.

5.9.4 Proof of Lemma 5.15

Let $\mathbf{W} = \mathbf{X} + \mathbf{Y}$. We have

$$\begin{aligned}
\mathbf{0} \preceq E\Big[&\Big(\mathbf{A}\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + (\mathbf{I}-\mathbf{A})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U}) - \boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\Big) \\
&\qquad \Big(\mathbf{A}\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + (\mathbf{I}-\mathbf{A})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U}) - \boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\Big)^{\top}\Big] \qquad (5.386) \\
= \mathbf{A}&E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right]\mathbf{A}^{\top} + \mathbf{A}E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right](\mathbf{I}-\mathbf{A})^{\top} \\
&- \mathbf{A}E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] + (\mathbf{I}-\mathbf{A})E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right]\mathbf{A}^{\top} \\
&+ (\mathbf{I}-\mathbf{A})E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right](\mathbf{I}-\mathbf{A})^{\top} - (\mathbf{I}-\mathbf{A})E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] \\
&- E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right]\mathbf{A}^{\top} - E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right](\mathbf{I}-\mathbf{A})^{\top} \\
&+ E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] \qquad (5.387)
\end{aligned}$$

We note that, from the definition of the conditional Fisher information matrix, we have

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right] = \mathbf{J}(\mathbf{X}|\mathbf{U}) \qquad (5.388)$$

$$E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right] = \mathbf{J}(\mathbf{Y}|\mathbf{U}) \qquad (5.389)$$

$$E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] = \mathbf{J}(\mathbf{W}|\mathbf{U}) \qquad (5.390)$$

Moreover, we have

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^\top\right] = \left(E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right]\right)^\top \tag{5.391}$$

$$= \left(E\left[E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\middle|\mathbf{U}=\mathbf{u}\right]E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\middle|\mathbf{U}=\mathbf{u}\right]\right]\right)^\top \tag{5.392}$$

$$= \mathbf{0} \tag{5.393}$$

where (5.392) comes from the fact that given $\mathbf{U}=\mathbf{u}$, $\mathbf{X}$ and $\mathbf{Y}$ are conditionally independent, and (5.393) follows from the first part of Lemma 5.12, namely

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\middle|\mathbf{U}=\mathbf{u}\right] = E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\middle|\mathbf{U}=\mathbf{u}\right] = \mathbf{0} \tag{5.394}$$

Furthermore, we have

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] = E\left[E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}=\mathbf{u})\middle|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right]\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] \tag{5.395}$$

$$= E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] \tag{5.396}$$

$$= \mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{5.397}$$

where (5.396) follows from Lemma 5.14, and (5.397) comes from the definition of the conditional Fisher information matrix. Similarly, we also have

$$E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] = E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] = E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^\top\right] = \mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{5.398}$$

Thus, using (5.388)-(5.390), (5.393), (5.397)-(5.398) in (5.387), we get

$$\begin{aligned}\mathbf{0} \preceq\ & \mathbf{A}\mathbf{J}(\mathbf{X}|\mathbf{U})\mathbf{A}^\top - \mathbf{A}\mathbf{J}(\mathbf{W}|\mathbf{U}) + (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{Y}|\mathbf{U})(\mathbf{I}-\mathbf{A})^\top - (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{W}|\mathbf{U}) \\ & - \mathbf{J}(\mathbf{W}|\mathbf{U})\mathbf{A}^\top - \mathbf{J}(\mathbf{W}|\mathbf{U})(\mathbf{I}-\mathbf{A})^\top + \mathbf{J}(\mathbf{W}|\mathbf{U}) \qquad (5.399) \\ =\ & \mathbf{A}\mathbf{J}(\mathbf{X}|\mathbf{U})\mathbf{A}^\top + (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{Y}|\mathbf{U})(\mathbf{I}-\mathbf{A})^\top - \mathbf{J}(\mathbf{W}|\mathbf{U}) \qquad (5.400)\end{aligned}$$

which completes the proof.

5.9.5 Proof of Lemma 5.18

Consider $\mathbf{J}(\mathbf{X}|\mathbf{U})$

$$\begin{aligned}\mathbf{J}(\mathbf{X}|\mathbf{U}) &= \mathbf{J}(\mathbf{X}|\mathbf{U},\mathbf{V}) \qquad (5.401) \\ &= E\left[\nabla_{\mathbf{x}} \log f(\mathbf{X}|\mathbf{U},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X}|\mathbf{U},\mathbf{V})^\top\right] \qquad (5.402) \\ &= E\left[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{U},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{U},\mathbf{V})^\top\right] \qquad (5.403) \\ &= E\Big[\big(\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) + \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})\big) \\ &\qquad\qquad \big(\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) + \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})\big)^\top\Big] \qquad (5.404) \\ &= E\left[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V})^\top\right] \\ &\quad + E\left[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^\top\right] \\ &\quad + E\left[\nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V})^\top\right] \\ &\quad + E\left[\nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^\top\right] \qquad (5.405)\end{aligned}$$

where (5.401) is due to the Markov chain $\mathbf{V} \to \mathbf{U} \to \mathbf{X}$, (5.403) comes from the fact that

$$\nabla_{\mathbf{x}} \log f(\mathbf{x}|\mathbf{u}, \mathbf{v}) = \nabla_{\mathbf{x}} \big(\log f(\mathbf{x}, \mathbf{u}, \mathbf{v}) - \log f(\mathbf{u}, \mathbf{v}) \big) \tag{5.406}$$

$$= \nabla_{\mathbf{x}} \log f(\mathbf{x}, \mathbf{u}, \mathbf{v}) \tag{5.407}$$

and (5.404) is due to the fact that $f(\mathbf{x}, \mathbf{u}, \mathbf{v}) = f(\mathbf{x}, \mathbf{v}) f(\mathbf{u}|\mathbf{x}, \mathbf{v})$. We note that

$$\mathbf{J}(\mathbf{X}|\mathbf{V}) = E \left[\nabla_{\mathbf{x}} \log f(\mathbf{X}, \mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X}, \mathbf{V})^{\top} \right] \tag{5.408}$$

and

$$E \left[\nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X}, \mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X}, \mathbf{V})^{\top} \right] \succeq \mathbf{0} \tag{5.409}$$

Using (5.408) and (5.409) in (5.405), we get

$$\begin{aligned} \mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathbf{J}(\mathbf{X}|\mathbf{V}) &+ E \left[\nabla_{\mathbf{x}} \log f(\mathbf{X}, \mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X}, \mathbf{V})^{\top} \right] \\ &+ E \left[\nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X}, \mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X}, \mathbf{V})^{\top} \right] \end{aligned} \tag{5.410}$$

We now show that the cross-terms in (5.410) vanish. To this end, consider the (i,j)th entry of the first cross-term

$$
\begin{aligned}
&E\Big[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^{\top}\Big]_{ij} \\
&\quad = E\left[\frac{\partial \log f(\mathbf{X},\mathbf{V})}{\partial x_i} \frac{\partial \log f(\mathbf{U}|\mathbf{X},\mathbf{V})}{\partial x_j}\right] && (5.411) \\
&\quad = \int \frac{\frac{\partial f(\mathbf{x},\mathbf{v})}{\partial x_i}}{f(\mathbf{x},\mathbf{v})} \frac{\frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j}}{f(\mathbf{u}|\mathbf{x},\mathbf{v})} \; f(\mathbf{x},\mathbf{u},\mathbf{v}) \; d\mathbf{u} \; d\mathbf{v} \; d\mathbf{x} && (5.412) \\
&\quad = \int \frac{\partial f(\mathbf{x},\mathbf{v})}{\partial x_i} \frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j} \; d\mathbf{u} \; d\mathbf{v} \; d\mathbf{x} && (5.413) \\
&\quad = \int \frac{\partial f(\mathbf{x},\mathbf{v})}{\partial x_i} \left[\int \frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j} \; d\mathbf{u}\right] \; d\mathbf{v} \; d\mathbf{x} && (5.414)
\end{aligned}
$$

where the inner integral can be evaluated as

$$
\int \frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j} \; d\mathbf{u} = \frac{\partial}{\partial x_j}\left[\int f(\mathbf{u}|\mathbf{x},\mathbf{v}) \; d\mathbf{u}\right] = \frac{\partial(1)}{\partial x_j} = 0 \tag{5.415}
$$

where the interchange of the differentiation and the integration is justified by the assumption given in (5.214). Thus, using (5.415) in (5.414) implies that

$$
E\Big[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^{\top}\Big] = \mathbf{0} \tag{5.416}
$$

Thus, using (5.416) in (5.410), we get

$$
\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathbf{J}(\mathbf{X}|\mathbf{V}) \tag{5.417}
$$

which completes the proof.

5.9.6 Proof of Lemma 5.19

Since we assumed $\mu_j > 0,\ j = 1, \ldots, m$, we can select

$$\tilde{\mathbf{\Sigma}}_{j+1} = \left[\left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} - \sum_{i=1}^{j} \mathbf{K}_i, \quad j = 0, 1 \ldots, m-1 \tag{5.418}$$

which is equivalent to

$$\mu_{j+1} \left(\sum_{i=1}^{j} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1} \right)^{-1} = \mu_{j+1} \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \mathbf{M}_{j+1}, \quad j = 0, 1 \ldots, m-1 \tag{5.419}$$

and that implies $\mathbf{0} \preceq \tilde{\mathbf{\Sigma}}_j \preceq \mathbf{\Sigma}_j,\ j = 1, \ldots, m$. Furthermore, for $j = 0, \ldots, m-1$, we have

$$\sum_{i=1}^{j+1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1} = \mathbf{K}_{j+1} + \left(\sum_{i=1}^{j} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1} \right) \tag{5.420}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} \tag{5.421}$$

$$= \mathbf{K}_{j+1} + \left[\mathbf{I} + \frac{1}{\mu_{j+1}} \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right) \mathbf{M}_{j+1} \right]^{-1} \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right) \tag{5.422}$$

$$= \mathbf{K}_{j+1} + \left[\mathbf{I} + \frac{1}{\mu_{j+1}} \left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right) \mathbf{M}_{j+1} \right]^{-1} \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right) \tag{5.423}$$

$$= \mathbf{K}_{j+1}$$
$$+ \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} \left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} \left(\sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right) \tag{5.424}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} \left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1}$$
$$\times \left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} - \mathbf{K}_{j+1} \right) \tag{5.425}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1}$$
$$- \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} \left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} \mathbf{K}_{j+1} \tag{5.426}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1}$$
$$- \left\{ \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} \right.$$
$$\left. \times \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right] \mathbf{K}_{j+1} \right\} \tag{5.427}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} - \mathbf{K}_{j+1} \tag{5.428}$$

$$= \left[\left(\sum_{i=1}^{j+1} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} \tag{5.429}$$

where (5.421) follows from (5.419), (5.423) and (5.427) are consequences of the KKT conditions $\mathbf{M}_j\mathbf{K}_j = \mathbf{K}_j\mathbf{M}_j = \mathbf{0},\ j = 1, \ldots, m$. Finally, (5.429) is equivalent to

$$\mu_{j+1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1} = \mu_{j+1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \mathbf{M}_{j+1}, \quad j = 0, \ldots, m-1 \tag{5.430}$$

Plugging (5.419) and (5.430) into the KKT conditions in (5.293) and (5.294) yields the third part of the lemma.

We now prove the second part of the lemma. To this end, consider the second equation of the third part of the lemma, i.e., the following

$$\mu_m\left(\sum_{i=1}^{m}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} = \mu_m\left(\sum_{i=1}^{m}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} + \mathbf{M}_Z \tag{5.431}$$

which implies $\tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$. Now, consider the first equation of the third part of the lemma for $j = m-1$, i.e., the following

$$\begin{aligned}\mu_{m-1}\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{m-1}\right)^{-1} - \mu_{m-1}\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} &= \mu_m\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} \\ &\quad - \mu_m\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1}\end{aligned} \tag{5.432}$$

Since the matrix on the right hand side of the equation is positive semi-definite due

to the fact that $\tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$, and we assume that $\mu_m \geq \mu_{m-1}$, (5.432) implies

$$\left(\sum_{i=1}^{m-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{m-1}\right)^{-1} \succeq \left(\sum_{i=1}^{m-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} \tag{5.433}$$

which in turn implies $\tilde{\mathbf{\Sigma}}_{m-1} \preceq \tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$. Similarly, if one keeps checking the first equation of the third part of the lemma in the reverse order, one can get

$$\tilde{\mathbf{\Sigma}}_1 \preceq \ldots \preceq \tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z \tag{5.434}$$

Moreover, the definition of $\tilde{\mathbf{\Sigma}}_1$, i.e., (5.419) for $j = 0$,

$$\tilde{\mathbf{\Sigma}}_1 = \left[\mathbf{\Sigma}_1^{-1} + \frac{1}{\mu_1}\mathbf{M}_1\right]^{-1} \tag{5.435}$$

implies that $\tilde{\mathbf{\Sigma}}_1 \succ \mathbf{0}$ completing the proof of the second part of the lemma.

We now show the fourth part of the lemma

$$\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)$$

$$=\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}-\mathbf{K}_{j+1}\right) \tag{5.436}$$

$$=\mathbf{I}-\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1}\mathbf{K}_{j+1} \tag{5.437}$$

$$=\mathbf{I}-\left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}+\frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]\mathbf{K}_{j+1} \tag{5.438}$$

$$=\mathbf{I}-\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\mathbf{K}_{j+1} \tag{5.439}$$

$$=\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)-\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\mathbf{K}_{j+1} \tag{5.440}$$

$$=\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right),\quad j=0,\ldots,m-1 \tag{5.441}$$

where (5.438) follows from (5.430) and (5.439) is a consequence of the KKT conditions $\mathbf{K}_j\mathbf{M}_j=\mathbf{M}_j\mathbf{K}_j=\mathbf{0},\ j=1,\ldots,m$.

The proof of the fifth part of the lemma follows similarly

$$\begin{aligned}
&\left(\mathbf{S}+\tilde{\mathbf{\Sigma}}_m\right)\left(\sum_{i=1}^{m}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)^{-1} \\
&\quad=\left(\mathbf{S}-\sum_{i=1}^{m}\mathbf{K}_i+\sum_{i=1}^{m}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)\left(\sum_{i=1}^{m}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)^{-1} \\
&\quad=\left(\mathbf{S}-\sum_{i=1}^{m}\mathbf{K}_i\right)\left(\sum_{i=1}^{m}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)^{-1}+\mathbf{I} && (5.442) \\
&\quad=\left(\mathbf{S}-\sum_{i=1}^{m}\mathbf{K}_i\right)\left[\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\frac{1}{\mu_m}\mathbf{M}_Z\right]+\mathbf{I} && (5.443) \\
&\quad=\left(\mathbf{S}-\sum_{i=1}^{m}\mathbf{K}_i\right)\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\mathbf{I} && (5.444) \\
&\quad=\left(\mathbf{S}-\sum_{i=1}^{m}\mathbf{K}_i\right)\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+ \\
&\qquad\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1} && (5.445) \\
&\quad=\left(\mathbf{S}+\mathbf{\Sigma}_Z\right)\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1} && (5.446)
\end{aligned}$$

where (5.443) follows from the second equation of the third part of the lemma, and (5.444) is a consequence of the KKT condition in (5.291), completing the proof.

5.9.7 An Alternative Proof for the Capacity Region of the Degraded Gaussian MIMO Broadcast Channel

In this appendix[8], we provide an alternative proof for the capacity region of the degraded Gaussian MIMO broadcast channel. Our aim is to demonstrate how our technique, developed in this chapter to evaluate the single-letter description for

[8]This appendix provides a short summary of the work published in [55].

the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel, can be used for other problems involving vector Gaussian models.

The Gaussian MIMO broadcast channel consists of one transmitter and an arbitrary number of receivers, where the transmitter and receivers are equipped with multiple antennas. In general, the Gaussian MIMO broadcast channel is non-degraded, thus, we do not have a single-letter description of the capacity region. Despite this lack of a single-letter description, the capacity region of the Gaussian MIMO broadcast channel is successfully obtained in [4]. Subsequently, an alternative proof is given in [51]. In both proofs, the *channel enhancement* technique [4] is the main tool. We note that although both of these previous proofs are for general, not necessarily degraded, channels, when they are adapted to the degraded case, they still need channel enhancement.

In this appendix, we revisit the degraded Gaussian MIMO broadcast channel and provide an alternative proof for the capacity region of this degraded channel, without using the channel enhancement technique. Though channel enhancement is an elegant technique that finds itself diverse applications, we believe that our proof is more direct. On the other hand, our proof is limited to the degraded case and does not seem to be extendable for the general case. In other words, to obtain the capacity region for the general case after finding the capacity region for the degraded case through our proof, one needs to use the channel enhancement technique [4].

Our proof starts with the single-letter description of the capacity region of the degraded broadcast channel, and by using it, obtains a tight (i.e., achievable) outer bound for the capacity region of the degraded Gaussian MIMO broadcast channel.

In this proof, we use the tools that we already introduced in this chapter to obtain the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. The only new tool is an inequality due to [56, 57] that gives a lower bound for the differential entropy in terms of the Fisher information matrix.

5.9.7.1 Channel Model and Main Result

The (aligned) degraded K-user Gaussian MIMO broadcast channel is defined by

$$\mathbf{Y}_k = \mathbf{X} + \mathbf{N}_k, \quad k = 1, \ldots, K \tag{5.447}$$

where $\mathbf{N}_k$ is Gaussian with covariance matrix $\mathbf{\Sigma}_k$, $k = 1, \ldots, K$, and the channel input $\mathbf{X}$ and outputs $\{\mathbf{Y}_k\}_{k=1}^K$ satisfy the Markov chain

$$\mathbf{X} \to \mathbf{Y}_1 \to \ldots \to \mathbf{Y}_K \tag{5.448}$$

which is equivalent to the covariance matrices $\{\mathbf{\Sigma}_k\}_{k=1}^K$ satisfying the following order

$$\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \ldots \preceq \mathbf{\Sigma}_K \tag{5.449}$$

The channel input is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{5.450}$$

where we assume $\mathbf{S} \succ \mathbf{0}$. The covariance constraint in (5.450) is more general than many other constraints including the trace constraint, in the sense that, once the capacity region is found for the constraint in (5.450), capacity regions arising from the use of other constraints subsumed by (5.450) can be obtained by using this capacity region [4].

We next note that the definition of degradedness can be generalized to the case where receivers get arbitrary linear combinations of the channel inputs, i.e.,

$$\mathbf{Y}_k = \mathbf{H}_k \mathbf{X} + \mathbf{N}_k, \quad k = 1, \ldots, K \tag{5.451}$$

The broadcast channel defined in (5.451) is said to be degraded, i.e., satisfies the Markov chain in (5.448), if there exist matrices $\{\mathbf{D}_k\}_{k=1}^{K-1}$ such that $\mathbf{D}_k \mathbf{H}_k = \mathbf{H}_{k+1}$ and $\mathbf{D}_k \mathbf{D}_k^\top \preceq \mathbf{I}$ [5]. However, once the capacity region of the aligned degraded Gaussian MIMO broadcast channel defined by (5.447) is obtained, the capacity region of the general degraded Gaussian MIMO broadcast channel defined by (5.451) can be obtained by following the analysis given in Section 5 of [5], which essentially relies on some limiting arguments. Since the key step to obtain the capacity region of the general degraded Gaussian MIMO broadcast channel defined by (5.451) is to establish the capacity region of the aligned degraded Gaussian MIMO broadcast channel defined by (5.447), here we consider only the latter channel model.

The capacity region of the Gaussian MIMO broadcast channel is established in [4] for the most general case. For the degraded case, it is given as follows.

Theorem 5.8 ([4, Theorem 2] *The capacity region of the K-user degraded Gaus-*

sian MIMO broadcast channel is given by the union of rate tuples $(R_1, \ldots, R_K)$ *satisfying*

$$R_k \leq \frac{1}{2} \log \frac{|\sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_k|}{|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k|} \tag{5.452}$$

where the union is over all positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^{K}$ *such that* $\sum_{i=1}^{K} \mathbf{K}_i = \mathbf{S}$.

In the next section, we provide an alternative proof for this theorem for $K = 2$. The proof for an arbitrary case can be found in [55]. In our proof, we use the capacity region of the degraded broadcast channel which is stated in the following theorem, for the Gaussian MIMO channel at hand.

Theorem 5.9 ([22, Theorem 15.6.2] *The capacity region of the degraded broadcast channel is given by the union of rate tuples* $(R_1, \ldots, R_K)$ *satisfying*

$$R_k \leq I(U_k; Y_k | U_{k+1}), \quad k = 1, \ldots, K \tag{5.453}$$

where $U_{K+1} = \phi, U_1 = X$*, and the union is over all* $\{U_k\}_{k=2}^{K}, X$ *such that*

$$U_K \rightarrow \ldots \rightarrow U_2 \rightarrow X \rightarrow Y_1 \rightarrow \ldots \rightarrow Y_K \tag{5.454}$$

5.9.7.2 Proof of Theorem 5.8 for $K = 2$

The following lemma is due to [56, 57] which lower bounds the differential entropy in terms of the Fisher information matrix.

Lemma 5.20 ([56, 57]) *Let $(U, \mathbf{X})$ be an $(n+1)$-dimensional random vector, where the conditional Fisher information matrix of $\mathbf{X}$, conditioned on U, exists. Then, we have*

$$h(\mathbf{X}|U) \geq \frac{1}{2}\log(2\pi e)^n |\mathbf{J}^{-1}(\mathbf{X}|U)| \tag{5.455}$$

In [56, 57], the unconditional version of this lemma, i.e., $U = \phi$, is provided. A proof for its generalization to this conditional form is given in Appendix 5.9.9.

5.9.7.3 Proof for $K = 2$

We first rewrite the capacity region of the degraded broadcast channel given in Theorem 5.9 for two users as a union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq I(X; Y_1|U) \tag{5.456}$$

$$R_2 \leq I(U; Y_2) \tag{5.457}$$

where we dropped the subscript of the auxiliary random variable U_2 and denoted it simply as U. The involved random variables satisfy the Markov chain $U \to X \to Y_1 \to Y_2$. To obtain the capacity region of the degraded Gaussian MIMO broadcast channel, we need to evaluate this region. In particular, we will show that the optimal random vector $(U, \mathbf{X})$ that exhausts this region is Gaussian, and the corresponding

capacity region is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{5.458}$$

$$R_2 \leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_2|}{|\mathbf{K} + \mathbf{\Sigma}_2|} \tag{5.459}$$

where the union is over all $\mathbf{K}$ such that $\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}$. We note that the region described by (5.458)-(5.459) comes from Theorem 5.8 by dropping the subscript of $\mathbf{K}_1$ and denoting it simply as $\mathbf{K}$.

We begin with the bound on R_2. Starting from (5.457), we get

$$R_2 \leq I(U; \mathbf{Y}_2) \tag{5.460}$$

$$= h(\mathbf{Y}_2) - h(\mathbf{Y}_2|U) \tag{5.461}$$

$$\leq \frac{1}{2} \log(2\pi e)^n |\mathbf{S} + \mathbf{\Sigma}_2| - h(\mathbf{Y}_2|U) \tag{5.462}$$

where the inequality in (5.462) comes from the maximum entropy theorem [22]. We now bound $h(\mathbf{Y}_2|U)$ in (5.462). We first get an upper bound as

$$h(\mathbf{Y}_2|U) \leq h(\mathbf{Y}_2) \leq \frac{1}{2} \log(2\pi e)^n |\mathbf{S} + \mathbf{\Sigma}_2| \tag{5.463}$$

where the first inequality comes from the fact that conditioning cannot increase entropy, and the second inequality is due to the maximum entropy theorem [22].

Furthermore, using Lemma 5.20, we can get the following lower bound for $h(\mathbf{Y}_2|U)$

$$h(\mathbf{Y}_2|U) \geq \frac{1}{2}\log(2\pi e)^n|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U)| \tag{5.464}$$

We next define the following function

$$r(t) = \frac{1}{2}\log(2\pi e)^n|\mathbf{A}(t)+\mathbf{\Sigma}_2|, \quad 0 \leq t \leq 1 \tag{5.465}$$

where $\mathbf{A}(t)$ is given as

$$\mathbf{A}(t) = (1-t)\left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2\right] + t\mathbf{S} \tag{5.466}$$

We first note that

$$\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2 \preceq \mathrm{Cov}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2 \tag{5.467}$$

$$= \mathrm{Cov}(\mathbf{X}|U) \tag{5.468}$$

$$\preceq \mathrm{Cov}(\mathbf{X}) \tag{5.469}$$

$$\preceq \mathbf{S} \tag{5.470}$$

where (5.467) is a consequence of Lemma 5.13, and (5.469) comes from the fact that the conditional covariance matrix is smaller than the unconditional one in the positive semi-definite ordering sense. This implies that for any $0 \leq t \leq 1$, $\mathbf{A}(t)$

satisfies

$$\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U)-\mathbf{\Sigma}_2 \preceq \mathbf{A}(t) \preceq \mathbf{S} \tag{5.471}$$

Using $r(t)$, bounds in (5.463) and (5.464) can be rewritten as

$$r(0) \leq h(\mathbf{Y}_2|U) \leq r(1) \tag{5.472}$$

As shown in Lemma 5.10, $r(t)$ is continuous in t. Hence, due to the intermediate value theorem, there exists a t^* such that

$$r(t^*) = h(\mathbf{Y}_2|U) = \frac{1}{2}\log(2\pi e)^n|\mathbf{A}(t^*)+\mathbf{\Sigma}_2| \tag{5.473}$$

where $\mathbf{A}(t^*)$ satisfies (5.471). Plugging (5.473) into (5.462) yields

$$R_2 \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{A}(t^*)+\mathbf{\Sigma}_2|} \tag{5.474}$$

which is the desired bound on R_2 given in (5.459).

We now obtain the desired bound on R_1. To this end, using (5.471) and Lemma 5.16, we get

$$\mathbf{A}(t^*) \succeq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U)-\mathbf{\Sigma}_2 \tag{5.475}$$

$$\succeq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}|U)-\mathbf{\Sigma}_N \tag{5.476}$$

for any Gaussian random vector $\mathbf{N}$ with covariance matrix $\mathbf{\Sigma}_N$ where $\mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2$. The order in (5.476) is equivalent to

$$(\mathbf{A}(t^*) + \mathbf{\Sigma}_N)^{-1} \preceq \mathbf{J}(\mathbf{X} + \mathbf{N}|U) \tag{5.477}$$

Next, we consider the bound on R_1 given by (5.456). To this end, we first find an upper bound for the differential entropy term $h(\mathbf{Y}_1|U)$ which will be subsequently used to obtain the desired bound on R_1.

$$\begin{aligned}
h(\mathbf{Y}_1|U) &= h(\mathbf{Y}_1|U) - h(\mathbf{Y}_2|U) + h(\mathbf{Y}_2|U) && (5.478)\\
&= h(\mathbf{Y}_1|U) - h(\mathbf{Y}_2|U) + \frac{1}{2}\log(2\pi e)^n|\mathbf{A}(t^*) + \mathbf{\Sigma}_2| && (5.479)\\
&= -\frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} \mathbf{J}(\mathbf{X} + \mathbf{N}|U) d\mathbf{\Sigma}_N + \frac{1}{2}\log(2\pi e)^n|\mathbf{A}(t^*) + \mathbf{\Sigma}_2| && (5.480)\\
&\leq -\frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} (\mathbf{A}(t^*) + \mathbf{\Sigma}_N)^{-1} d\mathbf{\Sigma}_N + \frac{1}{2}\log(2\pi e)^n|\mathbf{A}(t^*) + \mathbf{\Sigma}_2| && (5.481)\\
&= \frac{1}{2}\log\frac{|\mathbf{A}(t^*) + \mathbf{\Sigma}_1|}{|\mathbf{A}(t^*) + \mathbf{\Sigma}_2|} + \frac{1}{2}\log(2\pi e)^n|\mathbf{A}(t^*) + \mathbf{\Sigma}_2| && (5.482)\\
&= \frac{1}{2}\log(2\pi e)^n|\mathbf{A}(t^*) + \mathbf{\Sigma}_1| && (5.483)
\end{aligned}$$

where (5.479) is due to (5.473), (5.480) is obtained by using Lemma 5.17, and (5.481) is due to (5.477) and Lemma 5.8. Using (5.483) in (5.456), we get

$$\begin{aligned}
R_1 &\leq I(\mathbf{X}; \mathbf{Y}_1|U) && (5.484)\\
&= h(\mathbf{Y}_1|U) - \frac{1}{2}\log(2\pi e)^n|\mathbf{\Sigma}_1| && (5.485)\\
&\leq \frac{1}{2}\log\frac{|\mathbf{A}(t^*) + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} && (5.486)
\end{aligned}$$

which is the desired bound on R_1 given in (5.458); completing the proof. The proof for an arbitrary K can be found in [55].

5.9.8 An Outer Bound for the Vector Gaussian CEO Problem

Similar to the previous appendix, here also[9], we want to demonstrate how our technique, developed in this chapter to evaluate the single-letter description for the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel, can be used for other problems involving vector Gaussian models. To this end, we consider the vector Gaussian CEO problem and obtain an outer bound for its rate-distortion region.

5.9.8.1 Problem Statement and the Main Result

In the CEO problem, there are L sensors, each of which getting a noisy observation of a source. The goal of the sensors is to describe their observations to the CEO such that it can reconstruct the source within a given distortion. In the vector Gaussian CEO problem (see Figure 5.4), there is an i.i.d. vector Gaussian source $\{\mathbf{X}_i\}_{i=1}^n$ with zero-mean and covariance $\mathbf{K}_X$. Each sensor gets a noisy version of this Gaussian source

$$\mathbf{Y}_{\ell,i} = \mathbf{X}_i + \mathbf{N}_{\ell,i}, \quad \ell = 1, \ldots, L \tag{5.487}$$

[9]This appendix provides a short summary of the work reported in [58].

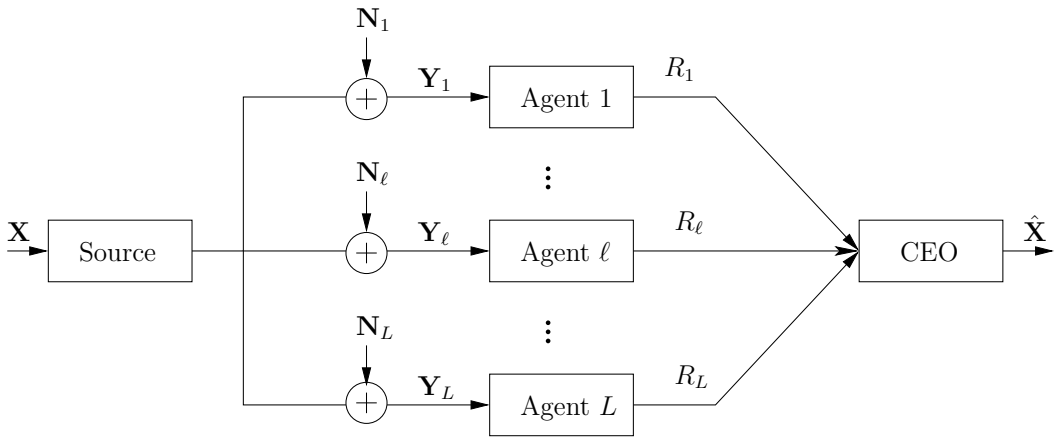

Figure 5.4: The vector Gaussian CEO problem.

where $\{\mathbf{N}_{\ell,i}\}_{i=1}^n$ is an i.i.d. sequence of Gaussian random vectors with zero-mean and covariance $\mathbf{\Sigma}_\ell$. Moreover, $\{\mathbf{N}_{\ell,i}\}_\ell^L$ are independent $\forall i$. The distortion of the reconstructed vector is measured by its mean square error matrix

$$\hat{\mathbf{D}}_n = \frac{1}{n}\sum_{i=1}^{n} E\left[\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)^\top\right] \tag{5.488}$$

where $\hat{\mathbf{X}}^n$ denotes the reconstructed vector.

An $(n, R_1, \ldots, R_L)$ code for the CEO problem consists of an encoding function at each sensor $f_\ell^n : \mathbb{R}^{M\times n} \to \mathcal{B}_\ell^n = \{1, \ldots, 2^{nR_\ell}\}$, i.e., $B_\ell^n = f_\ell^n(\mathbf{Y}_\ell^n)$ where $B_\ell^n \in \mathcal{B}_\ell^n,\ \ell = 1, \ldots, L$, and a decoding function at the CEO $g^n : \mathcal{B}_1^n \times \ldots \times \mathcal{B}_L^n \to \mathbb{R}^{M\times n}$, i.e., $\hat{\mathbf{X}}^n = g^n(B_1^n, \ldots, B_L^n)$, where M denotes the size of the vector Gaussian source $\mathbf{X}$.

Since the MMSE estimator, which is the conditional mean, minimizes the mean square error, the decoding function g^n can be chosen as the MMSE estimator.

Hence, we have $\hat{\mathbf{X}}_i = E\left[\mathbf{X}_i | \{B_\ell^n\}_{\ell=1}^L\right]$ using which in (5.488), we get

$$\hat{\mathbf{D}}_n = \frac{1}{n}\sum_{i=1}^{n} \mathrm{mmse}(\mathbf{X}_i | B_1^n, \ldots, B_L^n) \tag{5.489}$$

Hence, a rate tuple $(R_1, \ldots, R_L)$ is said to achieve the distortion $\mathbf{D}$ if there exists an $(n, R_1, \ldots, R_L)$ code such that

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n} \mathrm{mmse}(\mathbf{X}_i | B_1^n, \ldots, B_L^n) \preceq \mathbf{D} \tag{5.490}$$

where $\mathbf{D}$ is a strictly positive definite matrix. Throughout the paper, we assume that the distortion matrix $\mathbf{D}$ satisfies

$$\left(\mathbf{K}_X^{-1} + \sum_{\ell=1}^{L} \mathbf{\Sigma}_\ell^{-1}\right)^{-1} \preceq \mathbf{D} \preceq \mathbf{K}_X \tag{5.491}$$

where the lower bound on the distortion constraint $\mathbf{D}$ corresponds to the MMSE matrix obtained when the CEO has direct access to the observations of the agents $\{\mathbf{Y}_\ell\}_{\ell=1}^L$. In [58, Appendix A.2], we show that imposing the lower bound on $\mathbf{D}$ in (5.491) does not incur any loss of generality, while imposing the upper bound on $\mathbf{D}$ in (5.491) might incur some loss of generality.

The rate-distortion region $\mathcal{R}(\mathbf{D})$ of the vector Gaussian CEO problem is defined as the closure of all rate tuples $(R_1, \ldots, R_L)$ that can achieve the distortion $\mathbf{D}$.

We note that the rate-distortion region of the scalar Gaussian CEO problem is obtained in [59, 60]. However, the rate-distortion region of the vector case is a

largely open problem.

The main result we present in this Appendix is the following outer bound on the rate-distortion region $\mathcal{R}(\mathbf{D})$:

Theorem 5.10 *The rate-distortion region of the Gaussian CEO problem $\mathcal{R}(\mathbf{D})$ is contained in the region $\mathcal{R}^o(\mathbf{D})$ which is given by the union of rate tuples $(R_1, \ldots, R_L)$ satisfying*

$$\sum_{\ell \in \mathcal{A}} R_\ell \geq \frac{1}{2} \log^+ \frac{\left| \left(\mathbf{K}_X^{-1} + \sum_{\ell \in \mathcal{A}^c} \mathbf{\Sigma}_\ell^{-1} \left(\mathbf{\Sigma}_\ell - \mathbf{D}_\ell \right) \mathbf{\Sigma}_\ell^{-1} \right)^{-1} \right|}{|\mathbf{D}|} + \sum_{\ell \in \mathcal{A}} \frac{1}{2} \log \frac{|\mathbf{\Sigma}_\ell|}{|\mathbf{D}_\ell|} \quad (5.492)$$

for all $\mathcal{A} \subseteq \{1, \ldots, L\}$, where the union is over all positive semi-definite matrices $\{\mathbf{D}_\ell\}_{\ell=1}^L \in \mathcal{D}$, and $\mathcal{D}$ contains all $\{\mathbf{D}_\ell\}_{\ell=1}^L$ matrices satisfying the following constraints

$$\left(\mathbf{K}_X^{-1} + \sum_{\ell=1}^{L} \mathbf{\Sigma}_\ell^{-1} \left(\mathbf{\Sigma}_\ell - \mathbf{D}_\ell \right) \mathbf{\Sigma}_\ell^{-1} \right)^{-1} \preceq \mathbf{D} \quad (5.493)$$

$$\mathbf{0} \preceq \mathbf{D}_\ell \preceq \mathbf{\Sigma}_\ell, \quad \forall \ell \quad (5.494)$$

and $\log^+ x = \max(\log x, 0)$.

We obtain this outer bound by evaluating the outer bound given in [61]. This evaluation is carried out by using the technique we devised in this chapter to obtain the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel.

Next, we provide the following inner bound for the rate-distortion region $\mathcal{R}(\mathbf{D})$.

Theorem 5.11 *An inner bound for the rate-distortion region of the vector Gaussian CEO problem is given by the region* $\mathcal{R}^i(\mathbf{D})$ *which is described by the union of rate tuples* $(R_1, \ldots, R_L)$ *satisfying*

$$\sum_{\ell \in \mathcal{A}} R_\ell \geq \frac{1}{2} \log \frac{\left| \left(\mathbf{K}_X^{-1} + \sum_{\ell \in \mathcal{A}^c} \boldsymbol{\Sigma}_\ell^{-1} \left(\boldsymbol{\Sigma}_\ell - \mathbf{D}_\ell \right) \boldsymbol{\Sigma}_\ell^{-1} \right)^{-1} \right|}{\left| \left(\mathbf{K}_X^{-1} + \sum_{\ell=1}^{L} \boldsymbol{\Sigma}_\ell^{-1} \left(\boldsymbol{\Sigma}_\ell - \mathbf{D}_\ell \right) \boldsymbol{\Sigma}_\ell^{-1} \right)^{-1} \right|} + \sum_{\ell \in \mathcal{A}} \frac{1}{2} \log \frac{|\boldsymbol{\Sigma}_\ell|}{|\mathbf{D}_\ell|} \tag{5.495}$$

for all $\mathcal{A} \subseteq \{1, \ldots, L\}$*, where the union is over all positive semi-definite matrices* $\{\mathbf{D}_\ell\}_{\ell=1}^L \in \mathcal{D}$*.*

This inner bound is obtained by evaluating the Berger-Tung inner bound [62] by jointly Gaussian auxiliary random variables.

We note that for both the outer bound in Theorem 5.10 and the inner bound in Theorem 5.11, the feasible sets to which $\{\mathbf{D}_\ell\}_{\ell=1}^L$ belong are identical and given by $\mathcal{D}$. On the other hand, rate bounds differ as seen through (5.492) and (5.495). Despite this difference, there are cases where the outer and inner bounds match, providing a complete characterization of the rate-distortion region. Here, we note a general *sufficient* condition under which the outer and inner bounds coincide. If the boundary of the outer bound in Theorem 5.10 can be attained by $\{\mathbf{D}_\ell^*\}_{\ell=1}^L$ matrices which achieve the distortion constraint in (5.493) with equality, then the outer and inner bounds match, giving the rate-distortion region. For example, the outer and inner bounds match for the scalar Gaussian model [58].

5.9.8.2 Proof of Theorem 5.10

Here, we provide a sketch of the proof of Theorem 5.10 for $L = 2$. The proof of Theorem 5.10 for an arbitrary L can be found in [58]. We first state the following outer bound for the rate-distortion region of the CEO problem.

Theorem 5.12 ([61, Theorem 1]) *The rate-distortion region of the CEO problem* $\mathcal{R}(\mathbf{D})$ *is contained in the union of rate tuples* (R_1, R_2) *satisfying*

$$R_1 \geq I(\mathbf{X}; U_1|U_2) + I(\mathbf{Y}_1; U_1|\mathbf{X}, W) \tag{5.496}$$

$$R_2 \geq I(\mathbf{X}; U_2|U_1) + I(\mathbf{Y}_2; U_2|\mathbf{X}, W) \tag{5.497}$$

$$\sum_{\ell=1}^{2} R_\ell \geq I(\mathbf{X}; U_1, U_2) + \sum_{\ell=1}^{2} I(\mathbf{Y}_\ell; U_\ell|\mathbf{X}, W) \tag{5.498}$$

where the union is over all joint distributions

$$p(\mathbf{x}, \{\mathbf{y}_\ell, u_\ell\}_{\ell=1}^{2}, w) = p(\mathbf{x})p(w)\prod_{\ell=1}^{2} p(\mathbf{y}_\ell|\mathbf{x})p(u_\ell|\mathbf{y}_\ell, w) \tag{5.499}$$

satisfying

$$\text{mmse}(\mathbf{X}|U_1, U_2) \preceq \mathbf{D} \tag{5.500}$$

We evaluate this outer bound to obtain the outer bound in Theorem 5.10 for $L = 2$.

First, we consider the following mutual information terms

$$I(\mathbf{Y}_\ell; U_\ell|\mathbf{X}, W) = h(\mathbf{Y}_\ell|\mathbf{X}, W) - h(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell) \tag{5.501}$$

$$= \frac{1}{2}\log|(2\pi e)\mathbf{\Sigma}_\ell| - h(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell) \tag{5.502}$$

Using Lemma 5.20 and the fact that jointly Gaussian $(\mathbf{X}, W, U_\ell, \mathbf{Y}_\ell)$ maximizes $h(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell)$, we have the following bounds for the second term in (5.502)

$$\frac{1}{2}\log|(2\pi e)\mathbf{J}^{-1}(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell)| \le h(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell) \le \frac{1}{2}\log|(2\pi e)\mathrm{mmse}(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell)| \tag{5.503}$$

where $\mathbf{J}(\cdot|\cdot)$ denotes the conditional Fisher information matrix.

Since $\log|\cdot|$ is continuous in positive semi-definite matrices, there exists a matrix $\mathbf{D}_\ell$ in the following form

$$\mathbf{D}_\ell = \alpha_\ell \mathbf{J}^{-1}(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell) + \bar{\alpha}_\ell \mathrm{mmse}(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell) \tag{5.504}$$

with $\alpha_\ell = 1 - \bar{\alpha}_\ell \in [0, 1]$, which satisfies

$$h(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell) = \frac{1}{2}\log|(2\pi e)\mathbf{D}_\ell| \tag{5.505}$$

Hence, using (5.505) in (5.502), we have

$$I(\mathbf{Y}_\ell; U_\ell|\mathbf{X}, W) = \frac{1}{2}\log\frac{|\mathbf{\Sigma}_\ell|}{|\mathbf{D}_\ell|}, \quad \ell = 1, 2 \tag{5.506}$$

Moreover, using Lemma 5.13 and the fact that conditioning reduces MMSE, the following bounds on $\mathbf{D}_\ell$ can be obtained

$$\mathbf{0} \preceq \mathbf{D}_\ell \preceq \mathrm{mmse}(\mathbf{Y}_\ell|\mathbf{X}, W, U_\ell) \tag{5.507}$$

$$\preceq \mathbf{\Sigma}_\ell \tag{5.508}$$

which is the desired order on $\mathbf{D}_\ell$ stated in Theorem 5.10.

Next, we consider the following mutual information term

$$I(\mathbf{X}; U_1|U_2) = h(\mathbf{X}|U_2) - h(\mathbf{X}|U_1, U_2) \tag{5.509}$$

$$\geq h(\mathbf{X}|U_2) - \frac{1}{2}\log|(2\pi e)\mathrm{mmse}(\mathbf{X}|U_1, U_2)| \tag{5.510}$$

$$\geq h(\mathbf{X}|U_2) - \frac{1}{2}\log|(2\pi e)\mathbf{D}| \tag{5.511}$$

$$\geq h(\mathbf{X}|U_2, W) - \frac{1}{2}\log|(2\pi e)\mathbf{D}| \tag{5.512}$$

$$\geq \frac{1}{2}\log|(2\pi e)\mathbf{J}^{-1}(\mathbf{X}|U_2, W)| - \frac{1}{2}\log|(2\pi e)\mathbf{D}| \tag{5.513}$$

where (5.510) comes from the fact that $h(\mathbf{X}|U_1, U_2)$ is maximized by jointly Gaussian $(\mathbf{X}, U_1, U_2)$, (5.511) follows from the monotonicity of $\log|\cdot|$ function in positive semi-definite matrices in conjunction with the distortion constraint in (5.500), (5.512) comes from the fact that conditioning cannot increase entropy, and (5.513) is due to Lemma 5.20.

Next, we obtain a lower bound for $\mathbf{J}^{-1}(\mathbf{X}|U_2, W)$, which, in turn, will yield a lower bound for $h(\mathbf{X}|U_2, W)$. To obtain a lower bound for $h(\mathbf{X}|U_2, W)$, we will use an identity between the Fisher information matrix and the MMSE matrix, which

holds for additive Gaussian models as we have here. This identity is stated in the following lemma.

Lemma 5.21 ([52]) *Let* $(\mathbf{V}_1, \mathbf{V}_2)$ *be an arbitrary random vector with finite second moments, and* $\mathbf{N}$ *be a zero-mean Gaussian random vector with covariance* $\mathbf{\Sigma}_N$*. Assume* $(\mathbf{V}_1, \mathbf{V}_2)$ *and* $\mathbf{N}$ *are independent. We have*

$$\text{mmse}(\mathbf{V}_2|\mathbf{V}_1, \mathbf{V}_2 + \mathbf{N}) = \mathbf{\Sigma}_N - \mathbf{\Sigma}_N \mathbf{J}(\mathbf{V}_2 + \mathbf{N}|\mathbf{V}_1)\mathbf{\Sigma}_N \tag{5.514}$$

Before using this lemma to get a lower bound for $\mathbf{J}^{-1}(\mathbf{X}|U_2, W)$, we also need to rewrite $\mathbf{X}$ as follows

$$\mathbf{X} = \mathbf{A}_2\mathbf{Y}_2 + \tilde{\mathbf{N}}_2 \tag{5.515}$$

where $\mathbf{A}_2 = \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_2)^{-1}$, and $\tilde{\mathbf{N}}_2$ is a zero-mean Gaussian random vector with covariance matrix $\left(\mathbf{K}_X^{-1} + \mathbf{\Sigma}_2^{-1}\right)^{-1}$, and is independent of $\mathbf{Y}_2$. We note that (5.515) follows from the fact that $(\mathbf{X}, \mathbf{Y}_2)$ are jointly Gaussian. In view of (5.515), Lemma 5.21 implies

$$\text{mmse}(\mathbf{Y}_2|\mathbf{X}, W, U_2) = \mathbf{A}_2^{-1}\text{mmse}(\mathbf{A}_2\mathbf{Y}_2|\mathbf{A}_2\mathbf{Y}_2 + \tilde{\mathbf{N}}_2, W, U_2)\mathbf{A}_2^{-\top} \tag{5.516}$$

$$= \mathbf{A}_2^{-1}\left(\tilde{\mathbf{\Sigma}}_2 - \tilde{\mathbf{\Sigma}}_2\mathbf{J}(\mathbf{X}|U_2, W)\tilde{\mathbf{\Sigma}}_2\right)\mathbf{A}_2^{-\top} \tag{5.517}$$

using the definition of $\mathbf{A}_2$ and $\tilde{\mathbf{\Sigma}}_2$ in which, we get

$$\mathbf{J}^{-1}(\mathbf{X}|U_2, W) = \left(\mathbf{K}_X^{-1} + \mathbf{\Sigma}_2^{-1} - \mathbf{\Sigma}_2^{-1}\text{mmse}(\mathbf{Y}_2|\mathbf{X}, W, U_2)\mathbf{\Sigma}_2^{-1}\right)^{-1} \tag{5.518}$$

Using the order in (5.507) in (5.518), we get

$$\mathbf{J}^{-1}(\mathbf{X}|U_2, W) \succeq \left(\mathbf{K}_X^{-1} + \mathbf{\Sigma}_2^{-1} - \mathbf{\Sigma}_2^{-1}\mathbf{D}_2\mathbf{\Sigma}_2^{-1}\right)^{-1} \tag{5.519}$$

Moreover, in view of the monotonicity of $\log|\cdot|$ in positive semi-definite matrices, using (5.519) in (5.513), we can get

$$I(\mathbf{X}; U_1|U_2) \geq \frac{1}{2}\log^+ \frac{\left|\left(\mathbf{K}_X^{-1} + \mathbf{\Sigma}_2^{-1} - \mathbf{\Sigma}_2^{-1}\mathbf{D}_2\mathbf{\Sigma}_2^{-1}\right)^{-1}\right|}{|\mathbf{D}|} \tag{5.520}$$

where the positivity operator comes from the non-negativity of the mutual information. Using (5.506) and (5.520) in (5.496), we can get

$$R_1 \geq \frac{1}{2}\log^+ \frac{\left|\left(\mathbf{K}_X^{-1} + \mathbf{\Sigma}_2^{-1} - \mathbf{\Sigma}_2^{-1}\mathbf{D}_2\mathbf{\Sigma}_2^{-1}\right)^{-1}\right|}{|\mathbf{D}|} + \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{D}_1|} \tag{5.521}$$

which is the desired bound on R_1 given in Theorem 5.10. Similarly one can get the desired bound on R_2 as well.

Next, we consider the sum-rate $R_1 + R_2$. To this end, we note that using the maximum entropy theorem and the distortion constraint in (5.500), one can get

$$I(\mathbf{X}; U_1, U_2) \geq \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{D}|} \tag{5.522}$$

using which, and the identities in (5.506) for the sum-rate bound in (5.498), we have

$$R_1 + R_2 \geq \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{D}|} + \sum_{\ell=1}^{2}\frac{1}{2}\log\frac{|\mathbf{\Sigma}_\ell|}{|\mathbf{D}_\ell|} \tag{5.523}$$

which is the desired bound on the sum-rate given in Theorem 5.10.

Finally, we establish a connection between $\mathbf{D}$ and $(\mathbf{D}_1, \mathbf{D}_2)$, which will complete the proof of Theorem 5.10. To this end, we note that similar to (5.519), one can obtain the following lower bound for $\mathbf{J}^{-1}(\mathbf{X}|U_1, U_2, W)$

$$\left(\mathbf{K}_X^{-1} + \sum_{\ell=1}^{2}\mathbf{\Sigma}_\ell^{-1} - \sum_{\ell=1}^{2}\mathbf{\Sigma}_\ell^{-1}\mathbf{D}_\ell\mathbf{\Sigma}_\ell^{-1}\right)^{-1}$$

$$\preceq \mathbf{J}^{-1}(\mathbf{X}|U_1, U_2, W) \tag{5.524}$$

$$\preceq \text{mmse}(\mathbf{X}|U_1, U_2, W) \tag{5.525}$$

$$\preceq \text{mmse}(\mathbf{X}|U_1, U_2) \tag{5.526}$$

$$\preceq \mathbf{D} \tag{5.527}$$

where (5.525) is due to Lemma 5.13, (5.526) comes from the fact that conditioning reduces MMSE, and (5.527) follows from the distortion constraint in (5.500). The order in (5.527) gives us the desired order among $\mathbf{D}_\ell$ and $\mathbf{D}$; completing the proof. The proof for an arbitrary L can be found in [58].

5.9.9 Proof of Lemma 5.20

We define the function $f(\epsilon)$ as follows

$$f(\epsilon) = h(\mathbf{X} + \sqrt{\epsilon}\mathbf{N}|U) - \frac{1}{2}\log\left|(2\pi e)\left(\mathbf{J}^{-1}(\mathbf{X}|U) + \epsilon\mathbf{\Sigma}\right)\right|, \quad \epsilon \geq 0 \tag{5.528}$$

We need to prove that $f(0) \geq 0$. We will show that $f(\epsilon)$ is monotonically decreasing in ϵ, and that $\lim_{\epsilon\to\infty} f(\epsilon) = 0$. This will prove $f(0) \geq 0$.

Fix ϵ_1, ϵ_2 such that $0 < \epsilon_1 \leq \epsilon_2$. Using Lemma 5.17, we have

$$h(\mathbf{X} + \sqrt{\epsilon_2}\mathbf{N}|U) - h(\mathbf{X} + \sqrt{\epsilon_1}\mathbf{N}|U) = \frac{1}{2}\int_{\epsilon_1\mathbf{\Sigma}}^{\epsilon_2\mathbf{\Sigma}} \mathbf{J}(\mathbf{X} + \mathbf{T}|U)d\mathbf{\Sigma}_T \tag{5.529}$$

where $\mathbf{T}$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_T$ such that $\epsilon_1\mathbf{\Sigma} \preceq \mathbf{\Sigma}_T \preceq \epsilon_2\mathbf{\Sigma}$, and independent of $(U, \mathbf{X})$. Using Corollary 5.4 in conjunction with Lemma 5.13, we get

$$\mathbf{J}(\mathbf{X} + \mathbf{T}|U) \preceq \left[\mathbf{J}^{-1}(\mathbf{X}|U) + \mathbf{\Sigma}_T\right]^{-1} \tag{5.530}$$

Plugging (5.530) into (5.529) and invoking Lemma 5.8, we get

$$h(\mathbf{X} + \sqrt{\epsilon_2}\mathbf{N}|U) - h(\mathbf{X} + \sqrt{\epsilon_1}\mathbf{N}|U) \leq \frac{1}{2}\log\frac{|(2\pi e)\left(\mathbf{J}^{-1}(\mathbf{X}|U) + \epsilon_2\mathbf{\Sigma}\right)|}{|(2\pi e)\left(\mathbf{J}^{-1}(\mathbf{X}|U) + \epsilon_1\mathbf{\Sigma}\right)|} \tag{5.531}$$

Rearranging (5.531) yields

$$f(\epsilon_2) \leq f(\epsilon_1), \quad \epsilon_1 \leq \epsilon_2 \tag{5.532}$$

which proves that $f(\epsilon)$ is monotonically decreasing in ϵ.

We now consider upper and lower bounds on $f(\epsilon)$. We have the following upper bound on $f(\epsilon)$

$$\begin{aligned} f(\epsilon) &= h(\mathbf{X} + \sqrt{\epsilon}\mathbf{N}|U) - \frac{1}{2}\log\left|(2\pi e)\left(\mathbf{J}^{-1}(\mathbf{X}|U) + \epsilon\mathbf{\Sigma}\right)\right| && (5.533) \\ &\leq \frac{1}{2}\log\frac{|\mathbf{K} + \epsilon\mathbf{\Sigma}|}{|\mathbf{J}^{-1}(\mathbf{X}|U) + \epsilon\mathbf{\Sigma}|} && (5.534) \\ &= \frac{1}{2}\log\frac{|\mathbf{\Sigma}^{-1/2}\mathbf{K}\mathbf{\Sigma}^{-1/2} + \epsilon\mathbf{I}|}{|\mathbf{\Sigma}^{-1/2}\mathbf{J}^{-1}(\mathbf{X}|U)\mathbf{\Sigma}^{-1/2} + \epsilon\mathbf{I}|} && (5.535) \\ &= \frac{1}{2}\log\prod_{i=1}^{n}\frac{\tilde{\lambda}_i + \epsilon}{\lambda_i + \epsilon} && (5.536) \end{aligned}$$

where (5.534) comes from the maximum entropy theorem [22] and $\mathbf{K}$ denotes the covariance matrix of $\mathbf{X}$. In (5.536), we denote the eigenvalues of $\mathbf{\Sigma}^{-1/2}\mathbf{K}\mathbf{\Sigma}^{-1/2}$ with $\{\tilde{\lambda}_i\}_{i=1}^n$, and of $\mathbf{\Sigma}^{-1/2}\mathbf{J}^{-1}(\mathbf{X}|U)\mathbf{\Sigma}^{-1/2}$ with $\{\lambda_i\}_{i=1}^n$. Furthermore, we have the following lower bound on $f(\epsilon)$

$$\begin{aligned} f(\epsilon) &= h(\mathbf{X} + \sqrt{\epsilon}\mathbf{N}|U) - \frac{1}{2}\log\left|(2\pi e)\left(\mathbf{J}^{-1}(\mathbf{X}|U) + \epsilon\mathbf{\Sigma}\right)\right| && (5.537) \\ &\geq \frac{1}{2}\log\frac{|\epsilon\mathbf{\Sigma}|}{|\mathbf{J}^{-1}(\mathbf{X}|U) + \epsilon\mathbf{\Sigma}|} && (5.538) \\ &= \frac{1}{2}\log\frac{\epsilon^n}{|\mathbf{\Sigma}^{-1/2}\mathbf{J}^{-1}(\mathbf{X}|U)\mathbf{\Sigma}^{-1/2} + \epsilon\mathbf{I}|} && (5.539) \\ &= \frac{1}{2}\log\prod_{i=1}^{n}\frac{\epsilon}{\lambda_i + \epsilon} && (5.540) \end{aligned}$$

where (5.538) comes from the fact that conditioning cannot increase entropy, and in (5.540), we denote the eigenvalues of $\mathbf{\Sigma}^{-1/2}\mathbf{J}^{-1}(\mathbf{X}|U)\mathbf{\Sigma}^{-1/2}$ with $\{\lambda_i\}_{i=1}^n$. Comparison of (5.536) and (5.540) yields

$$\frac{1}{2}\log\prod_{i=1}^{n}\frac{\epsilon}{\lambda_i+\epsilon} \leq f(\epsilon) \leq \frac{1}{2}\log\prod_{i=1}^{n}\frac{\tilde{\lambda}_i+\epsilon}{\lambda_i+\epsilon} \tag{5.541}$$

Taking the limit as $\epsilon \to \infty$ yields $\lim_{\epsilon\to\infty} f(\epsilon) = 0$. Combining this with the fact that $f(\epsilon)$ decreases monotonically in ϵ yields $f(0) \geq 0$, and consequently,

$$h(\mathbf{X}|U) \geq \frac{1}{2}\log(2\pi e)^n|\mathbf{J}^{-1}(\mathbf{X}|U)| \tag{5.542}$$

completing the proof.

Chapter 6

Multi-receiver Wiretap Channel with Public and Confidential Messages

6.1 Introduction

In this chapter, we study the multi-receiver wiretap channel (see Figure 6.1) with public and confidential messages which generalizes the scenario we study in Chapters 3 and 5 by incorporating public messages in addition to confidential messages. In this model, confidential messages should be transmitted in perfect secrecy, while there are no secrecy constraints on the public messages.

First, we consider the degraded discrete memoryless multi-receiver wiretap channel (see Figure 6.2), and propose inner and outer bounds for its capacity region. Although these inner and outer bounds do not match in general, there are cases where they match, and hence, provide the capacity region. In particular, these inner and outer bounds match when: the public message rate of the second legitimate user (weak user) is zero, the confidential message rate of the first legitimate user (strong user) is zero, and the rates of both of the public messages are zero. We note that the last case corresponds to the secrecy capacity region of the degraded discrete memoryless multi-receiver wiretap channel which was already obtained in Chapter 3.

Second, we consider the general, not necessarily degraded, discrete memoryless

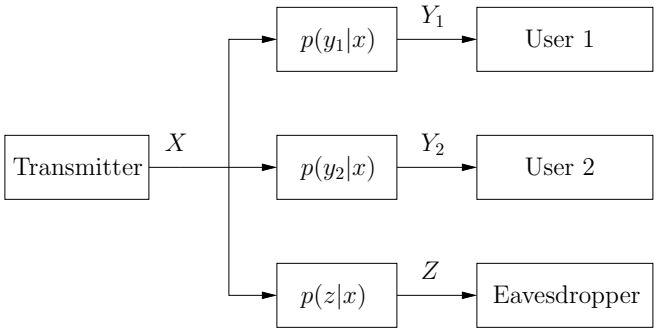

Figure 6.1: Multi-receiver wiretap channel.

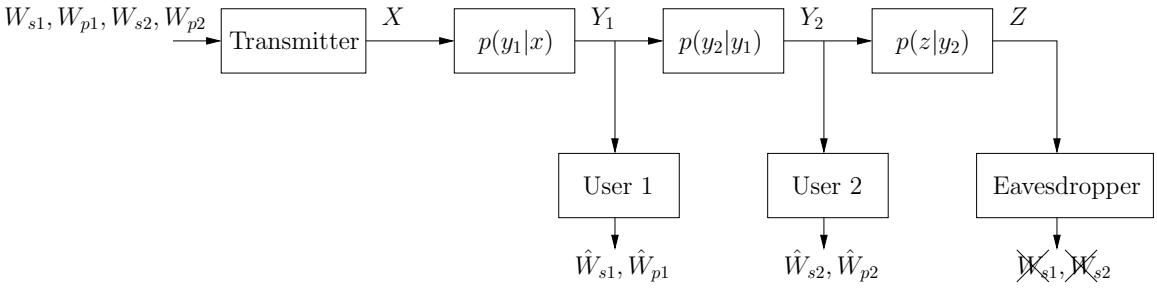

Figure 6.2: Degraded multi-receiver wiretap channel.

multi-receiver wiretap channel, and propose an inner bound for its capacity region by using Marton's inner bound [11], superposition coding, rate-splitting and binning. This inner bound generalizes the inner bound we proposed for the degraded case by using Marton's coding.

Third, we consider the degraded Gaussian MIMO instance of this channel model, and evaluate the inner and outer bounds we proposed for the degraded discrete memoryless case. In particular, we show the sufficiency of jointly Gaussian auxiliary random variables and channel input to exhaust the inner and outer bounds, by using our methodology proposed in Chapter 5 to evaluate the single-letter expressions for vector Gaussian models. Similar to the degraded discrete memoryless case, under the conditions listed for the degraded discrete memoryless case, these

inner and outer bounds match for the degraded MIMO channel as well, providing the capacity region.

Finally, we consider the general, not necessarily degraded, Gaussian MIMO multi-receiver wiretap channel. We evaluate the achievable scheme we proposed for the general discrete memoryless channel by using dirty-paper coding [12], and obtain an inner bound for the capacity region of the general Gaussian MIMO channel.

6.2 Discrete Memoryless Multi-receiver Wiretap Channels

Discrete memoryless multi-receiver wiretap channels consist of a transmitter, two legitimate users, and an eavesdropper. The channel is memoryless with a transition probability $p(y_1, y_2, z|x)$, where $X \in \mathcal{X}$ is the channel input, and $Y_1 \in \mathcal{Y}_1, Y_2 \in \mathcal{Y}_2, Z \in \mathcal{Z}$ denote the channel outputs of the first legitimate user, the second legitimate user, and the eavesdropper, respectively. We consider the scenario in which, the transmitter sends a pair of public and confidential messages to each legitimate user. While there are no secrecy constraints on the public messages, the confidential messages need to be transmitted in perfect secrecy. We call the channel model arising from this scenario the *multi-receiver wiretap channel with public and confidential messages*.

An $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code for this channel consists of four message sets, $\mathcal{W}_{p1} = \{1, \ldots, 2^{nR_{p1}}\}$, $\mathcal{W}_{s1} = \{1, \ldots, 2^{nR_{s1}}\}$, $\mathcal{W}_{p2} = \{1, \ldots, 2^{nR_{p2}}\}$, $\mathcal{W}_{s2} = \{1, \ldots, 2^{nR_{s2}}\}$, one encoder at the transmitter $f : \mathcal{W}_{p1} \times \mathcal{W}_{s1} \times \mathcal{W}_{p2} \times \mathcal{W}_{s2} \to \mathcal{X}^n$, and one decoder at each legitimate user $g_j : \mathcal{Y}_j^n \to \mathcal{W}_{pj} \times \mathcal{W}_{sj}$, for $j = 1, 2$. The

probability of error is defined as $P_e^n = \max\{P_{e,1}^n, P_{e,2}^n\}$, where $P_{e,j}^n = \Pr[g_j(Y_j^n) \neq (W_{pj}, W_{sj})]$, for $j = 1, 2$, and $W_{p1}, W_{s1}, W_{p2}, W_{s2}$ are uniformly distributed random variables in $\mathcal{W}_{p1}, \mathcal{W}_{s1}, \mathcal{W}_{p2}, \mathcal{W}_{s2}$, respectively. A rate tuple $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ is said to be achievable if there exists an $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code which satisfies $\lim_{n\to\infty} P_e^n = 0$ and[1]

$$\lim_{n\to\infty} \frac{1}{n} I(W_{s1}, W_{s2}; Z^n) = 0 \tag{6.1}$$

The capacity region of the multi-receiver wiretap channel with public and confidential messages, $\mathcal{C}$, is defined as the convex closure of all achievable rate tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$.

6.2.1 Degraded Channels

The degraded multi-receiver wiretap channel satisfies the following Markov chain

$$X \to Y_1 \to Y_2 \to Z \tag{6.2}$$

We first present an inner bound for $\mathcal{C}$ in the following theorem.

Theorem 6.1 *An achievable rate region, denoted by $\mathcal{R}^{\text{in}}$, for the multi-receiver wiretap channel with public and confidential messages is given by the union of rate*

[1] We note that (6.1) implies $\lim_{n\to\infty}(1/n) I(W_{sj}; Z^n) = 0,\ j = 1, 2$.

tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ *satisfying*

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{6.3}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{6.4}$$

$$R_{p2} + R_{s2} \leq I(U;Y_2) \tag{6.5}$$

$$R_{s1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z|U) \tag{6.6}$$

$$R_{p1} + R_{s1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{6.7}$$

where (U, X) *satisfy the following Markov chain*

$$U \to X \to Y_1 \to Y_2 \to Z \tag{6.8}$$

The achievable rate region given by Theorem 6.1 can be obtained from Theorem 6.3, which will be introduced in the next section. The achievable rate region in Theorem 6.1 can be shown by using superposition coding and binning. Superposition coding enables us to transmit messages of each user at a different layer, and binning enables us to ensure the protection of the confidential messages from the eavesdropper.

Now, we introduce the following outer bound for the capacity region of the degraded discrete memoryless multi-receiver wiretap channel with public and confidential messages.

Theorem 6.2 *The capacity region of the degraded multi-receiver wiretap channel with public and confidential messages is contained in* $\mathcal{R}^{\text{out}}$ *that is composed of rate*

tuples $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ *satisfying*

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{6.9}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{6.10}$$

$$R_{p2} + R_{s2} \leq I(U;Y_2) \tag{6.11}$$

$$R_{p1} + R_{s1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{6.12}$$

for some (U, X) *such that* U, X *exhibit the following Markov chain*

$$U \to X \to Y_1 \to Y_2 \to Z \tag{6.13}$$

The proof of Theorem 6.2 is given in Appendix 6.5.1.

We note that the inner bound in Theorem 6.1 and the outer bound in Theorem 6.2 do not match in general. In fact, in Section 6.3.1, we provide an example where the outer bound strictly includes the inner bound, i.e., there are rate tuples which are included in $\mathcal{R}^{\text{out}}$, but not in $\mathcal{R}^{\text{in}}$. However, there are cases for which the exact capacity region can be obtained. First, we note that the inner bound in Theorem 6.1 and the outer bound in Theorem 6.2 match when the confidential message rate of the first legitimate user is zero, i.e., $R_{s1} = 0$.

Corollary 6.1 *The capacity region of the degraded multi-receiver wiretap channel without the first legitimate user's confidential message is given by the union of rate*

triples (R_{p1}, R_{p2}, R_{s2}) *satisfying*

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{6.14}$$

$$R_{s2} + R_{p2} \leq I(U;Y_2) \tag{6.15}$$

$$R_{p1} + R_{p2} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{6.16}$$

where U, X *exhibit the following Markov chain*

$$U \to X \to Y_1 \to Y_2 \to Z \tag{6.17}$$

Corollary 6.1 can be proved by setting $R_{s1} = 0$ in both Theorem 6.1 and Theorem 6.2 and eliminating the redundant bounds.

Next, we note that the inner bound in Theorem 6.1 and the outer bound in Theorem 6.2 match when the public message rate of the second legitimate user is zero, i.e., $R_{p2} = 0$.

Corollary 6.2 *The capacity region of the degraded multi-receiver wiretap channel without the second legitimate user's public message is given by the union of rate triples* (R_{p1}, R_{s1}, R_{s2}) *satisfying*

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{6.18}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{6.19}$$

$$R_{p1} + R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) \tag{6.20}$$

where U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z \tag{6.21}$$

Corollary 6.2 can be proved by setting $R_{p2} = 0$ in both Theorem 6.1 and Theorem 6.2 and eliminating the redundant bounds.

Corollary 6.2 also implies that the inner bound in Theorem 6.1 and the outer bound in Theorem 6.2 match on the secrecy capacity region of the degraded multi-receiver wiretap channel (that was obtained in Corollary 3.1 of Chapter 3, and in [23]), i.e., when the rates of both public messages R_{p1}, R_{p2} are set to zero:

Corollary 6.3 *The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of rate pairs (R_{s1}, R_{s2}) satisfying*

$$R_{s2} \leq I(U;Y_2) - I(U;Z) \tag{6.22}$$

$$R_{s1} + R_{s2} \leq I(U;Y_2) + I(X;Y_1|U) - I(X;Z) \tag{6.23}$$

where U, X exhibit the following Markov chain

$$U \to X \to Y_1 \to Y_2 \to Z \tag{6.24}$$

So far, we provided examples where the inner and outer bounds match when one of the rates is zero. Next, we provide an example where the inner and outer bounds match when none of the rates is zero. To this end, we express the inner and

the outer bounds by using hyperplanes that are tangent to them:

$$L^{\text{in}} = \max_{(R_{p1},R_{s1},R_{p2},R_{s2})\in\mathcal{R}^{\text{in}}} \quad \mu_{p1}R_{p1} + \mu_{s1}R_{s1} + \mu_{p2}R_{p2} + \mu_{s2}R_{s2} \tag{6.25}$$

$$L^{\text{out}} = \max_{(R_{p1},R_{s1},R_{p2},R_{s2})\in\mathcal{R}^{\text{out}}} \quad \mu_{p1}R_{p1} + \mu_{s1}R_{s1} + \mu_{p2}R_{p2} + \mu_{s2}R_{s2} \tag{6.26}$$

Assume that the following condition holds:

$$\mu_{s2} > \max(\mu_{s1}, \mu_{p2}) \geq \min(\mu_{s1}, \mu_{p2}) > \mu_{p1} \tag{6.27}$$

$$\mu_{s2} + \mu_{p1} > \mu_{s1} + \mu_{p2} \tag{6.28}$$

Under these conditions, we have

$$\begin{aligned} L^{\text{out}} = \max_{(R_{p1},R_{s1},R_{p2},R_{s2})\in\mathcal{R}^{\text{out}}} \; & \mu_{p1}(R_{p1} + R_{s1} + R_{p2} + R_{s2}) + (\mu_{s1} - \mu_{p1})(R_{s1} + R_{s2}) \\ & + (\mu_{p2} - \mu_{p1})(R_{p2} + R_{s2}) + (\mu_{s2} + \mu_{p1} - \mu_{s1} - \mu_{p2})R_{s2} \end{aligned} \tag{6.29}$$

$$\begin{aligned} = \max_{(U,X)\in\mathcal{F}} \; & \mu_{p1}\big[I(U;Y_2) + I(X;Y_1|U)\big] \\ & + (\mu_{s1} - \mu_{p1})\big[I(U;Y_2) + I(X;Y_1|U) - I(X;Z)\big] \\ & + (\mu_{p2} - \mu_{p1})I(U;Y_2) + (\mu_{s2} + \mu_{p1} - \mu_{s1} - \mu_{p2})\big[I(U;Y_2) - I(U;Z)\big] \end{aligned} \tag{6.30}$$

$$\begin{aligned} = \max_{(U,X)\in\mathcal{F}} \; & \mu_{p1}I(X;Z|U) + \mu_{s1}\big[I(X;Y_1|U) - I(X;Z|U)\big] + \mu_{p2}I(U;Z) \\ & + \mu_{s2}\big[I(U;Y_2) - I(U;Z)\big] \end{aligned} \tag{6.31}$$

$$= L^{\text{in}} \tag{6.32}$$

where the set $\mathcal{F}$ is given by the union of (U, X) pairs that satisfy the Markov chain in (6.13), and (6.31) follows from the fact $(R_{p1}^*, R_{s1}^*, R_{p2}^*, R_{s2}^*) \in \mathcal{R}^{\text{in}}$ attains (6.32), and $(R_{p1}^*, R_{s1}^*, R_{p2}^*, R_{s2}^*)$ is given by

$$(R_{p1}^*, R_{s1}^*) = \big(I(X;Z|U), I(X;Y_1|U) - I(X;Z|U)\big) \tag{6.33}$$

$$(R_{p2}^*, R_{s2}^*) = \big(I(U;Z), I(U;Y_2) - I(U;Z)\big) \tag{6.34}$$

Hence, this example shows that there are parts of the capacity region where none of the rates is zero, and the inner and outer bounds match.

Next, we provide an example where the inner bound is strictly contained in the outer bound, i.e., there are rate tuples that are inside the outer bound, but outside the inner bound. To provide such an example, we again use the alternative descriptions of the inner and outer bounds by means of tangent hyperplanes as given by (6.25) and (6.26), respectively. We assume that the following condition holds

$$\mu_{s1} > \mu_{p2} > \mu_{p1} > \mu_{s2} \tag{6.35}$$

Under this condition, we have

$$\begin{aligned} L^{\text{out}} \geq \max_{(U,X)\in\mathcal{F}} \quad & \mu_{p1}\big[I(X;Z) - \min(I(U;Y_2), I(X;Z))\big] + \mu_{p2}\min(I(U;Y_2), I(X;Z)) \\ & + \mu_{s1}\big[I(U;Y_2) + I(X;Y_1|U) - I(X;Z)\big] \end{aligned} \tag{6.36}$$

$$L^{\text{in}} = \max_{(U,X)\in\mathcal{F}} \quad \mu_{p1} I(X;Z|U) + \mu_{p2} I(U;Z) + \mu_{s1}\big[I(U;Y_2) + I(X;Y_1|U) - I(X;Z)\big] \tag{6.37}$$

which can be shown by following the analysis in (6.29)-(6.32). The set $\mathcal{F}$ contains (U, X) pairs that satisfy the Markov chain in (6.13). Using (6.36) and (6.37), we have

$$L^{\text{out}} - L^{\text{in}} \geq (\mu_{p2} - \mu_{p1}) \min(I(U; Y_2|Z), I(X; Z|U)) \tag{6.38}$$

where the right hand-side of (6.38) can be strictly positive for certain channel models. In particular, for the degraded Gaussian model we consider in Section 6.3.1, one can find (U, X) such that the right hand-side of (6.38) is strictly positive. This observation implies that the outer bound strictly contains the inner bound.

6.2.2 General Channels

We now consider the general, not necessarily degraded, discrete memoryless multi-receiver wiretap channel with public and confidential messages. We propose an inner bound for the capacity region of the general discrete memoryless multi-receiver wiretap channel as follows.

Theorem 6.3 *An achievable rate region for the discrete memoryless multi-receiver wiretap channel with public and confidential messages is given by the union of rate tuples* $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ *satisfying*

$$R_{s1} \leq \min_{j=1,2} I(U; Y_j|Q) + I(V_1; Y_1|U) - I(U, V_1; Z|Q) \tag{6.39}$$

$$R_{s2} \leq \min_{j=1,2} I(U; Y_j|Q) + I(V_2; Y_2|U) - I(U, V_2; Z|Q) \tag{6.40}$$

$$R_{s1} + R_{s2} \leq \min_{j=1,2} I(U;Y_j|Q) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) - I(U,V_1,V_2;Z|Q) \tag{6.41}$$

$$R_{s1} + R_{p1} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) \tag{6.42}$$

$$R_{s2} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + I(V_2;Y_2|U) \tag{6.43}$$

$$R_{s1} + R_{p1} + R_{s2} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_2;Z|U) \tag{6.44}$$

$$R_{s1} + R_{p1} + R_{s2} \leq \min_{j=1,2} I(U;Y_j) + 2I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) - I(V_1,V_2;Z|U) \tag{6.45}$$

$$R_{s1} + R_{s2} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;Z|U) \tag{6.46}$$

$$R_{s1} + R_{s2} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + 2I(V_2;Y_2|U) - I(V_1;V_2|U) - I(V_1,V_2;Z|U) \tag{6.47}$$

$$R_{s1} + R_{p1} + R_{s2} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) \tag{6.48}$$

$$0 \leq \min_{j=1,2} I(U;Y_j|Q) - I(U;Z|Q) \tag{6.49}$$

$$0 \leq I(V_1;Y_1|U) - I(V_1;Z|U) \tag{6.50}$$

$$0 \leq I(V_2;Y_2|U) - I(V_2;Z|U) \tag{6.51}$$

$$0 \leq I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) - I(V_1,V_2;Z|U) \tag{6.52}$$

for some Q, U, V_1, V_2 *such that*

$$p(q, u, v_1, v_2, x, y_1, y_2, z) = p(q, u)p(v_1, v_2, x|u)p(y_1, y_2, z|x) \tag{6.53}$$

The proof of Theorem 6.3 is given in Appendix 6.5.2. We note that if one sets $Q = \phi, V_2 = U, V_1 = X$ in Theorem 6.3, the achievable rate region in Theorem 6.3 reduces to the one provided in Theorem 6.1. Thus, the achievable scheme in Theorem 6.3 can be seen as a generalization of the achievable scheme in Theorem 6.1, where we achieve this generalization by using Marton's coding and rate-splitting in addition to the superposition coding and binning that were already used for the achievable scheme in Theorem 6.1.

Next, we provide an outline of the achievable scheme in Theorem 6.3. In this achievable scheme, we first divide each public message W_{pj} into three parts as $W_{pj}^1, W_{pj}^2, W_{pj}^3$, where the rates of the messages $W_{pj}^1, W_{pj}^2, W_{pj}^3$ are given by $R_{pj}^1, R_{pj}^2, R_{pj}^3$, respectively, and $R_{pj} = R_{pj}^1 + R_{pj}^2 + R_{pj}^3$. Similarly, we divide each confidential message W_{sj} into two parts as W_{sj}^1, W_{sj}^2, where the rates of the messages W_{sj}^1, W_{sj}^2 are given by R_{sj}^1, R_{sj}^2, respectively, and $R_{sj} = R_{sj}^1 + R_{sj}^2$. The first parts of the public messages, i.e., W_{p1}^1 and W_{p2}^1, are sent through the sequences generated by Q. The second parts of the public messages, i.e., W_{p1}^2 and W_{p2}^2, and the first parts of the confidential messages, i.e., W_{s1}^1 and W_{s2}^1, are sent through the sequences generated by U. Both legitimate receivers decode these sequences, and hence, each legitimate receiver decodes the parts of the other legitimate user's public and confidential messages. The last parts of each public message and each confidential message, i.e.,

W_{pj}^3 and W_{sj}^2, are encoded by the sequences generated through V_j. This encoding is performed by using Marton's coding [11]. Each legitimate receiver, after decoding Q^n and U^n, decodes the sequences V_j^n. The details of the proof is given in Appendix 6.5.2.

6.3 Gaussian MIMO Multi-receiver Wiretap Channels

Here, we consider the Gaussian MIMO multi-receiver wiretap channel which is defined by

$$\mathbf{Y}_j = \mathbf{X} + \mathbf{N}_j, \quad j = 1, 2 \tag{6.54}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{6.55}$$

where the channel input $\mathbf{X}$ is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{6.56}$$

where $\mathbf{S} \succ \mathbf{0}$ and $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2, \mathbf{\Sigma}_Z$, respectively.

In Section 6.3.1, we consider *degraded* Gaussian MIMO multi-receiver wiretap channels for which the noise covariance matrices $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2, \mathbf{\Sigma}_Z$ satisfy the following order

$$\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z \tag{6.57}$$

In a multi-receiver wiretap channel, since the capacity region depends only on the conditional marginal distributions of the transmitter-receiver links, but not on the entire joint distribution of the channel, the correlations among $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ do not affect the capacity region. Thus, without changing the corresponding capacity region, we can adjust the correlation structure among these noise vectors to ensure that they satisfy the Markov chain

$$\mathbf{X} \rightarrow \mathbf{Y}_1 \rightarrow \mathbf{Y}_2 \rightarrow \mathbf{Z} \tag{6.58}$$

which is always possible because of our assumption about the covariance matrices in (6.57).

6.3.1 Degraded Channels

We first provide an inner bound for the capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel with public and confidential messages by using Theorem 6.1. The corresponding achievable rate region is stated in the following theorem.

Theorem 6.4 *An achievable rate region for the degraded Gaussian MIMO multi-receiver wiretap channel with public and confidential messages is given by the union of rate tuples* $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ *satisfying*

$$R_{s2} \leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_2|}{|\mathbf{K} + \mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{K} + \mathbf{\Sigma}_Z|} \tag{6.59}$$

$$R_{s1} + R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{6.60}$$

$$R_{s2} + R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} \tag{6.61}$$

$$R_{s1} + R_{s2} + R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{6.62}$$

$$R_{s1} + R_{s2} + R_{p1} + R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{6.63}$$

where $\mathbf{K}$ *is a positive semi-definite matrix satisfying* $\mathbf{K} \preceq \mathbf{S}$.

This achievable rate region given in Theorem 6.4 can be obtained by evaluating the achievable rate region in Theorem 6.1 for the degraded Gaussian MIMO multi-receiver wiretap channel by using the following selection for $U, \mathbf{X}$: i) U is a zero-mean Gaussian random vector with covariance matrix $\mathbf{S}-\mathbf{K}$, ii) $\mathbf{X} = U + U'$ where U' is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}$, and is independent of U. We note that besides this jointly Gaussian $(U, \mathbf{X})$ selection, there might be other possible $(U, \mathbf{X})$ selections which may yield a larger region than the one obtained by using jointly Gaussian $(U, \mathbf{X})$. However, we show that jointly Gaussian $(U, \mathbf{X})$ selection is sufficient to evaluate the achievable rate region in Theorem 6.1 for the degraded Gaussian MIMO multi-receiver wiretap channel. In other words, jointly Gaussian $(U, \mathbf{X})$ selection exhausts the achievable rate region in Theorem 6.1 for the degraded Gaussian MIMO multi-receiver wiretap channel. This sufficiency result is stated in the following theorem.

Theorem 6.5 *For the degraded Gaussian MIMO multi-receiver wiretap channel, the achievable rate region in Theorem 6.1 is exhausted by jointly Gaussian* $(U, \mathbf{X})$*. In particular, for any non-Gaussian* $(U, \mathbf{X})$*, there exists a Gaussian* $(U^G, \mathbf{X}^G)$ *which yields a larger region than the one obtained by using the non-Gaussian* $(U, \mathbf{X})$*.*

Next, we provide an outer bound for the capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. This outer bound can be obtained by evaluating the outer bound given in Theorem 6.2 for the degraded Gaussian MIMO multi-receiver wiretap channel. This evaluation is tantamount to finding the optimal $(U, \mathbf{X})$ which exhausts the outer bound in Theorem 6.2 for the degraded Gaussian MIMO multi-receiver wiretap channel. We show that jointly Gaussian $(U, \mathbf{X})$ is sufficient to exhaust the outer bound in Theorem 6.2 for the degraded Gaussian MIMO channel. The corresponding outer bound is stated in the following theorem.

Theorem 6.6 *The capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel is contained in the union of rate tuples* $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$ *satisfying*

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{6.64}$$

$$\begin{aligned} R_{s1}+R_{s2} \leq{}& \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \\ & - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{6.65}$$

$$R_{s2}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} \tag{6.66}$$

$$R_{s1}+R_{s2}+R_{p1}+R_{p2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{6.67}$$

where $\mathbf{K}$ *is a positive semi-definite matrix satisfying* $\mathbf{K} \preceq \mathbf{S}$.

The proofs of Theorem 6.5 and Theorem 6.6 are given in Appendix 6.5.4. We prove Theorem 6.5 and Theorem 6.6 by using our methodology that was proposed in Chapter 5 to evaluate single-letter expressions for vector Gaussian models. In particular, to prove Theorem 6.5, we consider the region in Theorem 6.1, and show that for any non-Gaussian $(U, \mathbf{X})$, there exists a Gaussian $(U^G, \mathbf{X}^G)$ which yields a larger region than the one that is obtained by evaluating the region in Theorem 6.1 with the non-Gaussian $(U, \mathbf{X})$. We note that this proof of Theorem 6.5 implies the proof of Theorem 6.6. In particular, since the region in Theorem 6.1 includes all the constraints involved in the outer bound given in Theorem 6.2, the proof of Theorem 6.5 reveals that for any non-Gaussian $(U, \mathbf{X})$, there exists a Gaussian $(U^G, \mathbf{X}^G)$ which yields a larger region than the one that is obtained by evaluating the region in Theorem 6.2 with the non-Gaussian $(U, \mathbf{X})$.

The inner bound in Theorem 6.4 and the outer bound in Theorem 6.6 do not match in general. However, similar to the discrete memoryless case in Section 6.2.1, here also we can specialize the inner and outer bounds for the cases i) $R_{s1} = 0$, ii) $R_{p2} = 0$, and iii) $R_{p1} = R_{p2} = 0$, where they match; yielding the capacity region. These three cases correspond to the extension of Corollaries 6.1, 6.2, 6.3 to the degraded Gaussian MIMO model. Finally, we note that the case $R_{p1} = R_{p2} = 0$ gives us the secrecy capacity region of the degraded Gaussian MIMO model, and in fact, the secrecy capacity region of the general, not necessarily degraded, Gaussian MIMO model was already obtained in Chapter 5.

6.3.2 General Channels

Here we consider the general, i.e., *not necessarily degraded*, Gaussian MIMO multi-receiver wiretap channel with public and confidential messages, and propose an inner bound for the capacity region of the general Gaussian MIMO multi-receiver wiretap channel as follows.

Theorem 6.7 *An achievable rate region for the general Gaussian MIMO multi-receiver wiretap channel with public and confidential messages is given by*

$$\mathrm{conv}\left(\mathcal{R}_{12}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)\cup\mathcal{R}_{21}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)\right) \tag{6.68}$$

where $\mathcal{R}_{21}(\mathbf{K}_0,\mathbf{K}_1,\mathbf{K}_2)$ *is given by the union of rate tuples* $(R_{p1},R_{s1},R_{p2},R_{s2})$ *satisfying*

$$\begin{aligned}
R_{s1} &\le \min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|}+\frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|}\\
&\quad-\frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}-\frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} &(6.69)\\
R_{s2} &\le \min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|}+\frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|}\\
&\quad-\frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} &(6.70)\\
R_{s1}+R_{s2} &\le \min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|}+\frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|}\\
&\quad+\frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|}-\frac{1}{2}\log\frac{|\mathbf{K}_0+\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} &(6.71)\\
R_{s1}+R_{p1} &\le \min_{j=1,2}\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_j|}{|\mathbf{K}_1+\mathbf{K}_2+\mathbf{\Sigma}_j|}+\frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} &(6.72)
\end{aligned}$$

$$R_{s2} + R_{p2} \leq \min_{j=1,2} \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_j|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_j|} + \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{K}_1 + \mathbf{\Sigma}_2|} \tag{6.73}$$

$$R_{s1} + R_{p1} + R_{s2} \leq \min_{j=1,2} \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_j|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_j|} + \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} + \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{K}_1 + \mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_1 + \mathbf{\Sigma}_Z|} \tag{6.74}$$

$$R_{s1} + R_{s2} + R_{p2} \leq \min_{j=1,2} \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_j|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_j|} + \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{K}_1 + \mathbf{\Sigma}_2|} + \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{6.75}$$

$$R_{s1} + R_{p1} + R_{s2} + R_{p2} \leq \min_{j=1,2} \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_j|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_j|} + \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{K}_1 + \mathbf{\Sigma}_2|} + \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{6.76}$$

for some positive semi-definite matrices $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2$ *satisfying* $\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$. $\mathcal{R}_{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ *can be obtained from* $\mathcal{R}_{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ *by swapping the subscripts 1 and 2.*

The proof of Theorem 6.7 is given in Appendix 6.5.5. We obtain Theorem 6.7 by evaluating the achievable rate region given in Theorem 6.3 with jointly Gaussian $(Q, U, V_1, V_2, \mathbf{X})$ having a specific correlation structure. In particular, Q, U are selected in accordance with superposition coding, and V_1, V_2 are encoded by using dirty-paper encoding [12].

We note that the achievable rate region in Theorem 6.4 can be obtained from Theorem 6.7 by considering the region $\mathcal{R}_{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ with $\mathbf{K}_2 = \phi, \mathbf{K}_1 = \mathbf{K}, \mathbf{S} = \mathbf{K}_0 + \mathbf{K}_1$, and eliminating the redundant bounds from the corresponding region.

6.4 Conclusions

In this chapter, we study the multi-receiver wiretap channel with public and confidential messages. First, we consider the degraded discrete memoryless case as well as its MIMO instance. For the degraded case, we obtain inner and outer bounds which match under certain conditions providing the capacity region. Second, we study the general, not necessarily degraded, channels (both discrete memoryless channel and its MIMO instance), and obtain an inner bound for their capacity region.

6.5 Appendix

6.5.1 Proof of Theorem 6.2

We define the following auxiliary random variables

$$U_i = W_{s2} W_{p2} Y_1^{i-1} Z_{i+1}^n, \quad i = 1, \ldots, n \tag{6.77}$$

which satisfy the Markov chains $U_i \to X_i \to Y_{1i} \to Y_{2i} \to Z_i, \forall i$, since the channel is degraded and memoryless. For any $(n, 2^{nR_{p1}}, 2^{nR_{s1}}, 2^{nR_{p2}}, 2^{nR_{s2}})$ code achieving the rate tuple $(R_{p1}, R_{s1}, R_{p2}, R_{s2})$, we have

$$H(W_{sj}, W_{pj} | Y_j^n) \leq n\epsilon_n, \ j = 1, 2 \tag{6.78}$$

$$I(W_{s1}, W_{s2}; Z^n) \leq n\gamma_n \tag{6.79}$$

where $\epsilon_n \to 0, \gamma_n \to 0$ as $n \to \infty$. Equation (6.78) is due to Fano's lemma, and (6.79) is due to the perfect secrecy requirement in (6.1). We note that (6.79) implies the following

$$H(W_{s1}, W_{s2}) \leq H(W_{s1}, W_{s2}, W_{p1}, W_{p2}|Z^n) + n\gamma_n \tag{6.80}$$

We introduce the following lemma which follows from Csiszar-Korner sum identity [3, Lemma 7].

Lemma 6.1

$$\begin{aligned} &I(W; T_1^n|Q) - (W; T_2^n|Q) \\ &\qquad = \sum_{i=1}^{n} I(W; T_{1i}|Q, T_1^{i-1}, T_{2,i+1}^n) - I(W; T_{2i}|Q, T_1^{i-1}, T_{2,i+1}^n) \end{aligned} \tag{6.81}$$

First, we obtain an outer bound for R_{s2} as follows

$$nR_{s2} \leq \sum_{i=1}^{n} I(W_{s2}; Y_{2i}|Y_2^{i-1}, Z_{i+1}^n) - I(W_{s2}; Z_i|Y_2^{i-1}, Z_{i+1}^n) + n(\epsilon_n + \gamma_n) \tag{6.82}$$

$$\leq \sum_{i=1}^{n} I(W_{s2}, W_{p2}, Y_2^{i-1}, Z_{i+1}^n, Y_1^{i-1}; Y_{2i}) - I(W_{s2}, W_{p2}, Y_2^{i-1}, Z_{i+1}^n, Y_1^{i-1}; Z_i)$$

$$+ n(\epsilon_n + \gamma_n) \tag{6.83}$$

$$= \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(U_i; Z_i) + n(\gamma_n + \epsilon_n) \tag{6.84}$$

where (6.82) comes from the converse proof for the secrecy capacity of wiretap channels in [3], and (6.83)-(6.84) come from the following Markov chains

$$W_{s2}, W_{p2}, Y_2^{i-1}, Z_{i+1}^n, Y_1^{i-1} \to Y_{2i} \to Z_i \tag{6.85}$$

$$W_{s2}, W_{p2}, Z_i^n, Y_{2i} \to Y_1^{i-1} \to Y_2^{i-1} \tag{6.86}$$

respectively, which follow from the fact that the channel is degraded and memoryless.

Next, we obtain an outer bound for $R_{s1} + R_{s2}$ as follows

$$n(R_{s1} + R_{s2}) \leq H(W_{s1}, W_{p1}, W_{s2}, W_{p2}|Z^n) + n\gamma_n \tag{6.87}$$

$$\leq I(W_{s1}, W_{p1}; Y_1^n|W_{s2}, W_{p2}) - I(W_{s1}, W_{p1}; Z^n|W_{s2}, W_{p2}) + I(W_{s2}, W_{p2}; Y_2^n)$$

$$- I(W_{s2}, W_{p2}; Z^n) + n(\gamma_n + 2\epsilon_n) \tag{6.88}$$

$$\leq I(W_{s1}, W_{p1}; Y_1^n|W_{s2}, W_{p2}) - I(W_{s1}, W_{p1}; Z^n|W_{s2}, W_{p2})$$

$$+ \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(U_i; Z_i) + n(\gamma_n + 2\epsilon_n) \tag{6.89}$$

$$= \sum_{i=1}^{n} I(W_{s1}, W_{p1}; Y_{1i}|U_i) - I(W_{s1}, W_{p1}; Z_i|U_i) + I(U_i; Y_{2i}) - I(U_i; Z_i)$$

$$+ n(\gamma_n + 2\epsilon_n) \tag{6.90}$$

$$\leq \sum_{i=1}^{n} I(X_i; Y_{1i}|U_i) + I(U_i; Y_{2i}) - I(X_i; Z_i) + n(\gamma_n + 2\epsilon_n) \tag{6.91}$$

where (6.87) comes from (6.80), (6.89) is due to (6.84), (6.90) comes from Lemma 6.1, (6.91) is a consequence of the fact that the channel is memoryless and degraded.

Next, we obtain an outer bound for $R_{p2} + R_{s2}$ as follows

$$n(R_{p2} + R_{s2}) \leq I(W_{s2}, W_{p2}; Y_2^n) + n\epsilon_n \tag{6.92}$$

$$= \sum_{i=1}^{n} I(W_{s2}, W_{p2}; Y_{2i}|Y_2^{i-1}) + n\epsilon_n \tag{6.93}$$

$$= \sum_{i=1}^{n} I(W_{s2}, W_{p2}, Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|Y_2^{i-1}) - I(Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|W_{s2}, W_{p2}, Y_2^{i-1})$$

$$+ n\epsilon_n \tag{6.94}$$

$$\leq \sum_{i=1}^{n} I(W_{s2}, W_{p2}, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n; Y_{2i}) - I(Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|W_{s2}, W_{p2}, Y_2^{i-1})$$

$$+ n\epsilon_n \tag{6.95}$$

$$= \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(Y_1^{i-1}, Z_{i+1}^n; Y_{2i}|W_{s2}, W_{p2}, Y_2^{i-1}) + n\epsilon_n \tag{6.96}$$

$$\leq \sum_{i=1}^{n} I(U_i; Y_{2i}) + n\epsilon_n \tag{6.97}$$

where (6.96) comes from the Markov chain in (6.86).

Finally, we obtain an outer bound for the sum rate $R_{p1} + R_{s1} + R_{p2} + R_{s2}$. To this end, we consider the following

$$n(R_{p1} + R_{s1}) \leq I(W_{p1}, W_{s1}; Y_1^n|W_{p2}, W_{s2}) + n\epsilon_n \tag{6.98}$$

$$= \sum_{i=1}^{n} I(W_{p1}, W_{s1}; Y_{1i}|W_{p2}, W_{s2}, Y_1^{i-1}) + n\epsilon_n \tag{6.99}$$

$$\leq \sum_{i=1}^{n} I(W_{p1}, W_{s1}, Z_{i+1}^n; Y_{1i}|W_{p2}, W_{s2}, Y_1^{i-1}) + n\epsilon_n \tag{6.100}$$

$$= \sum_{i=1}^{n} I(Z_{i+1}^n; Y_{1i}|W_{p2}, W_{s2}, Y_1^{i-1}) + I(W_{p1}, W_{s1}; Y_{1i}|U_i) + n\epsilon_n \tag{6.101}$$

$$\leq \sum_{i=1}^{n} I(Z_{i+1}^n; Y_{1i}|W_{p2}, W_{s2}, Y_1^{i-1}) + I(X_i; Y_{1i}|U_i) + n\epsilon_n \tag{6.102}$$

using which and (6.96), we have

$$
\begin{aligned}
& n(R_{p1}+R_{s1}+R_{p2}+R_{s2}) \\
& \leq \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1},Z_{i+1}^n;Y_{2i}|Y_2^{i-1},W_{s2},W_{p2}) \\
& \quad + I(Z_{i+1}^n;Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n && (6.103) \\
& = \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Z_{i+1}^n;Y_{2i}|Y_2^{i-1},W_{s2},W_{p2}) - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\
& \quad + I(Z_{i+1}^n;Y_{1i}|W_{p2},W_{s2},Y_1^{i-1}) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n && (6.104) \\
& = \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_2^{i-1};Z_i|W_{s2},W_{p2},Z_{i+1}^n) - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\
& \quad + I(Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n && (6.105) \\
& = \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_2^{i-1};Z_i|W_{s2},W_{p2},Z_{i+1}^n) - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\
& \quad + I(Y_2^{i-1},Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n && (6.106) \\
& = \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\
& \quad + I(Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n,Y_2^{i-1}) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n && (6.107) \\
& = \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1};Y_{2i},Z_i|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n) \\
& \quad + I(Y_1^{i-1};Z_i|W_{p2},W_{s2},Z_{i+1}^n,Y_2^{i-1}) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n && (6.108) \\
& = \sum_{i=1}^{n} I(U_i;Y_{2i}) - I(Y_1^{i-1};Y_{2i}|Y_2^{i-1},W_{s2},W_{p2},Z_{i+1}^n,Z_i) + I(X_i;Y_{1i}|U_i) + 2n\epsilon_n \\
& && (6.109)
\end{aligned}
$$

where (6.105) comes from Csiszar-Korner sum identity [3, Lemma 7], (6.106) is due to the Markov chain in (6.86), and (6.108) is a consequence of the Markov chain in

(6.85). Equation (6.109) implies

$$n(R_{p1} + R_{s1} + R_{p2} + R_{s2}) \leq \sum_{i=1}^{n} I(U_i; Y_{2i}) + I(X_i; Y_{1i}|U_i) + 2n\epsilon_n \tag{6.110}$$

Using (6.84), (6.91), (6.97) and (6.110), Theorem 6.2 can be concluded.

6.5.2 Proof of Theorem 6.3

We first consider a more general scenario than the scenario introduced in Section 6.2.2, where the transmitter sends a pair of common public and confidential messages to the legitimate users in addition to a pair of public and confidential messages intended to each legitimate user. Thus, in this case, the transmitter has the message tuple $(W_{p0}, W_{s0}, W_{p1}, W_{s1}, W_{p2}, W_{s2})$, where the common public message W_{p0} and the common confidential message W_{s0} are sent to both legitimate users, and a pair of public and confidential messages (W_{pj}, W_{sj}) are sent to the jth legitimate user, $j = 1, 2$[2]. There is no secrecy concern on the public messages $\{W_{pj}\}_{j=0}^{2}$ while the confidential messages $\{W_{sj}\}_{j=0}^{2}$ need to be transmitted in perfect secrecy:

$$\lim_{n\to\infty} \frac{1}{n} I(W_{s0}, W_{s1}, W_{s2}; Z^n) = 0 \tag{6.111}$$

Next, we prove an achievable rate region for the more general scenario we just introduced.

[2]The inner bound in Theorem 6.3 can also be obtained by using rate-splitting for $\{W_{pj}, W_{sj}\}_{j=1}^{2}$ as mentioned in Section 6.2.2. Here, we introduce a pair of common messages $\{W_{p0}, W_{s0}\}$, because the corresponding scenario results in an achievable scheme that encompasses the one obtained by using rate-splitting.

We fix the joint distribution

$$p(q,u,v_1,v_2,x,y_1,y_2,z) = p(q,u)p(v_1,v_2,x|u)p(y_1,y_2,z|x) \tag{6.112}$$

Next, we divide the common public message W_{p0} into two parts as $W_{p0} = (\tilde{W}_{p0}, \tilde{\tilde{W}}_{p0})$, where the rate of $\tilde{W}_{p0}$ is $\tilde{R}_{p0}$, and the rate of $\tilde{\tilde{W}}_{p0}$ is $\tilde{\tilde{R}}_{p0}$. We use rate-splitting for the common public message because due to [3], we know that rate-splitting might enhance the achievable public and confidential message rate pairs even for the single legitimate user case.

Codebook generation:

- Generate $2^{n\tilde{R}_{p0}}$ length-n sequences q^n through $p(q^n) = \prod_{i=1}^{n} p(q_i)$, and index them as $q^n(\tilde{w}_{p0})$, where $\tilde{w}_{p0} \in \{1,\ldots,2^{n\tilde{R}_{p0}}\}$.

- For each $q^n(\tilde{w}_{p0})$ sequence, generate $2^{n(\tilde{\tilde{R}}_{p0}+R_{s0}+\Delta_0)}$ length-n sequences u^n through $p(u^n|q^n) = \prod_{i=1}^{n} p(u_i|q_i)$, and index them as $u^n(\tilde{w}_{p0}, \tilde{\tilde{w}}_{p0}, w_{s0}, d_0)$, where $\tilde{\tilde{w}}_{p0} \in \{1,\ldots,2^{n\tilde{\tilde{R}}_{p0}}\}, w_{s0} \in \{1,\ldots,2^{nR_{s0}}\}, d_0 \in \{1,\ldots,2^{n\Delta_0}\}$.

- For each $u^n(\tilde{w}_{p0}, \tilde{\tilde{w}}_{p0}, w_{s0}, d_0)$ sequence, generate $2^{n(R_{pj}+R_{sj}+\Delta_j+L_j)}$ length-n sequences v_j^n through $p(v_j^n|u^n) = \prod_{i=1}^{n} p(v_{ji}|u_i)$, and index them as

$$v_j^n(\tilde{w}_{p0}, \tilde{\tilde{w}}_{p0}, w_{s0}, d_0, w_{pj}, w_{sj}, d_j, l_j) \tag{6.113}$$

where $w_{pj} \in \{1,\ldots,2^{nR_{pj}}\}, w_{sj} \in \{1,\ldots,2^{nR_{sj}}\}$, $d_j \in \{1,\ldots,2^{n\Delta_j}\}, l_j \in \{1,\ldots,2^{nL_j}\}$.

Encoding:

Assume $(w_{p0}, w_{s0}, w_{p1}, w_{s1}, w_{p2}, w_{s2})$ is the message to be transmitted. Randomly pick d_0, d_1, d_2. Next, we find an (l_1, l_2) pair such that the corresponding sequence tuple (q^n, u^n, v_1^n, v_2^n) is jointly typical. Due to mutual covering lemma [63], if L_1, L_2 satisfy

$$L_1 + L_2 \geq I(V_1; V_2|U) \tag{6.114}$$

with high probability, there will be at least one such l_1, l_2 pair.

Decoding:

The jth legitimate user decodes $(w_{p0}, w_{s0}, d_0, w_{pj}, w_{sj}, d_j)$ in two steps. In the first step, it decodes (w_{p0}, w_{s0}, d_0) by looking for the unique (q^n, u^n) pair such that (q^n, u^n, y_j^n) is jointly typical. In the second step, given that (w_{p0}, w_{s0}, d_0) is decoded correctly in the first step, the jth legitimate user decodes (w_{sj}, w_{pj}, d_j) by looking for the unique (q^n, u^n, v_j^n) tuple such that (q^n, u^n, v_j^n, y_j^n) is jointly typical. If the following conditions are satisfied,

$$R_{p0} + R_{s0} + \Delta_0 \leq \min_{j=1,2} I(U; Y_j) \tag{6.115}$$

$$\tilde{\tilde{R}}_{p0} + R_{s0} + \Delta_0 \leq I(U; Y_1|Q) \tag{6.116}$$

$$R_{p1} + R_{s1} + \Delta_1 + L_1 \leq I(V_1; Y_1|U) \tag{6.117}$$

$$\tilde{\tilde{R}}_{p0} + R_{s0} + \Delta_0 \leq I(U; Y_2|Q) \tag{6.118}$$

$$R_{p2} + R_{s2} + \Delta_2 + L_2 \leq I(V_2; Y_2|U) \tag{6.119}$$

both legitimate users decode their messages with vanishingly small probability of error.

Equivocation computation:

We now show that the proposed coding scheme satisfies the perfect secrecy requirement on the confidential messages given by (6.111). We start as follows.

$$
\begin{aligned}
&H(W_{s0}, W_{s1}, W_{s2}|Z^n) \geq H(W_{s0}, W_{s1}, W_{s2}|Z^n, Q^n) \\
&= H(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n) \\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \qquad (6.120) \\
&= H(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Q^n) \\
&\quad - I(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2; Z^n|Q^n) \\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \qquad (6.121) \\
&= H(W_{s0}, W_{s1}, W_{s2}) + H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2) \\
&\quad - I(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2; Z^n|Q^n) \\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \qquad (6.122) \\
&= H(W_{s0}, W_{s1}, W_{s2}) + n(\tilde{\tilde{R}}_{p0} + R_{p1} + R_{p2} + \Delta_0 + \Delta_1 + \Delta_2) \\
&\quad - I(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2; Z^n|Q^n) \\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \qquad (6.123) \\
&\geq H(W_{s0}, W_{s1}, W_{s2}) + n(\tilde{\tilde{R}}_{p0} + R_{p1} + R_{p2} + \Delta_0 + \Delta_1 + \Delta_2) \\
&\quad - I(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2, U^n, V_1^n, V_2^n; Z^n|Q^n) \\
&\quad - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \qquad (6.124)
\end{aligned}
$$

$$= H(W_{s0}, W_{s1}, W_{s2}) + n(\tilde{\tilde{R}}_{p0} + R_{p1} + R_{p2} + \Delta_0 + \Delta_1 + \Delta_2)$$
$$- I(U^n, V_1^n, V_2^n; Z^n|Q^n) - H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \tag{6.125}$$

$$\geq H(W_{s0}, W_{s1}, W_{s2}) + n(\tilde{\tilde{R}}_{p0} + R_{p1} + R_{p2} + \Delta_0 + \Delta_1 + \Delta_2)$$
$$- n(I(U, V_1, V_2; Z|Q) + \gamma_{1n})$$
$$- H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \tag{6.126}$$

where (6.122)-(6.123) follow from the facts that the messages

$$W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2 \tag{6.127}$$

are independent among themselves, uniformly distributed, and also are independent of Q^n, (6.125) stems from the fact that given the codewords (Q^n, U^n, V_1^n, V_2^n), $(W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2)$ and Z^n are independent, (6.126) comes from the fact that

$$I(U^n, V_1^n, V_2^n; Z^n|Q^n) \leq nI(U, V_1, V_2; Z|Q) + n\gamma_{1n} \tag{6.128}$$

where $\gamma_{1n} \to 0$ as $n \to \infty$. The bound in (6.128) can be shown by following the analysis in [64]. Next, we consider the conditional entropy term in (6.126). To this end, we introduce the following lemma.

Lemma 6.2 *We have*

$$H(W_{p1}, W_{p2}, D_1, D_2 | Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}, \tilde{\tilde{W}}_{p0}, D_0) \leq n\gamma_{2n} \tag{6.129}$$

where $\gamma_{2n} \to 0$ *as* $n \to \infty$*, if the following conditions are satisfied.*

$$R_{p1} + \Delta_1 + L_1 + R_{p2} + \Delta_2 + L_2 \leq I(V_1, V_2; Z|U) + I(V_1; V_2|U) \tag{6.130}$$

$$R_{p1} + \Delta_1 + L_1 \leq I(V_1; Z, V_2|U) \tag{6.131}$$

$$R_{p2} + \Delta_2 + L_2 \leq I(V_2; Z, V_1|U) \tag{6.132}$$

The proof of Lemma 6.2 is given in Appendix 6.5.3. This lemma implies the following.

Corollary 6.4 *We have*

$$H(\tilde{\tilde{W}}_{p0}, D_0 | Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \leq n\gamma_{3n} \tag{6.133}$$

where $\gamma_{3n} \to 0$ *as* $n \to \infty$*, if the following condition is satisfied.*

$$\tilde{\tilde{R}}_{p0} + \Delta_0 \leq I(U; Z|Q) \tag{6.134}$$

Now, we set the rates $\tilde{\tilde{R}}_{p0}, \Delta_0, R_{p1}, \Delta_1, L_1, R_{p2}, \Delta_2, L_2$ as follows.

$$\tilde{\tilde{R}}_{p0} + \Delta_0 = I(U; Z|Q) - \epsilon \tag{6.135}$$

$$L_1 + L_2 = I(V_1; V_2|U) + \frac{\epsilon}{2} \tag{6.136}$$

$$R_{p1} + \Delta_1 + R_{p2} + \Delta_2 = I(V_1, V_2; Z|U) - \epsilon \tag{6.137}$$

$$R_{p1} + \Delta_1 + L_1 < I(V_1; Z, V_2|U) \tag{6.138}$$

$$R_{p2} + \Delta_2 + L_2 < I(V_2; Z, V_1|U) \tag{6.139}$$

In view of Lemma 6.2 and Corollary 6.4, the selections of $\tilde{\tilde{R}}_{p0}, \Delta_0, R_{p1}, \Delta_1, L_1, R_{p2}, \Delta_2, L_2$ in (6.135)-(6.139) imply that

$$H(\tilde{\tilde{W}}_{p0}, W_{p1}, W_{p2}, D_0, D_1, D_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}) \leq n\gamma_{2n} \tag{6.140}$$

using which and (6.135)-(6.137) in (6.126), we get

$$\begin{aligned} H(W_{s0}, W_{s1}, W_{s2}|Z^n) &\geq H(W_{s0}, W_{s1}, W_{s2}) + n(\tilde{\tilde{R}}_{p0} + R_{p1} + R_{p2} + \Delta_0 + \Delta_1 + \Delta_2) \\ &\quad - n(I(U, V_1, V_2; Z|Q) + \gamma_{1n}) - n\gamma_{2n} \qquad (6.141) \\ &= H(W_{s0}, W_{s1}, W_{s2}) - n\frac{3\epsilon}{2} - n(\gamma_{1n} + \gamma_{2n} + \gamma_{3n}) \qquad (6.142) \end{aligned}$$

which implies that the proposed coding scheme satisfies the perfect secrecy requirement on the confidential messages; completing the equivocation computation.

Hence, we show that rate tuples $(R_{p0}, R_{s0}, R_{p1}, R_{s1}, R_{p2}, R_{s2})$ satisfying

$$L_1 + L_2 = I(V_1; V_2|U) \tag{6.143}$$

$$R_{p0} + R_{s0} + \Delta_0 \leq \min_{j=1,2} I(U; Y_j) \tag{6.144}$$

$$\tilde{\tilde{R}}_{p0} + R_{s0} + \Delta_0 \leq \min_{j=1,2} I(U; Y_j|Q) \tag{6.145}$$

$$R_{p1} + R_{s1} + \Delta_1 + L_1 \leq I(V_1; Y_1|U) \tag{6.146}$$

$$R_{p2} + R_{s2} + \Delta_2 + L_2 \leq I(V_2; Y_2|U) \tag{6.147}$$

$$\tilde{\tilde{R}}_{p0} + \Delta_0 = I(U; Z|Q) \tag{6.148}$$

$$R_{p1} + \Delta_1 + R_{p2} + \Delta_2 = I(V_1, V_2; Z|U) \tag{6.149}$$

$$R_{p1} + \Delta_1 + L_1 \leq I(V_1; Z, V_2|U) \tag{6.150}$$

$$R_{p2} + \Delta_2 + L_2 \leq I(V_2; Z, V_1|U) \tag{6.151}$$

are achievable. Next, one can obtain the achievable rate region in Theorem 6.3 by using Fourier-Motzkin elimination in conjunction with the fact that since the common public and confidential messages W_{p0}, W_{s0} are decoded by both users, they can be converted into public and confidential messages $(W_{p1}, W_{s1}, W_{p2}, W_{s2})$ of the legitimate users.

6.5.3 Proof of Lemma 6.2

Assume that, given $(W_{s0} = w_{s0}, W_{s1} = w_{s1}, W_{s2} = w_{s1}, W_{p0} = w_{p0})$, the eavesdropper tries to decode $W_{p1}, D_1, L_1, W_{p2}, D_2, L_2$ by looking for the unique (V_1^n, V_2^n) such that $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical. There are four possible error events:

- $\mathcal{E}_0^e = \{(q^n, u^n, v_1^n, v_2^n, z^n)$ is not jointly typical for the transmitted $(q^n, u^n, v_1^n, v_2^n)\}$,
- $\mathcal{E}_i^e = \{(W_{p1}, D_1, L_1) = (1,1,1), (W_{p2}, D_2, L_2) \neq (1,1,1)$, and the corresponding tuple $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical$\}$,
- $\mathcal{E}_{ii}^e = \{(W_{p1}, D_1, L_1) \neq (1,1,1), (W_{p2}, D_2, L_2) = (1,1,1)$, and the corresponding tuple $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical$\}$,
- $\mathcal{E}_{iii}^e = \{(W_{p1}, D_1, L_1) \neq (1,1,1), (W_{p2}, D_2, L_2) \neq (1,1,1)$, and the corresponding tuple $(q^n, u^n, v_1^n, v_2^n, z^n)$ is jointly typical$\}$,

Thus, the probability of decoding error at the eavesdropper is given by

$$\Pr[\mathcal{E}^e] \leq \Pr[\mathcal{E}_0^e] + \Pr[\mathcal{E}_i^e] + \Pr[\mathcal{E}_{ii}^e] + \Pr[\mathcal{E}_{iii}^e] \tag{6.152}$$

$$\leq \epsilon_{1n} + \Pr[\mathcal{E}_i^e] + \Pr[\mathcal{E}_{ii}^e] + \Pr[\mathcal{E}_{iii}^e] \tag{6.153}$$

where we first use the union bound, and next the fact that $\Pr[\mathcal{E}_0^e] \leq \epsilon_{1n}$ for some ϵ_{1n} satisfying $\epsilon_{1n} \to 0$ as $n \to \infty$, which follows from the properties of the jointly typical sequences [22]. Next, we consider $\Pr[\mathcal{E}_i^e]$ as follows

$$\Pr[\mathcal{E}_i^e] \leq \sum_{(w_{p2},d_2,l_2)\neq(1,1,1)} \Pr[(q^n, u^n, v_1^n, V_2^n, Z^n) \in \mathcal{A}_\epsilon^n] \tag{6.154}$$

$$\leq \sum_{(w_{p2},d_2,l_2)\neq(1,1,1)} \sum_{(v_2^n,z^n)\in\mathcal{A}_\epsilon^n} p(v_2^n|u^n) p(z^n|u^n, v_1^n) \tag{6.155}$$

$$\leq \sum_{(w_{p2},d_2,l_2)\neq(1,1,1)} \sum_{(v_2^n,z^n)\in\mathcal{A}_\epsilon^n} 2^{-n(H(V_2|U)-\gamma_\epsilon)} 2^{-n(H(Z|U,V_1)-\gamma_\epsilon)} \tag{6.156}$$

$$= \sum_{(w_{p2},d_2,l_2)\neq(1,1,1)} |\mathcal{A}_\epsilon^n| 2^{-n(H(V_2|U)-\gamma_\epsilon)} 2^{-n(H(Z|U,V_1)-\gamma_\epsilon)} \tag{6.157}$$

$$\leq \sum_{(w_{p2},d_2,l_2)\neq(1,1,1)} 2^{n(H(V_2,Z|U,V_1)+\gamma_\epsilon)} 2^{-n(H(V_2|U)-\gamma_\epsilon)} 2^{-n(H(Z|U,V_1)-\gamma_\epsilon)} \tag{6.158}$$

$$\leq 2^{n(R_{p2}+\Delta_2+L_2)} 2^{-n(I(V_2;Z,V_1|U)-3\gamma_\epsilon)} \tag{6.159}$$

where $\mathcal{A}_\epsilon^n$ denotes the typical set, γ_ϵ is a constant that is a function of ϵ, and satisfies $\gamma_\epsilon \to 0$ as $\epsilon \to 0$, (6.155) is due to the joint distribution of (q^n, u^n, v_1^n, v_2^n), (6.156) is due to the properties of the typical sequences [22], and (6.158) comes from the bounds on the size of $\mathcal{A}_\epsilon^n$ [22]. Equation (6.159) implies that $\Pr[\mathcal{E}_i^e] \to 0$ as $n \to \infty$ if the following condition is satisfied.

$$R_{p2} + \Delta_2 + L_2 < I(V_2; Z, V_1|U) - 3\gamma_\epsilon \tag{6.160}$$

Similarly, we can show that $\Pr[\mathcal{E}_{ii}^e] \to 0$ as $n \to \infty$ if the following condition is satisfied.

$$R_{p1} + \Delta_1 + L_1 < I(V_1; Z, V_2|U) - 3\gamma_\epsilon \tag{6.161}$$

Next, we consider $\Pr[\mathcal{E}_{iii}^e]$ as follows

$$\Pr[\mathcal{E}_{iii}^e] \leq \sum_{\substack{(w_{p1},d_1,l_1)\neq(1,1,1)\\(w_{p2},d_2,l_2)\neq(1,1,1)}} \Pr[(q^n, u^n, V_1^n, V_2^n, Z^n) \in \mathcal{A}_\epsilon^n] \tag{6.162}$$

$$\leq \sum_{\substack{(w_{p1},d_1,l_1)\neq(1,1,1)\\(w_{p2},d_2,l_2)\neq(1,1,1)}} \sum_{(v_1^n,v_2^n,z^n)\in\mathcal{A}_\epsilon^n} p(v_1^n|u^n)p(v_2^n|u^n)p(z^n|u^n) \tag{6.163}$$

$$\leq \sum_{\substack{(w_{p1},d_1,l_1)\neq(1,1,1)\\(w_{p2},d_2,l_2)\neq(1,1,1)}} \sum_{(v_1^n,v_2^n,z^n)\in\mathcal{A}_\epsilon^n} 2^{-n(H(V_1|U)-\gamma_\epsilon)}2^{-n(H(V_2|U)-\gamma_\epsilon)}2^{-n(H(Z|U)-\gamma_\epsilon)} \tag{6.164}$$

$$= \sum_{\substack{(w_{p1},d_1,l_1)\neq(1,1,1)\\(w_{p2},d_2,l_2)\neq(1,1,1)}} |\mathcal{A}_\epsilon^n|2^{-n(H(V_1|U)+H(V_2|U)+H(Z|U)-3\gamma_\epsilon)} \tag{6.165}$$

$$\leq \sum_{\substack{(w_{p1},d_1,l_1)\neq(1,1,1)\\(w_{p2},d_2,l_2)\neq(1,1,1)}} 2^{n(H(V_1,V_2,Z|U)+\gamma_\epsilon)}2^{-n(H(V_1|U)+H(V_2|U)+H(Z|U)-3\gamma_\epsilon)} \tag{6.166}$$

$$\leq 2^{n(R_{p1}+\Delta_1+L_1+R_{p2}+\Delta_2+L_2)}2^{-n(I(V_1,V_2;Z|U)+I(V_2;V_1|U)-4\gamma_\epsilon)} \tag{6.167}$$

where (6.163) is due to the joint distribution of (q^n, u^n, v_1^n, v_2^n), (6.164) stems from the properties of the typical sequences [22], and (6.166) comes from the bounds on the size of $\mathcal{A}_\epsilon^n$ [22]. Equation (6.167) implies that $\Pr[\mathcal{E}_{iii}^e]$ vanishes as $n \to \infty$ if the following condition is satisfied.

$$R_{p1} + \Delta_1 + L_1 + R_{p2} + \Delta_2 + R_{p2} < I(V_1, V_2; Z|U) + I(V_2; V_1|U) - 4\gamma_\epsilon \tag{6.168}$$

Thus, we show that if the rates $(R_{p1}, \Delta_1, L_1, R_{p2}, \Delta_2, L_2)$ satisfy (6.160), (6.161),(6.168), the eavesdropper can decode $W_{p1}, D_1, L_1, W_{p2}, D_2, L_2$ by using its knowledge of $(W_{s0}, W_{s1}, W_{s2}, W_{p0})$, i.e., $\Pr[\mathcal{E}^e]$ vanishes as $n \to \infty$. In view of this fact, using Fano's lemma, we get

$$H(W_{p1}, D_1, L_1, W_{p2}, D_2, L_2|Z^n, Q^n, W_{s0}, W_{s1}, W_{s2}, W_{p0}, D_0) \leq n\gamma_{2n} \tag{6.169}$$

where $\gamma_{2n} \to 0$ as $n \to \infty$; completing the proof.

6.5.4 Proofs of Theorems 6.5 and 6.6

First, we prove Theorem 6.5 by showing that for any $(U, V, \mathbf{X})$, there exists a Gaussian $(U^G, V^G, \mathbf{X}^G)$ which provides a larger region. Essentially, this proof will also yield a proof for Theorem 6.6 because the outer bound in Theorem 6.2 is defined by the same inequalities that define the inner bound given in Theorem 6.1 except for the inequality in (6.6). Thus, we only provide the proof of Theorem 6.5. We also note that in this proof, we will use the methodology we devised in Chapter 5 to evaluate single-letter expressions for vector Gaussian models.

First step: We consider the bound on R_{s2} given in (6.3) as follows

$$R_{s2} \leq I(U;\mathbf{Y}_2) - I(U;\mathbf{Z}) \tag{6.170}$$

$$= [h(\mathbf{Y}_2) - h(\mathbf{Z})] + [h(\mathbf{Z}|U) - h(\mathbf{Y}_2|U)] \tag{6.171}$$

$$\leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{S}+\mathbf{\Sigma}_Z|} + [h(\mathbf{Z}|U) - h(\mathbf{Y}_2|U)] \tag{6.172}$$

where (6.172) follows from the worst additive noise lemma [36, Lemma II.2]. Next, we consider the remaining terms in (6.172) as follows

$$h(\mathbf{Z}|U) - h(\mathbf{Y}_2|U) = \frac{1}{2}\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \mathbf{J}(\mathbf{X}+\mathbf{N}|U)d\mathbf{\Sigma}_N \tag{6.173}$$

which follows from Lemma 5.17, and $\mathbf{N}$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N$ satisfying $\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_Z$. Using Lemma 5.16, we have

$$\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2 \preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}|U) - \mathbf{\Sigma}_N \preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|U) - \mathbf{\Sigma}_Z \tag{6.174}$$

for any $\mathbf{\Sigma}_N$ satisfying $\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_Z$, which imply

$$\left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|U) - \mathbf{\Sigma}_Z + \mathbf{\Sigma}_N\right]^{-1} \preceq \mathbf{J}(\mathbf{X}+\mathbf{N}|U) \preceq \left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2 + \mathbf{\Sigma}_N\right]^{-1} \tag{6.175}$$

Using these inequalities in (6.173) in conjunction with Lemma 5.8, we get

$$\begin{aligned} \frac{1}{2}\log\frac{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|U)|}{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z) - \mathbf{\Sigma}_Z + \mathbf{\Sigma}_2|} &\leq h(\mathbf{Z}|U) - h(\mathbf{Y}_2|U) \\ &\leq \frac{1}{2}\log\frac{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2)|} \end{aligned} \tag{6.176}$$

which can be expressed as

$$f(0) \leq h(\mathbf{Z}|U) - h(\mathbf{Y}_2|U) \leq f(1) \tag{6.177}$$

where $f(t)$ is defined as

$$f(t) = \frac{1}{2}\log\frac{|\mathbf{K}_1(t) + \mathbf{\Sigma}_Z|}{|\mathbf{K}_1(t) + \mathbf{\Sigma}_2|}, \quad 0 \leq t \leq 1 \tag{6.178}$$

and $\mathbf{K}_1(t)$ is given by

$$\mathbf{K}_1(t) = (1-t)\left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|U) - \mathbf{\Sigma}_Z\right] + t\left[\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2\right] \tag{6.179}$$

Since $f(t)$ is continuous in t, due to the intermediate value theorem, there exists a

t_1^* such that $0 \leq t_1^* \leq 1$, and

$$f(t_1^*) = h(\mathbf{Z}|U) - h(\mathbf{Y}_2|U) = \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_1 + \mathbf{\Sigma}_2|} \tag{6.180}$$

where $\mathbf{K}_1 = \mathbf{K}_1(t_1^*)$. Since $0 \leq t_1^* \leq 1$, $\mathbf{K}_1$ satisfies

$$\mathbf{J}^{-1}(\mathbf{X} + \mathbf{N}_2|U) - \mathbf{\Sigma}_2 \preceq \mathbf{K}_1 \preceq \mathbf{J}^{-1}(\mathbf{X} + \mathbf{N}_Z|U) - \mathbf{\Sigma}_Z \tag{6.181}$$

in view of (6.179). Moreover, we have

$$\mathbf{K}_1 \preceq \mathbf{J}^{-1}(\mathbf{X} + \mathbf{N}_Z|U) - \mathbf{\Sigma}_Z \tag{6.182}$$

$$\preceq \mathrm{Cov}(\mathbf{X} + \mathbf{N}_Z|U) - \mathbf{\Sigma}_Z \tag{6.183}$$

$$\preceq \mathrm{Cov}(\mathbf{X} + \mathbf{N}_Z) - \mathbf{\Sigma}_Z \tag{6.184}$$

$$\preceq \mathbf{S} \tag{6.185}$$

where (6.183) comes from Lemma 5.13 and (6.184) is due to the fact that conditioning reduces the MMSE matrix in a positive semi-definite ordering sense. Thus, in view of (6.181) and (6.185), $\mathbf{K}_1$ satisfies

$$\mathbf{J}^{-1}(\mathbf{X} + \mathbf{N}_2|U) - \mathbf{\Sigma}_2 \preceq \mathbf{K}_1 \preceq \mathbf{S} \tag{6.186}$$

Now, using (6.180) in (6.172), we get the following bound on R_{s2}

$$R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} \tag{6.187}$$

which completes the first step of the proof.

Second step: We consider the bound on $R_{s1}+R_{s2}$ given in (6.4) as follows

$$\begin{aligned} R_{s1}+R_{s2} &\leq I(U;\mathbf{Y}_2) + I(\mathbf{X};\mathbf{Y}_1|U) - I(\mathbf{X};\mathbf{Z}) && (6.188)\\ &= [h(\mathbf{Y}_2)-h(\mathbf{Z})] + [h(\mathbf{Y}_1|U)-h(\mathbf{Y}_2|U)] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} && (6.189)\\ &\leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{S}+\mathbf{\Sigma}_Z|} + [h(\mathbf{Y}_1|U)-h(\mathbf{Y}_2|U)] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} && (6.190)\end{aligned}$$

where (6.190) comes from the worst additive noise lemma [36, Lemma II.2]. Next, we consider the remaining term in (6.190) as follows

$$h(\mathbf{Y}_2|U) - h(\mathbf{Y}_1|U) = \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} \mathbf{J}(\mathbf{X}+\mathbf{N}|U)d\mathbf{\Sigma}_N \tag{6.191}$$

which follows from Lemma 5.17, and $\mathbf{N}$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N$ satisfying $\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2$. For any Gaussian random vector $\mathbf{N}$ with $\mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2$, we have

$$\begin{aligned} \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}|U) - \mathbf{\Sigma}_N &\preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_2|U) - \mathbf{\Sigma}_2 && (6.192)\\ &\preceq \mathbf{K}_1 && (6.193)\end{aligned}$$

where (6.192) is due to Lemma 5.16, and (6.193) comes from (6.186). Equation (6.193) implies

$$\mathbf{J}(\mathbf{X}+\mathbf{N}|U) \succeq (\mathbf{K}_1+\mathbf{\Sigma}_N)^{-1}, \quad \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2 \tag{6.194}$$

Using (6.194) in (6.191) in conjunction with Lemma 5.8, we have

$$h(\mathbf{Y}_2|U) - h(\mathbf{Y}_1|U) \geq \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} (\mathbf{K}_1+\mathbf{\Sigma}_N)^{-1} d\mathbf{\Sigma}_N \tag{6.195}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_1|} \tag{6.196}$$

Using (6.196) in (6.190), we get

$$R_{s1}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{6.197}$$

which completes the second step of the proof.

Third step: We consider the bound on $R_{s2}+R_{p2}$ given in (6.5) as follows

$$R_{p2}+R_{s2} \leq I(U;\mathbf{Y}_2) \tag{6.198}$$

$$\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| - h(\mathbf{Y}_2|U) \tag{6.199}$$

where (6.199) comes from the maximum entropy theorem [22]. Next, we consider

the remaining term in (6.199). Using (6.180), we have

$$h(\mathbf{Y}_2|U) = h(\mathbf{Z}|U) - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \tag{6.200}$$

$$\geq \frac{1}{2}\log|(2\pi e)\mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}_Z|U)| - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \tag{6.201}$$

$$\geq \frac{1}{2}\log|(2\pi e)(\mathbf{K}_1+\mathbf{\Sigma}_Z)| - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \tag{6.202}$$

$$= \frac{1}{2}\log|(2\pi e)(\mathbf{K}_1+\mathbf{\Sigma}_2)| \tag{6.203}$$

where (6.201) is due to Lemma 5.20, and (6.202) comes from (6.182) and monotonicity of $|\cdot|$ in positive semi-definite matrices. Using (6.203) in (6.199), we get

$$R_{p2}+R_{s2} \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} \tag{6.204}$$

which completes the third step of the proof.

Fourth step: We consider the bound in (6.6) as follows

$$R_{s1}+R_{p2}+R_{s2} \leq I(U;\mathbf{Y}_2)+I(\mathbf{X};\mathbf{Y}_1|U)-I(\mathbf{X};\mathbf{Z}|U) \tag{6.205}$$

$$= h(\mathbf{Y}_2)-h(\mathbf{Y}_2|U)+[h(\mathbf{Y}_1|U)-h(\mathbf{Z}|U)]-\frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \tag{6.206}$$

$$\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)|-h(\mathbf{Y}_2|U)+[h(\mathbf{Y}_1|U)-h(\mathbf{Z}|U)]-\frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \tag{6.207}$$

$$\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)|-\frac{1}{2}\log|(2\pi e)(\mathbf{K}_1+\mathbf{\Sigma}_2)|+[h(\mathbf{Y}_1|U)-h(\mathbf{Z}|U)] - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \tag{6.208}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + [h(\mathbf{Y}_1|U) - h(\mathbf{Y}_2|U)] + [h(\mathbf{Y}_2|U) - h(\mathbf{Z}|U)]$$
$$- \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \tag{6.209}$$
$$= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + [h(\mathbf{Y}_1|U) - h(\mathbf{Y}_2|U)] + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \tag{6.210}$$
$$\leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} \tag{6.211}$$
$$= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{6.212}$$

where (6.207) comes from the maximum entropy theorem [22], (6.208) comes from (6.203), (6.210) is due to (6.180), and (6.211) comes from (6.196).

Fifth step: We consider the bound in (6.7) as follows

$$R_{p1} + R_{s1} + R_{p2} + R_{s2} \leq I(U;\mathbf{Y}_2) + I(\mathbf{X};\mathbf{Y}_1|U) \tag{6.213}$$
$$= h(\mathbf{Y}_2) + [h(\mathbf{Y}_1|U) - h(\mathbf{Y}_2|U)] - \frac{1}{2}\log|(2\pi e)\mathbf{\Sigma}_1| \tag{6.214}$$
$$\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| + [h(\mathbf{Y}_1|U) - h(\mathbf{Y}_2|U)] - \frac{1}{2}\log|(2\pi e)\mathbf{\Sigma}_1| \tag{6.215}$$
$$\leq \frac{1}{2}\log|(2\pi e)(\mathbf{S}+\mathbf{\Sigma}_2)| + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} - \frac{1}{2}\log|(2\pi e)\mathbf{\Sigma}_1| \tag{6.216}$$
$$= \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{K}_1+\mathbf{\Sigma}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_1+\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{6.217}$$

where (6.215) comes from the maximum entropy theorem [22], and (6.216) comes from (6.196).

Hence, we have shown that for any feasible $(U, \mathbf{X})$, there exists a Gaussian $(U^G, \mathbf{X}^G)$ which yields a larger rate region. This completes the proof.

6.5.5 Proof of Theorem 6.7

We now obtain an alternative rate region by using the one given in Theorem 6.3, which is more amenable for evaluation for the Gaussian MIMO channel. We note that the following region is included in the one given by Theorem 6.3

$$R_{s1} \leq \min_{j=1,2} I(U;Y_j|Q) + I(V_1;Y_1|U) - I(U;Z|Q) - I(V_1;Z,V_2|U) \tag{6.218}$$

$$R_{s2} \leq \min_{j=1,2} I(U;Y_j|Q) + I(V_2;Y_2|U) - I(U,V_2;Z|Q) \tag{6.219}$$

$$\sum_{j=1}^{2} R_{sj} \leq \min_{j=1,2} I(U;Y_j|Q) + \sum_{j=1}^{2} I(V_j;Y_j|U) - I(V_1;V_2|U) - I(U,V_1,V_2;Z|Q) \tag{6.220}$$

$$R_{s1} + R_{p1} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) - I(V_1;V_2|U) \tag{6.221}$$

$$R_{s2} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + I(V_2;Y_2|U) \tag{6.222}$$

$$\sum_{j=1}^{2} R_{sj} + R_{p1} \leq \min_{j=1,2} I(U;Y_j) + \sum_{j=1}^{2} I(V_j;Y_j|U) - I(V_1;V_2|U) - I(V_2;Z|U) \tag{6.223}$$

$$\sum_{j=1}^{2} R_{sj} + R_{p2} \leq \min_{j=1,2} I(U;Y_j) + \sum_{j=1}^{2} I(V_j;Y_j|U) - I(V_1;V_2|U) - I(V_1;Z|U,V_2) \tag{6.224}$$

$$\sum_{j=1}^{2} R_{sj} + R_{pj} \leq \min_{j=1,2} I(U;Y_j) + I(V_1;Y_1|U) + I(V_2;Y_2|U) - I(V_1;V_2|U) \tag{6.225}$$

$$0 \leq \min_{j=1,2} I(U;Y_j|Q) - I(U;Z|Q) \tag{6.226}$$

$$0 \leq \min\{I(V_1;Y_1|U) - I(V_1;Z,V_2|U), I(V_2;Y_2|U) - I(V_2;Z|U)\} \tag{6.227}$$

where we can remove the constraints given by (6.226)-(6.227) without enlarging the region given by (6.218)-(6.225). We denote the region defined by (6.218)-(6.225) by $\mathcal{R}_{21}$. $\mathcal{R}_{12}$ can be obtained by swapping the subscripts 1 and 2 in $\mathcal{R}_{12}$. Hence, we obtain the achievable rate region $\mathcal{R}$:

$$\mathcal{R} = \text{conv}\left(\mathcal{R}_{12} \cup \mathcal{R}_{21}\right) \tag{6.228}$$

We note that for the achievable rate region $\mathcal{R}_{21}$, the transmitter first encodes V_2^n, and then, next using the non-causal knowledge of V_2^n, encodes V_1^n, i.e., uses Gelfand-Pinsker encoding for V_2^n.

Next, we obtain an achievable rate region for the Gaussian MIMO multi-receiver wiretap channel with public and confidential messages. We provide this achievable rate region by evaluating the regions $\mathcal{R}_{12}$ and $\mathcal{R}_{21}$ with a specific choice of $Q, U, V_1, V_2, \mathbf{X}$. In particular, to evaluate $\mathcal{R}_{21}$, we use the following selection for $Q, U, V_1, V_2, \mathbf{X}$:

- Q is a zero-mean Gaussian random vector with covariance matrix $\mathbf{S} - \mathbf{K}_0 - \mathbf{K}_1 - \mathbf{K}_2$, where $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2$ are positive semi-definite matrices satisfying $\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$,

- $U = Q + Q'$, where Q' is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}_0$, and is independent of Q,

- $V_2 = U + U_2$, where U_2 is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}_2$, and is independent of Q, Q',

- $V_1 = U_1 + \mathbf{A}U_2 + U$, where U_1 is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}_1$, is independent of Q, Q', U_2, and $\mathbf{A} = \mathbf{K}_1 \left[\mathbf{K}_1 + \mathbf{\Sigma}_1\right]^{-1}$,
- $\mathbf{X} = Q + Q' + U_2 + U_1$.

We note that we use dirty-paper coding [12] to encode V_1, which leads to the following.

$$I(V_1; \mathbf{Y}_1|U) - I(V_1; V_2|U) = \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} \tag{6.229}$$

The other mutual information terms in the region $\mathcal{R}_{21}$ can be computed straightforwardly, which leads to the achievable rate region $\mathcal{R}_{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ given in Theorem 6.7. Moreover, $\mathcal{R}_{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ can be obtained from $\mathcal{R}_{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ by swapping the subscripts 1 and 2.

Chapter 7

On the Secrecy of Multiple Access Wiretap Channel

7.1 Introduction

The multiple access wiretap channel (MAC-WT), which is introduced in [65, 66], consists of an eavesdropper in addition to the ordinary MAC (see Figure 7.1), where the users would like to send confidential messages to the legitimate receiver in the presence of an external eavesdropper. For this channel, an achievable scheme is proposed in [65], where also the sum secrecy capacity of the degraded Gaussian channel is found. In [66], a general, not necessarily degraded, Gaussian MAC-WT is considered, and achievable sum secrecy rate maximization problems are studied.

In this chapter, we consider a class of MAC-WT where each user's link to the legitimate receiver is stronger than its link to the eavesdropper. We call this class of MAC-WT the *weak eavesdropper* class. We develop an n-letter outer bound for this class, which partially matches the achievable rate region. Even though the matching achievable region and the outer bound give us the capacity, unfortunately, the capacity expressions are in n-letter form, and are not amenable for an efficient computation. Despite this, we show that a loosened version of our outer bound can be evaluated for the weak eavesdropper Gaussian MAC-WT to yield close approximations to the capacity region along the individual rate axes. In particular, we show that the gap between our inner and outer bounds is independent of the chan-

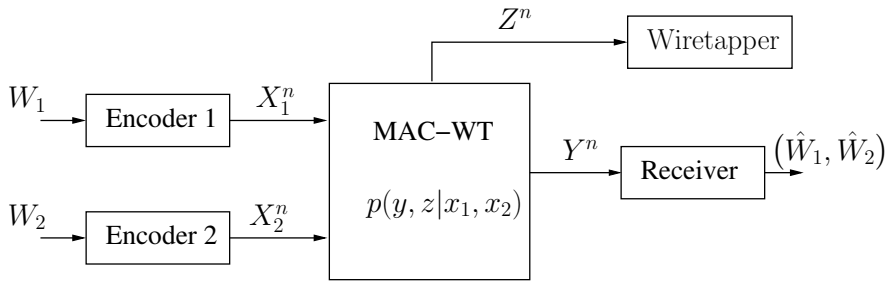

Figure 7.1: The multiple access wiretap channel (MAC-WT).

nel parameters, and is less than 0.5 bits/channel use. Moreover, the entire secrecy capacity region can be obtained to within 0.5 bits/channel use if the users' links to the legitimate user are orthogonal to each other.

In the final part of this chapter, we discuss the implications of our results on the degraded MAC-WT which, by definition, belongs to the weak eavesdropper class studied in this paper. Moreover, we consider the IC-WT which consists of an ordinary IC and an eavesdropper listening to the ongoing communication in the IC. The similarity between the IC-WT with *very strong* interference among the users and the weak eavesdropper Gaussian MAC-WT with orthogonal components is also discussed.

7.2 Channel Model

The MAC-WT (Figure 7.1) consists of two input alphabets, $\mathcal{X}_1, \mathcal{X}_2$, and two output alphabets, $\mathcal{Y}, \mathcal{Z}$. The channel is assumed to be memoryless with conditional distribution $p(y, z|x_1, x_2)$. The inputs can be selected from product distributions on $\mathcal{X}_1 \times \mathcal{X}_2$. A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two independent message sets $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}, \mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, two encoders $f_i : \mathcal{W}_i \to \mathcal{X}_i^n$, $i = 1, 2$, and

a decoder $g : \mathcal{Y}^n \to \mathcal{W}_1 \times \mathcal{W}_2$. The error probability is $P_e^n = \Pr\left(g(Y^n) \neq (W_1, W_2)\right)$. The secrecy of the users is measured by the equivocation rates at the eavesdropper which are $\frac{1}{n}H(W_1|Z^n)$, $\frac{1}{n}H(W_2|Z^n)$ and $\frac{1}{n}H(W_1, W_2|Z^n)$. A rate pair, (R_1, R_2), is said to be achievable with perfect secrecy if there exists a $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code satisfying $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(W_1|Z^n) \geq R_1 \tag{7.1}$$

$$\lim_{n\to\infty} \frac{1}{n} H(W_2|Z^n) \geq R_2 \tag{7.2}$$

$$\lim_{n\to\infty} \frac{1}{n} H(W_1, W_2|Z^n) \geq R_1 + R_2 \tag{7.3}$$

Thus, we only consider *perfect* secrecy in this chapter.

The Gaussian MAC-WT is given by

$$Y = X_1 + X_2 + N_y \tag{7.4}$$

$$Z = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_z \tag{7.5}$$

where N_y and N_z are i.i.d. Gaussian random variables with zero-mean and unit-variance. We have average power constraints on the channel inputs: $E\left[X_j^2\right] \leq P_j,\ j = 1, 2$.

7.3 MAC-WT with Weak Eavesdropper

We define the weak eavesdropper MAC-WT channels as those that satisfy

$$I(X_1; Y|X_2) \geq I(X_1; Z|X_2) \tag{7.6}$$

$$I(X_2; Y|X_1) \geq I(X_2; Z|X_1) \tag{7.7}$$

for all joint input distributions of the form $p(x_1, x_2) = p(x_1)p(x_2)$. This condition can be interpreted as requiring each user to have a *more capable* channel to its legitimate receiver in the absence of the other user.

We first state an achievable region for the *general* MAC-WT in the following theorem.

Theorem 7.1 *The rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} [I(X_1^n; Y^n|X_2^n) - I(X_1^n; Z^n)]^+ \tag{7.8}$$

$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} [I(X_2^n; Y^n|X_1^n) - I(X_2^n; Z^n)]^+ \tag{7.9}$$

$$R_1 + R_2 \leq \lim_{n\to\infty} \frac{1}{n} [I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n)]^+ \tag{7.10}$$

are achievable with perfect secrecy for any distribution of the form $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$.

In Theorem 7.1, $(\cdot)^+$ denotes the positivity operator, i.e., $(x)^+ = \max(0, x)$. This theorem is an extension of the achievable region provided in [65], hence its proof is omitted.

For a MAC-WT channel satisfying (7.6)-(7.7), the rates in (7.8)-(7.9) are always positive [67]. Thus, as long as we consider channels that satisfy (7.6)-(7.7), we do not need the positivity operators in (7.8)-(7.9). However, we note that the conditions in (7.6)-(7.7) do not imply the positivity of the achievable sum secrecy rate in (7.10). Therefore, even in the weak eavesdropper MAC-WT, we do need the positivity operator in (7.10). The following corollary states these observations formally.

Corollary 7.1 *For weak eavesdropper MAC-WT, the rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n; Y^n | X_2^n) - I(X_1^n; Z^n) \right] \tag{7.11}$$

$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_2^n; Y^n | X_1^n) - I(X_2^n; Z^n) \right] \tag{7.12}$$

$$R_1 + R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) \right]^+ \tag{7.13}$$

are achievable with perfect secrecy for any distribution of the form $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$.

Next, we provide our outer bound on the secrecy capacity of the weak eavesdropper MAC-WT.

Theorem 7.2 *The secrecy capacity region of a weak eavesdropper MAC-WT lies in*

the union of the rates satisfying

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n; Y^n | X_2^n) - I(X_1^n; Z^n) \right] \tag{7.14}$$

$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_2^n; Y^n | X_1^n) - I(X_2^n; Z^n) \right] \tag{7.15}$$

$$R_1 + R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n; Y^n | X_2^n) + I(X_2^n; Y^n | X_1^n) - I(X_1^n, X_2^n; Z^n) \right] \tag{7.16}$$

where the union is taken over all $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$.

This theorem is proved in Appendix 7.8.1. The difference between our inner and outer bounds for the weak eavesdropper MAC-WT is in the sum secrecy rate expressions in (7.13) and (7.16). Apart from these, the individual achievable secrecy rate terms in (7.11)-(7.12) and the individual secrecy rate upper bounds in (7.14)-(7.15) match, yielding a partial characterization of the secrecy capacity region in an n-letter form.

7.4 Gaussian MAC-WT with Weak Eavesdropper

Gaussian MAC-WT channels that satisfy the weak eavesdropper conditions in (7.6)-(7.7) have $h_1, h_2 < 1$; see Appendix 7.8.2 for a proof. For the weak eavesdropper Gaussian MAC-WT (as for any weak eavesdropper MAC-WT), the identical inequalities in (7.11)-(7.12) and (7.14)-(7.15) give the secrecy capacity along the individual rate axes. However, the difficulty is, even for Gaussian channels, finding the optimal input distributions $p(x_1^n)$, $p(x_2^n)$ and evaluating the boundary of (7.11)-(7.12) and (7.14)-(7.15) seems to be intractable for now. Consequently, we loosen our outer

bound to obtain computable expressions. We show however that even the loosened outer bound is within 0.5 bits/channel use of the achievable region along the individual rate dimensions. We give our loosened outer bound in the following theorem, which we prove in Appendix 7.8.2.

Theorem 7.3 *The secrecy capacity region of Gaussian MAC-WT with* $h_1, h_2 < 1$ *is contained in the following region.*

$$R_1 \leq \frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_2P_2)}\right) \tag{7.17}$$

$$R_2 \leq \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_1P_1)}\right) \tag{7.18}$$

Next, we compare our outer bound in Theorem 7.3 with our achievable rates in Corollary 7.1. The optimum set of achievable rates that Corollary 7.1 gives is not known. However, we can always obtain potentially sub-optimal achievable rates by using i.i.d. (in time) Gaussian signalling. We note that the ultimate achievable rates thus calculated may yield either a pentagon, a triangle or a trapezoid, as the sum rate expression in (7.13) may dominate the individual rates in (7.11) and (7.12). Since our aim is to investigate how far our outer bound is from the achievable region along the individual rate axes, we will choose our parameters to guarantee that we do not have a triangle as an achievable region. Thus, let us assume that h_1, h_2, P_1, P_2

are such that at least one of the inequalities

$$h_1 \leq \frac{1}{1+P_2}, \quad h_2 \leq \frac{1}{1+P_1} \tag{7.19}$$

is satisfied so that we have either a trapezoid or a pentagon as an achievable region; see Figure 7.2. Then, we have the following achievable rates expressed in four different possible cases.

Corollary 7.2 *Without loss of generality, we assume $h_1 < h_2 < 1$. The following secrecy regions are achievable.*

- *Case I:* $h_1 \leq \frac{1}{1+P_2}$, $h_2 \leq \frac{1}{1+P_1}$

$$R_1 \leq \frac{1}{2}\log(1+P_1) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right) \tag{7.20}$$

$$R_2 \leq \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \tag{7.21}$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \tag{7.22}$$

- *Case II:* $h_1 \leq \frac{1}{1+P_2}$, $\frac{1}{1+P_1} \leq h_2 \leq \frac{1+h_1P_1}{1+P_1}$

$$R_2 \leq \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \tag{7.23}$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \tag{7.24}$$

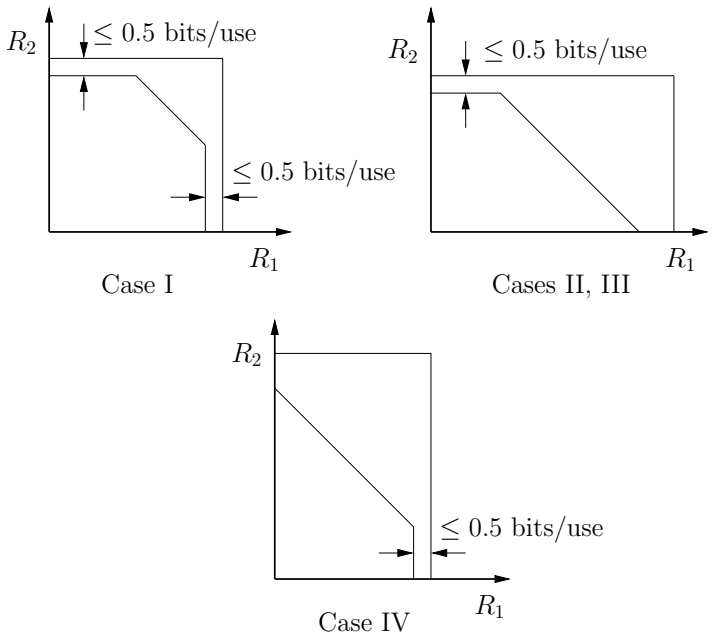

Figure 7.2: Illustration of outer and inner bounds for different h_1, h_2 values.

- *Case III:* $h_1 \leq \frac{1}{1+P_2}$, $\frac{1+h_1P_1}{1+P_1} \leq h_2$

$$R_2 \leq \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \tag{7.25}$$

$$R_1 + R_2 \leq \frac{1}{2}\log(1+P_1) - \frac{1}{2}\log(1+h_1P_1) \tag{7.26}$$

- *Case IV:* $\frac{1}{1+P_2} \leq h_1$, $h_2 \leq \frac{1}{1+P_1}$

$$R_1 \leq \frac{1}{2}\log(1+P_1) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right) \tag{7.27}$$

$$R_1 + R_2 \leq \frac{1}{2}\log(1+P_1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \tag{7.28}$$

The achievable regions in Corollary 7.2 are obtained by using i.i.d. (in time) Gaussian signalling in Corollary 7.1. We now check the gap between our inner and outer bounds on the individual rates. Here, as an example, we evaluate the difference between the achievable rate and the outer bound for user 1, i.e., the difference of (7.20) and (7.27) with (7.17); such difference for the rate of user 2 can be calculated similarly. For user 1, this difference is:

$$\frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right)-\frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_2P_2)}\right)=\frac{1}{2}\log\left(\frac{2(1+h_1P_1+h_2P_2)}{2+h_1P_1+h_2P_2}\right) \tag{7.29}$$

which is always less than 0.5 bits/channel use. Thus, if the first (resp. second) inequality in (7.19) is satisfied, then the secrecy rate achievable for the second (resp. first) user via i.i.d. Gaussian signalling and without pre-processing is within half bit of the maximum possible secrecy rate for that user. A graphical illustration of our inner and outer bounds is given in Figure 7.2.

7.5 A Special Class: Orthogonal Components

We now consider a special sub-class of weak eavesdropper Gaussian MAC-WT class where each user has an orthogonal link to the legitimate receiver while the links

from the users to the eavesdropper form a general Gaussian MAC:

$$Y_1 = X_1 + N_{y1} \tag{7.30}$$

$$Y_2 = X_2 + N_{y2} \tag{7.31}$$

$$Z = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_z \tag{7.32}$$

where N_{y1}, N_{y2} and N_z are i.i.d. zero-mean unit-variance Gaussian random variables. Here again we have $h_1, h_2 < 1$. We have the following achievable region.

Corollary 7.3 *The following region is achievable for the orthogonal-component weak eavesdropper Gaussian MAC-WT*

$$R_1 \leq \frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(1+\frac{h_1P_1}{1+h_2P_2}\right) \tag{7.33}$$

$$R_2 \leq \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(1+\frac{h_2P_2}{1+h_1P_1}\right) \tag{7.34}$$

$$R_1 + R_2 \leq \frac{1}{2}\log\left(1+P_1\right) + \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(1+h_1P_1+h_2P_2\right) \tag{7.35}$$

This achievable region is obtained by using i.i.d. (in time) Gaussian signalling in Corollary 7.1. We have the following outer bound on the secrecy capacity region of this channel.

Theorem 7.4 *The secrecy capacity region of the orthogonal-component weak eaves-*

dropper Gaussian MAC-WT is contained in the following region.

$$R_1 \leq \frac{1}{2}\log\left(1+P_1\right) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_2P_2)}\right) \tag{7.36}$$

$$R_2 \leq \frac{1}{2}\log\left(1+P_2\right) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2(1+h_1P_1)}\right) \tag{7.37}$$

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1) + \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log\left(\frac{2+h_1P_1+h_2P_2}{2}\right) \tag{7.38}$$

This theorem is proved in Appendix 7.8.3. Thus, for this special class of channels, using a calculation similar to that in (7.29), we can show that the difference between the sum secrecy rate expressions on the right hand sides of (7.35) and (7.38) is less than 0.5 bits/channel use. The situation in this special weak eavesdropper Gaussian MAC-WT is illustrated in Figure 7.3.

Moreover, if we restrict the channel gains to $h_1+h_2<1$, then we can determine the sum secrecy capacity of this channel as stated in the next theorem, which we prove in Appendix 7.8.4.

Theorem 7.5 *If $h_1+h_2<1$, then the sum secrecy capacity of this channel is given by*

$$R_1+R_2 \leq \frac{1}{2}\log(1+P_1) + \frac{1}{2}\log(1+P_2) - \frac{1}{2}\log(1+h_1P_1+h_2P_2) \tag{7.39}$$

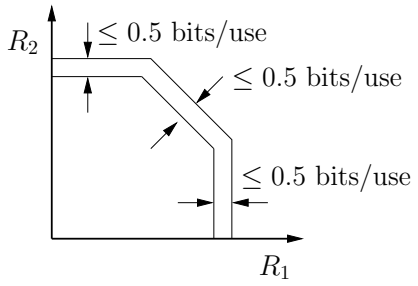

Figure 7.3: Illustration of outer and inner bounds for MAC-WT with orthogonal components.

7.6 Further Remarks

We now discuss the implications of our results on the secrecy capacity of the degraded MAC-WT. Degraded MAC-WT satisfies the Markov chain

$$(X_1, X_2) \rightarrow Y \rightarrow Z \tag{7.40}$$

and consequently, satisfies the conditions given in (7.6)-(7.7). Thus, our outer bound in Theorem 7.2 holds for these channels as well. Indeed, our Theorem 7.2 can be improved to give the entire capacity region in an n-letter form as given in the following theorem.

Theorem 7.6 *The secrecy capacity region of a degraded MAC-WT is given by the union of the following rates*

$$R_1 \leq \lim_{n\rightarrow\infty} \frac{1}{n} \left[I(X_1^n; Y^n | X_2^n) - I(X_1^n; Z^n) \right] \tag{7.41}$$

$$R_2 \leq \lim_{n\rightarrow\infty} \frac{1}{n} \left[I(X_2^n; Y^n | X_1^n) - I(X_2^n; Z^n) \right] \tag{7.42}$$

$$R_1 + R_2 \leq \lim_{n\rightarrow\infty} \frac{1}{n} \left[I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) \right] \tag{7.43}$$

where the union is taken over all $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$.

The proof of Theorem 7.6 is given in Appendix 7.8.5. We further remark that the sum secrecy capacity of the degraded MAC-WT can be put into a single-letter form as $I(X_1, X_2; Y|Z)$.

As a result of Theorem 7.6, we establish the secrecy capacity region of the degraded MAC-WT in n-letter form. Prior to our result here, only the sum secrecy capacity of the degraded Gaussian MAC-WT was known due to [65], where the degraded Gaussian MAC-WT is defined by (7.4)-(7.5) with $h_1 = h_2 = h < 1$. Hence, using our outer bound in Theorem 7.3, and with the sum rate capacity result of [65], we have the following corollary for the degraded Gaussian MAC-WT.

Corollary 7.4 *The achievable region described by (7.20)-(7.22) coincides with the sum secrecy rate points of the degraded Gaussian MAC-WT. Moreover, this region is within half bit of the straight lines of the pentagon corresponding to the capacity region if* $h \leq \min\left(1/(1+P_1), 1/(1+P_2)\right)$.

In Corollary 7.4, the claim regarding the sum secrecy capacity is due to [65]. The other claim can be proved by simply setting $h_1 = h_2 = h$ in Theorem 7.3 and in Corollary 7.2, and checking the gap between these rates as it is done in (7.29).

A further remark is about IC-WT when the interference among the users is *very strong*. We now show that the results obtained for the Gaussian MAC-WT with orthogonal components in Section 7.5 hold for IC-WT with very strong interference

as well. The Gaussian IC-WT is defined by

$$Y_1 = X_1 + \sqrt{\alpha} X_2 + N_{y1} \tag{7.44}$$

$$Y_2 = X_2 + \sqrt{\beta} X_1 + N_{y2} \tag{7.45}$$

$$Z = \sqrt{h_1} X_1 + \sqrt{h_2} X_2 + N_z \tag{7.46}$$

where Y_1, Y_2 and Z denote the users' and the eavesdropper's observation, respectively. We have power constraints on the channel inputs as $E\left[X_j^2\right] \leq P_j,\ j = 1, 2$ and the channel inputs should be independent. All of the definitions in Section 7.2 regarding the codes and the achievability hold for IC-WT with appropriate modifications. Since there are now two receivers, we have two decoders, each one associated with one receiver. Consequently, each decoder has its own probability of error that needs to decay to zero. Similar to MAC-WT, each transmitter uses a codebook that is independent of the other user's codebook and the secrecy is measured through $\frac{1}{n} H(W_1|Z^n), \frac{1}{n} H(W_2|Z^n), \frac{1}{n} H(W_1, W_2|Z^n)$.

If α and β satisfy

$$\alpha \geq 1 + P_1, \quad \beta \geq 1 + P_2 \tag{7.47}$$

interference at each terminal becomes *very strong* which can be eliminated entirely leaving each user a clean, single-user channel [68]. Consequently, the resulting channel becomes equivalent to the channel in (7.30)-(7.32). Thus, in light of the results obtained in Section 7.5, we find the secrecy capacity region of this channel to within

half bit. This is stated in the next theorem which is proved in Appendix 7.8.6.

Theorem 7.7 *The achievable secrecy region given in Corollary 7.3 is within half bit of the secrecy capacity region of the IC-WT if α and β satisfy (7.47) and $h_1, h_2 < 1$. Moreover, if $h_1 + h_2 < 1$, then the sum secrecy capacity is given by (7.39).*

7.7 Conclusions

In this chapter, we focus on a special class of MAC-WT which we call the weak eavesdropper MAC-WT for which we provide an n-letter outer bound. Evaluation of this outer bound for the weak eavesdropper Gaussian MAC-WT provides us with close approximations of the secrecy capacity region. In particular, the results of this chapter imply that plain i.i.d. Gaussian signaling is close to optimal in the low power regime for the weak eavesdropper Gaussian MAC-WT.

However, in general, it has been shown that plain i.i.d. Gaussian signaling is not optimal for Gaussian MAC-WT channel. In particular, for the Gaussian MAC-WT, [69, 70] use structured coding (by means of lattice codes [69] and interference alignment [70]) instead of plain i.i.d. Gaussian signalling, and show that secrecy rates attainable by structured coding scale with the available power, i.e., they attain non-zero secure degrees of freedom, while plain i.i.d. Gaussian signalling cannot provide any non-zero secure degrees of freedom [65, 66, 71].

7.8 Appendix

7.8.1 Proof of Theorem 7.2

First, we note that for channels satisfying (7.6)-(7.7), we also have

$$I(X_1^n; Y^n | X_2^n, U) \geq I(X_1^n; Z^n | X_2^n, U) \tag{7.48}$$

$$I(X_2^n; Y^n | X_1^n, U) \geq I(X_2^n; Z^n | X_1^n, U) \tag{7.49}$$

for all $p(x_1^n, x_2^n) = p(x_1^n)p(x_2^n)$ and any random variable U such that $U \to (X_1^n, X_2^n) \to (Y^n, Z^n)$, $X_1^n \to U \to X_2^n$ [67]. Thus, using this result, we can obtain

$$I(X_1^n; Y^n | X_2^n, W_1) \geq I(X_1^n; Z^n | X_2^n, W_1) \tag{7.50}$$

$$\geq I(X_1^n; Z^n | W_1) \tag{7.51}$$

where in the second inequality, we use the fact that (X_1^n, W_1) and X_2^n are independent, and that conditioning decreases entropy. Similarly, we have

$$I(X_2^n; Y^n | X_1^n, W_2) \geq I(X_2^n; Z^n | X_1^n, W_2) \tag{7.52}$$

$$\geq I(X_2^n; Z^n | W_2) \tag{7.53}$$

Furthermore, starting with (7.48), we get

$$I(X_1^n; Y^n | X_2^n, W_1) \geq I(X_1^n; Z^n | X_2^n, W_1) \tag{7.54}$$

$$= I(X_1^n; Z^n | X_2^n, W_1, W_2) \tag{7.55}$$

$$\geq I(X_1^n; Z^n | W_1, W_2) \tag{7.56}$$

where the equality is due to the fact that given X_2^n, W_2 is independent of everything else and the last inequality follows from the fact that (X_1^n, W_1) and (X_2^n, W_2) are independent and that conditioning decreases entropy. If we combine (7.56) with

$$I(X_2^n; Y^n | X_1^n, W_2) \geq I(X_2^n; Z^n | X_1^n, W_2, W_1) \tag{7.57}$$

which follows from (7.55) due to symmetry, we get

$$I(X_1^n; Y^n | X_2^n, W_1) + I(X_2^n; Y^n | X_1^n, W_2) \geq I(X_1^n, X_2^n; Z^n | W_1, W_2) \tag{7.58}$$

which will be used in the derivation of our outer bound on the sum secrecy rate. Hence, we have all the necessary inequalities, i.e., (7.51), (7.53), (7.58), for the remaining part of the proof.

We start with the derivation of our outer bound on R_1,

$$nR_1 \leq H(W_1|Z^n) \leq I(W_1;Y^n) - I(W_1;Z^n) + \epsilon_n \tag{7.59}$$

$$\leq I(W_1;Y^n|X_2^n) - I(W_1;Z^n) + \epsilon_n \tag{7.60}$$

$$\leq I(W_1;Y^n|X_2^n) - I(W_1;Z^n) + I(X_1^n;Y^n|X_2^n,W_1)$$

$$- I(X_1;Z^n|W_1) + \epsilon_n \tag{7.61}$$

$$= I(W_1,X_1^n;Y^n|X_2^n) - I(W_1,X_1^n;Z^n) + \epsilon_n \tag{7.62}$$

$$= I(X_1^n;Y^n|X_2^n) - I(X_1^n;Z^n) + \epsilon_n \tag{7.63}$$

where (7.59) is due to Fano's lemma [22], (7.60) is due to the fact that W_1 and X_2^n are independent and that conditioning decreases entropy, (7.61) is obtained by using (7.51), and (7.63) follows from the fact that given X_1^n, W_1 is independent of everything else. This gives us (7.14). Similarly, one can get (7.15).

We next prove our outer bound on the sum secrecy rate.

$$n(R_1+R_2) \leq H(W_1,W_2|Z^n) \tag{7.64}$$

$$\leq I(W_1,W_2;Y^n) - I(W_1,W_2;Z^n) + \epsilon_n \tag{7.65}$$

$$\leq I(W_1;Y^n|X_2^n) + I(W_2;Y^n|X_1^n) - I(W_1,W_2;Z^n) + \epsilon_n \tag{7.66}$$

$$\leq I(W_1;Y^n|X_2^n) + I(W_2;Y^n|X_1^n) - I(W_1,W_2;Z^n) + I(X_1^n;Y^n|X_2^n,W_1)$$

$$+ I(X_2^n;Y^n|X_1^n,W_2) - I(X_1^n,X_2^n;Z^n|W_1,W_2) + \epsilon_n \tag{7.67}$$

$$= I(X_1^n;Y^n|X_2^n) + I(X_2^n;Y^n|X_1^n) - I(X_1^n,X_2^n;Z^n) + \epsilon_n \tag{7.68}$$

where (7.65) is due to Fano's lemma [22], (7.66) follows from the fact that W_1 (resp. W_2) and X_2^n (resp. X_1^n) are independent and that conditioning decreases entropy, (7.67) follows by using (7.58) and (7.68) comes from the fact that given X_1^n (resp. X_2^n)), W_1 (resp. W_2) is independent of everything else. This gives us (7.16).

7.8.2 Proof of Theorem 7.3

First, we show that Gaussian MAC-WT with $h_1, h_2 < 1$ satisfies (7.6)-(7.7), hence Theorem 7.2 is applicable. To this end, define the following random variables

$$\tilde{Y}_1 = Y - X_2 = X_1 + N_y \tag{7.69}$$

$$\tilde{Z}_1 = \sqrt{h_1}(X_1 + N_y) + \sqrt{1 - h_1}\tilde{N} \tag{7.70}$$

where $\tilde{N} \sim \mathcal{N}(0, 1)$ and is independent of everything else. Note that $\tilde{Y}_1$ and $\tilde{Z}_1$ satisfy

$$I(X_1; Y|X_2) = I(X_1; \tilde{Y}_1) = I(X_1; \tilde{Y}_1, \tilde{Z}_1) \tag{7.71}$$

$$I(X_1; Z|X_2) = I(X_1; \tilde{Z}_1) \tag{7.72}$$

where the second equality of (7.71) is due to the Markov chain $X_1 \to \tilde{Y}_1 \to \tilde{Z}_1$. Thus, we have

$$I(X_1;Y|X_2) - I(X_1;Z|X_2) = I(X_1;\tilde{Y}_1,\tilde{Z}_1) - I(X_1;\tilde{Z}_1) \tag{7.73}$$

$$= I(X_1;\tilde{Y}_1|\tilde{Z}_1) \tag{7.74}$$

$$\geq 0 \tag{7.75}$$

proving that Gaussian MAC-WT with $h_1, h_2 < 1$ satisfies (7.6)-(7.7).

We now bound the following term

$$I(X_1^n;Y^n|X_2^n) - I(X_1^n;Z^n) = H(X_1^n + N_y^n) + H(\sqrt{h_2}X_2^n + N_z^n) \\ - H(\sqrt{h_1}X_1^n + \sqrt{h_2}X_2^n + N_z^n) - H(N_y^n) \tag{7.76}$$

where we use $H(\cdot)$ to denote the differential entropy of a continuous random variable. We will use a variant of the entropy-power inequality given in [72]. Let $\{U_i^n\}_{i=1}^N$ be independent length-n random vectors. If $\mathcal{C}$ denotes an arbitrary collection of subsets of $\{1,\ldots,N\}$, then we have

$$\exp\left(\frac{2}{n}H\left(\sum_{i=1}^N U_i^n\right)\right) \geq \frac{1}{r}\sum_{\mathbf{S}\in\mathcal{C}} \exp\left(\frac{2}{n}H\Big(\sum_{i\in\mathbf{S}} U_i^n\Big)\right) \tag{7.77}$$

where r denotes the maximum number of subsets in $\mathcal{C}$ in which any one index, i, appears, and $\mathbf{S}$ denotes a subset of $\{1,\ldots,n\}$ that is in the collection $\mathcal{C}$.

Before using this inequality, first decompose N_z^n as follows

$$N_z^n = \sqrt{h_1} N_y^n + \sqrt{1-h_1}\tilde{N}^n \tag{7.78}$$

where $\tilde{N}^n \sim \mathcal{N}(0, \mathbf{I})$ and is independent of everything else. Furthermore, let us define

$$t_1 = H(X_1^n + N_y^n) \tag{7.79}$$

$$= H(\sqrt{h_1} X_1^n + \sqrt{h_1} N_y^n) - \frac{n}{2}\log(h_1) \tag{7.80}$$

and

$$t_2 = H(\sqrt{h}_2 X_2 + N_z^n) \tag{7.81}$$

$$= H(\sqrt{h_2} X_2^n + \sqrt{h_1} N_y^n + \sqrt{1-h_1}\tilde{N}^n) \tag{7.82}$$

Using the inequality in (7.77), we have the following lower bound

$$H(\sqrt{h_1} X_1^n + \sqrt{h_2} X_2^n + N_z^n) \geq \frac{n}{2}\log\left(\frac{h_1}{2}\exp\left(\frac{2t_1}{n}\right) + \frac{1}{2}\exp\left(\frac{2t_2}{n}\right) + 2\pi e \frac{1-h_1}{2}\right) \tag{7.83}$$

Using (7.76) and (7.83), we obtain the following upper bound

$$I(X_1^n; Y^n | X_2^n) - I(X_1^n; Z^n) \leq \max_{t_1, t_2} f(t_1, t_2) \tag{7.84}$$

where $f(t_1, t_2)$ is

$$f(t_1, t_2) = t_1 + t_2 - \frac{n}{2} \log \left(\frac{h_1}{2} \exp \left(\frac{2t_1}{n} \right) + \frac{1}{2} \exp \left(\frac{2t_2}{n} \right) + 2\pi e \frac{1 - h_1}{2} \right) - \frac{n}{2} \log(2\pi e) \tag{7.85}$$

Note that $f(t_1, t_2)$ is monotonically increasing in both t_1 and t_2. Since t_1 and t_2 are maximized when $X_1^n \sim \mathcal{N}(0, P_1\mathbf{I})$ and $X_2^n \sim \mathcal{N}(0, P_2\mathbf{I})$, the maximum value of $f(t_1, t_2)$ is

$$\frac{1}{2} \log (1 + P_1) - \frac{1}{2} \log \left(\frac{2 + h_1 P_1 + h_2 P_2}{2(1 + h_2 P_2)} \right) \tag{7.86}$$

This completes the proof of the upper bound on R_1 given in (7.17). The upper bound on R_2 given in (7.18) follows from symmetry.

7.8.3 Proof of Theorem 7.4

We define $Y^n = (Y_1^n, Y_2^n)$. Using the facts that X_1^n (resp. X_2^n) and Y_2^n (resp. X_1^n) are independent, we get

$$I(X_1^n; Y^n | X_2^n) = I(X_1^n; Y_1^n) \tag{7.87}$$

$$I(X_2^n; Y^n | X_1^n) = I(X_2^n; Y_2^n) \tag{7.88}$$

$$I(X_1^n, X_2^n; Y^n) = I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) \tag{7.89}$$

Moreover, following the analysis carried out in the proof of Theorem 7.3 in Appendix 7.8.2, we can show that this channel satisfies (7.6)-(7.7). Thus, our outer bound in Theorem 7.2 can be applied to this channel as well. Hence, plugging the expressions in (7.87)-(7.89) into Corollary 7.1 and Theorem 7.2, we get the secrecy capacity region of this channel as follows.

$$R_1 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_1^n; Y_1^n) - I(X_1^n; Z^n) \right] \tag{7.90}$$

$$R_2 \leq \lim_{n\to\infty} \frac{1}{n} \left[I(X_2^n; Y_2^n) - I(X_2^n; Z^n) \right] \tag{7.91}$$

$$R_1 + R_2 \leq \lim_{n\to\infty} \frac{1}{n} \big[I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) - I(X_1^n, X_2^n; Z^n) \big] \tag{7.92}$$

As opposed to the general weak eavesdropper MAC-WT class, for this subclass, we are able to obtain the entire secrecy capacity region in an n-letter form, because the expression in (7.13) is guaranteed to be positive, and the expressions in (7.13) and (7.16) become identical, due to (7.87)-(7.89). The two bounds on the individual secrecy rate terms are identical to those in the proof of Theorem 7.3 given in Appendix 7.8.2, and hence the bounds in Theorem 7.3 directly apply for this channel as well. Hence, we only need to consider the sum secrecy rate term which is

$$\begin{aligned} &I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) - I(X_1^n, X_2^n; Z^n) \\ &= H(X_1^n + N_{y1}^n) + H(X_2^n + N_{y2}^n) - H(\sqrt{h_1} X_1^n + \sqrt{h_2} X_2^n + N_z^n) - \frac{n}{2} \log(2\pi e) \end{aligned} \tag{7.93}$$

We decompose the noise of the eavesdropper as

$$N_z^n = \sqrt{h_1}\tilde{N}_1^n + \sqrt{h_2 - h_1}\tilde{N}_2^n + \sqrt{1 - h_2}\tilde{N}_3^n \tag{7.94}$$

where $\tilde{N}_1^n, \tilde{N}_2^n, \tilde{N}_3^n$ are independent Gaussian random vectors with zero-mean and identity covariance matrices. We also define

$$t_1 = H(X_1^n + N_{y1}^n) \tag{7.95}$$

$$= H(\sqrt{h_1}X_1^n + \sqrt{h_1}\tilde{N}_1^n) - \frac{n}{2}\log h_1 \tag{7.96}$$

and

$$t_2 = H(X_2^n + N_{y2}^n) \tag{7.97}$$

$$= H(\sqrt{h_2}X_2^n + \sqrt{h_2 - h_1}\tilde{N}_2^n + \sqrt{h_1}\tilde{N}_1^n) - \frac{n}{2}\log h_2 \tag{7.98}$$

Using the entropy power inequality of [72] given in (7.77), we get

$$\frac{2}{n}H(\sqrt{h_1}X_1^n + \sqrt{h_2}X_2^n + N_z^n) \geq g(t_1, t_2) \tag{7.99}$$

where $g(t_1, t_2)$ is

$$\log\left(\frac{h_1}{2}\exp\left(\frac{2t_1}{n}\right) + \frac{h_2}{2}\exp\left(\frac{2t_2}{n}\right) + 2\pi e\frac{2 - h_2 - h_1}{2}\right) \tag{7.100}$$

Thus, the sum secrecy rate can be upper bounded as

$$I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) - I(X_1^n, X_2^n; Z^n) \leq \max_{t_1,t_2} f(t_1, t_2) \tag{7.101}$$

where $f(t_1, t_2)$ is

$$\frac{2}{n} f(t_1, t_2) = \frac{2}{n}(t_1 + t_2) + \log(2\pi e) - g(t_1, t_2) \tag{7.102}$$

which is monotonically increasing in both t_1 and t_2. Since t_1 and t_2 are maximized when $X_1^n \sim \mathcal{N}(0, P_1\mathbf{I})$ and $X_2^n \sim \mathcal{N}(0, P_2\mathbf{I})$, the maximum value of $f(t_1, t_2)$ is

$$\frac{1}{2}\log(1 + P_1) + \frac{1}{2}\log(1 + P_2) - \frac{1}{2}\log\left(\frac{2 + h_1P_1 + h_2P_2}{2}\right) \tag{7.103}$$

This completes the proof of the upper bound on the sum secrecy rate given in (7.38).

7.8.4 Proof of Theorem 7.5

The proof of Theorem 7.5 is similar to the proof of the sum rate secrecy bound in Theorem 7.4. The differences are in the way we decompose the eavesdropper noise and apply the entropy power inequality. Here, the classical entropy power inequality [41, 43] is sufficient to get the result, i.e, we do not make use of the additional properties of the one in (7.77) [72]. Instead of decomposing the noise as

in (7.94), we will use

$$N_z^n = \sqrt{h_1} N_{y1}^n + \sqrt{h_2} N_{y2}^n + \tilde{N}^n \tag{7.104}$$

where $\tilde{N}^n$ is i.i.d. Gaussian noise sequence with zero-mean and variance of $1-h_1-h_2$. Consequently, using entropy power inequality, we get

$$\frac{2}{n} I(X_1^n, X_2^n; Z^n) = \frac{2}{n} H(\sqrt{h_1} X_1^n + \sqrt{h_2} X_2^n + N_z^n) - \log(2\pi e) \tag{7.105}$$

$$\geq g(t_1, t_2) \tag{7.106}$$

where $g(t_1, t_2)$ is

$$\log\left(\frac{h_1}{2\pi e} \exp\left(\frac{2t_1}{n}\right) + \frac{h_2}{2\pi e} \exp\left(\frac{2t_2}{n}\right) + 1 - h_1 - h_2\right) \tag{7.107}$$

and t_1, t_2 are

$$t_1 = H\left(X_1^n + N_{y1}^n\right) \tag{7.108}$$

$$t_2 = H\left(X_2^n + N_{y2}^n\right) \tag{7.109}$$

Therefore, the sum secrecy rate can be upper bounded as

$$I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) - I(X_1^n, X_2^n; Z^n) \leq \max_{t_1, t_2} f(t_1, t_2) \tag{7.110}$$

where $f(t_1, t_2)$ is

$$\frac{2}{n} f(t_1, t_2) = \frac{2}{n}(t_1 + t_2) - 2\log(2\pi e) - g(t_1, t_2) \tag{7.111}$$

which is monotonically increasing in both t_1 and t_2. Since t_1 and t_2 are maximized when X_1^n, X_2^n are selected as Gaussian with zero-mean and covariance matrices of $P_1\mathbf{I}, P_2\mathbf{I}$, we get

$$\begin{aligned} I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) - I(X_1^n, X_2^n; Z^n) \leq \frac{n}{2}\log(1 + P_1) + \frac{n}{2}\log(1 + P_2) \\ - \frac{n}{2}\log(1 + h_1 P_1 + h_2 P_2) \end{aligned} \tag{7.112}$$

which completes the proof.

7.8.5 Proof of Theorem 7.6

Since degraded channels already satisfy the conditions in (7.6)-(7.7), the outer bound in Theorem 7.2 is valid for them. Thus, to prove Theorem 7.6, we only need to consider the sum secrecy rate. First, note that for degraded channels

$$\begin{aligned} & I(X_1^n, X_2^n; Y^n | W_1, W_2) - I(X_1^n, X_2^n; Z^n | W_1, W_2) \\ & \quad = I(X_1^n, X_2^n; Y^n, Z^n | W_1, W_2) - I(X_1^n, X_2^n; Z^n | W_1, W_2) && (7.113) \\ & \quad = I(X_1^n, X_2^n; Y^n | W_1, W_2, Z^n) && (7.114) \\ & \quad \geq 0 && (7.115) \end{aligned}$$

where the first equality is due to the degradedness. We now bound sum secrecy rate of the degraded channels.

$$H(W_1, W_2|Z^n) \leq I(W_1, W_2; Y^n) - I(W_1, W_2; Z^n) + \epsilon_n \tag{7.116}$$

$$\leq I(W_1, W_2; Y^n) - I(W_1, W_2; Z^n) + \epsilon_n$$

$$+ I(X_1^n, X_2^n; Y^n|W_1, W_2) - I(X_1^n, X_2^n; Z^n|W_1, W_2) \tag{7.117}$$

$$= I(X_1^n, X_2^n; Y^n) - I(X_1^n, X_2^n; Z^n) + \epsilon_n \tag{7.118}$$

where (7.116) is due to Fano's lemma [22], (7.117) is obtained by using (7.115), and (7.118) is a consequence of the fact that given (X_1^n, X_2^n), (W_1, W_2) is independent of the channel outputs.

7.8.6 Proof of Theorem 7.7

We prove Theorem 7.7 in two parts, starting with achievability. User i $(i = 1, 2)$ generates $2^{n(R_i+\tilde{R}_i)}$ length-n codewords $\mathbf{X}_i$ through $\mathcal{N}(0, P_i\mathbf{I})$ and labels them $\mathbf{X}_i(w_i, \tilde{w}_i)$ where $w_i \in \{1, \ldots, 2^{nR_i}\}$, $\tilde{w}_i \in \{1, \ldots, 2^{n\tilde{R}_i}\}$. Here, R_i denotes the rate of the information-carrying messages and $\tilde{R}_i$ is the rate sacrificed to confuse the eavesdropper to achieve secrecy for user $i = 1, 2$. For example, if w_i is the message to be transmitted, user i selects a $\tilde{W}_i$ randomly and transmits $\mathbf{x}_i(w_i, \tilde{w}_i)$. Furthermore,

these rates satisfy

$$R_i + \tilde{R}_i \leq \frac{1}{2}\log(1+P_i), \qquad i = 1,2 \tag{7.119}$$

$$\tilde{R}_i \leq \frac{1}{2}\log(1+h_i P_i), \qquad i = 1,2 \tag{7.120}$$

$$\tilde{R}_1 + \tilde{R}_2 = \frac{1}{2}\log(1+h_1 P_1 + h_2 P_2) \tag{7.121}$$

Since interference gains, α, β, satisfy (7.47), each user can decode both other user's messages and its own message with vanishingly small probability of error [68]. Hence, we only need to show that this scheme yields perfect secrecy. To this end, we consider joint secrecy condition which is sufficient to ensure that secrecy constraints on the individual messages are satisfied [65]. We have,

$$H(W_1, W_2|Z^n) = H(W_1, W_2, Z^n) - H(Z^n) \tag{7.122}$$

$$= H(W_1, W_2, X_1^n, X_2^n, Z^n) - H(X_1^n, X_2^n|W_1, W_2, Z^n)$$

$$- H(Z^n) \tag{7.123}$$

$$= H(W_1, W_2) + H(X_1^n, X_2^n|W_1, W_2) + H(Z^n|X_1^n, X_2^n)$$

$$- H(X_1^n, X_2^n|W_1, W_2, Z^n) - H(Z^n) \tag{7.124}$$

$$= H(W_1, W_2) + H(X_1^n, X_2^n|W_1, W_2) - I(X_1^n, X_2^n; Z^n)$$

$$- H(X_1^n, X_2^n|W_1, W_2, Z^n) \tag{7.125}$$

where (7.124) is obtained by using the chain rule and the fact that given (X_1^n, X_2^n), (W_1, W_2) and Z^n are independent. We now consider each term of (7.125) separately.

Since given (W_1, W_2), (X_1^n, X_2^n) can take $2^{n(\tilde{R}_1+\tilde{R}_2)}$ different values uniformly, we have

$$H(X_1^n, X_2^n|W_1, W_2) = n(\tilde{R}_1 + \tilde{R}_2) \tag{7.126}$$

$$= \frac{n}{2}\log(1 + h_1P_1 + h_2P_2) \tag{7.127}$$

The third term of (7.125) is bounded as

$$I(X_1^n, X_2^n; Z^n) \leq \frac{n}{2}\log(1 + h_1P_1 + h_2P_2) \tag{7.128}$$

due to the fact that i.i.d. Gaussian signalling achieves the capacity of a memoryless Gaussian channel. Finally, we bound the last term of (7.125). To this end, assume that eavesdropper is decoding (X_1^n, X_2^n) given (W_1, W_2). Since $\tilde{R}_1$ and $\tilde{R}_2$ are selected to lie in the capacity region of the MAC between the users and the eavesdropper, the error probability of this decoding is vanishingly small, implying

$$H(X_1^n, X_2^n|W_1, W_2, Z^n) \leq \epsilon_n \tag{7.129}$$

due to Fano's lemma. Plugging (7.127), (7.128), (7.129) into (7.125), we get

$$H(W_1, W_2|Z^n) \geq H(W_1, W_2) - \epsilon_n \tag{7.130}$$

Thus, this scheme yields perfect secrecy. After eliminating $\tilde{R}_1$ and $\tilde{R}_2$ from (7.119), (7.120) and (7.121), one can get the achievable region of Corollary 7.3. Hence, we complete the achievability part.

For the outer bound, we note that this channel satisfies the conditions in (7.6)-(7.7) and consequently, following similar lines as in the proof of Theorem 7.4, one can get the outer bound given in this theorem. Moreover, we can show the sum secrecy capacity for the case $h_1 + h_2 < 1$ by using the proof technique developed for Theorem 7.5 in Appendix 7.8.4.

Chapter 8

Cooperative Secrecy in Relay Broadcast Channels

8.1 Introduction

In this chapter, we study the effects of cooperation on the secrecy of *multiple users* where secrecy refers to simultaneous individual confidentiality of all users against each other. For that purpose, we consider the cooperative relay broadcast channel (CRBC), where there is a single transmitter and two receivers, and each receiver wants to keep its message secret from the other user; see Figures 8.1 and 8.2. In this model, in order to incorporate the effects of cooperation, there is either a single-sided (Figure 8.1) or double-sided (Figure 8.2) cooperative link between the users. We note that the CRBC is the simplest model (except perhaps for the "dual" model of cooperating transmitters in a MAC with per-user secrecy constraints that will be considered in the next chapter) that allows us to study the effects of user cooperation on secrecy.

Although, in the literature, there have been some work focusing on the effects of cooperation on secrecy [73–79], none of these works consider the effects of cooperation on the simultaneous secrecy of multiple users. In particular, [73–79] consider secrecy in relay channels, where in [73–76], the relay is the eavesdropper, while in [77, 78] there is an external eavesdropper. In [79], the relay helps the transmitter to improve its rate while it receives confidential messages that should be kept hidden

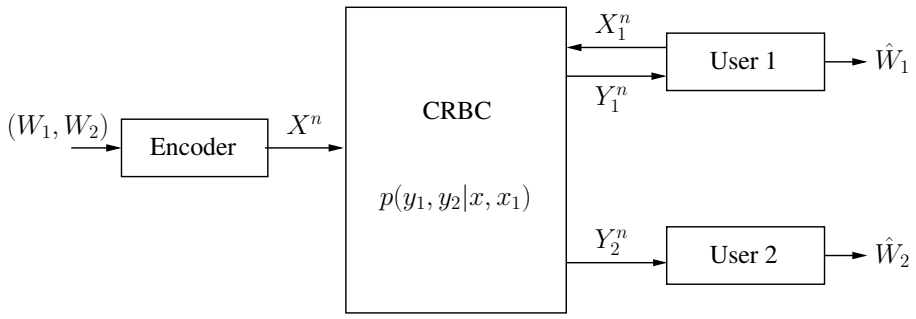

Figure 8.1: Cooperative relay broadcast channel (CRBC) with single-sided cooperation link.

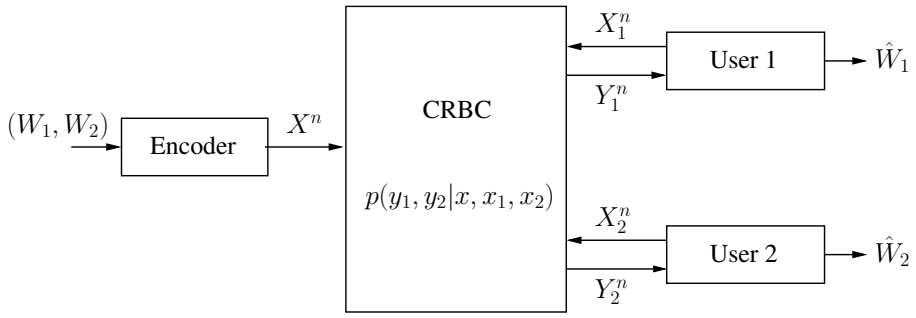

Figure 8.2: Cooperative relay broadcast channel (CRBC) with a two-sided cooperation link.

from the main receiver. Hence, our model is the first to consider the interactions between user cooperation and simultaneous secrecy of multiple users.

We note that, in the CRBC, each user eavesdrops as well as helps the other user. That is, the users are untrusted but non-malicious. There can be such communication scenarios. For instance, there can be military or other organizational networks, where even though multiple users are valid members of a network (hence are non-malicious), they may have different clearance levels with respect to the transmitted information. In this scenario also, users would want to (or be required to) help each other, but would not be allowed to decode each other's message.

In this chapter, we first propose an achievable scheme that combines Marton's

coding scheme for broadcast channels [11] and Cover and El Gamal's CAF scheme for relay channels [80]. A similar achievable scheme appeared in [74–76], where CAF is applied to a relay channel to provide improved secrecy for the main transmitter. A relay channel can be considered as a special case of the single-sided CRBC where the rate of the first user is set to zero.

To visualize the effects of cooperation on secrecy, we consider a Gaussian CRBC and show that both users can have positive secrecy rates through user cooperation. To obtain positive secrecy rates for both users, we provide different assignments for the auxiliary random variables appearing in the achievable rates. These auxiliary random variable assignments have dirty paper coding (DPC) interpretations [81]. In addition, we combine jamming and relaying to provide secrecy for both users when the relaying user is weak. Finally, we consider the CRBC with a two-sided cooperation link and provide an achievable scheme for this channel.

The aforementioned Gaussian CRBC example demonstrates that by means of cooperation, both users can have simultaneous secure communication with the transmitter, although this is not possible without cooperation. Hence, this example shows that, in fact, there can be synergy between cooperation and secrecy, and this synergy can be created by using CAF as the cooperative strategy.

8.2 Channel Model and Definitions

From here until the beginning of Section 8.8, we will focus on a single-sided CRBC, and refer to it simply as CRBC. The CRBC can be viewed as a relay channel

where the transmitter sends messages both to the relay node and the destination. Therefore, one of the users, user 1 in our case, in a CRBC both decodes its own message and also helps the other user. A CRBC consists of two message sets $w_1 \in \mathcal{W}_1, w_2 \in \mathcal{W}_2$, two input alphabets, one at the transmitter $x \in \mathcal{X}$ and one at user 1 $x_1 \in \mathcal{X}_1$, and two output alphabets $y_1 \in \mathcal{Y}_1, y_2 \in \mathcal{Y}_2$, where the former is for user 1 and the latter is for user 2. The channel is assumed to be memoryless and its transition probability distribution is $p(y_1, y_2|x, x_1)$.

A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two message sets as $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}$ and $\mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, an encoder at the transmitter with mapping $\mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, a set of relay functions at user 1, $x_{1,i} = f_i(y_{1,1}, \ldots, y_{1,i-1})$ for $1 \leq i \leq n$, two decoders, one at each user with the mappings $g_1 : \mathcal{Y}_1^n \to \mathcal{W}_1$ and $g_2 : \mathcal{Y}_2^n \to \mathcal{W}_2$. The probability of error is defined as $P_e^n = \max\left\{P_{e,1}^n, P_{e,2}^n\right\}$ where $P_{e,1}^n = \Pr\left(g_1(Y_1^n) \neq W_1\right), P_{e,2}^n = \Pr\left(g_2(Y_2^n) \neq W_2\right)$. The secrecy of the users is measured by the equivocation rates which are $\frac{1}{n}H(W_1|Y_2^n)$ and $\frac{1}{n}H(W_2|Y_1^n, X_1^n)$. Since user 1 has its own channel input, we condition the entropy rate of user 2's messages on this channel input.

A rate tuple $(R_1, R_2, R_{e,1}, R_{e,2})$ is said to be achievable if there exists a $(2^{nR_1}, 2^{nR_2}, n)$ code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n) \geq R_{e,1}, \quad \lim_{n\to\infty} \frac{1}{n} H(W_2|Y_1^n, X_1^n) \geq R_{e,2} \tag{8.1}$$

8.3 An Achievable Scheme

We now provide an achievable scheme which combines Marton's coding scheme for broadcast channels [11], the random binning scheme of [2, 3] for wiretap channels, and Cover and El Gamal's CAF scheme for relay channels [80]. The corresponding achievable rate-equivocation region is given by the following theorem.

Theorem 8.1 *The rate tuples* $(R_1, R_2, R_{e,1}, R_{e,2})$ *satisfying*

$$\begin{aligned}
R_1 &\leq I(V_1; Y_1|X_1) && (8.2)\\
R_2 &\leq I(V_2; Y_2, \hat{Y}_1|X_1) && (8.3)\\
R_1 + R_2 &\leq I(V_1; Y_1|X_1) + I(V_2; Y_2, \hat{Y}_1|X_1) - I(V_1; V_2) && (8.4)\\
R_{e,1} &\leq R_1 && (8.5)\\
R_{e,1} &\leq \Big[I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, X_1) - I(V_1; V_2)\Big]^+ && (8.6)\\
R_{e,2} &\leq R_2 && (8.7)\\
R_{e,2} &\leq \Big[I(V_2; Y_2, \hat{Y}_1|X_1) - I(V_2; Y_1|V_1, X_1) - I(V_1; V_2)\Big]^+ && (8.8)
\end{aligned}$$

are achievable for any distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(x_1)p(\hat{y}_1|x_1, v_1, y_1)p(y_1, y_2|x, x_1) \tag{8.9}$$

subject to the constraint

$$I(\hat{Y}_1; Y_1|X_1, V_1) \leq I(\hat{Y}_1, X_1; Y_2) \tag{8.10}$$

This theorem is a special case of Theorem 8.4 and obtained from the latter by setting $U = X_1$. Therefore, we will omit the proof of Theorem 8.1 here and will provide the proof of Theorem 8.4 in Appendix 8.11.4. In (8.6) and (8.8), $(x)^+$ is the positivity operator, i.e., $(x)^+ = \max(0, x)$.

In the achievable scheme given in Theorem 8.1, the transmitter uses a coding scheme that blends Marton's coding scheme and the random binning scheme of [2, 3]. Intuitively, the transmitter divides each user's message into two parts as the confidential and non-confidential parts, where the confidential part needs to be transmitted in perfect secrecy whereas there is no secrecy constraint on the non-confidential part. The division of each message into two parts forms the basis of the random binning scheme used in [2, 3] to provide confidentiality. In particular, the non-confidential message can be viewed as the necessary randomness to protect the confidential message. The transmitter encodes all these messages by using Marton's coding scheme, where the messages of one user, say user 1, are first encoded by using a standard single-user codebook, and the messages of the other user, say user 2, are encoded by using Gelfand-Pinsker's scheme [82]. While using Gelfand-Pinsker's scheme [82] for user 2's messages, the knowledge of user 1's codeword is exploited to improve the rate of user 2. Furthermore, to enlarge the achievable region, the transmitter can reverse the order of encoding, i.e., first encode user 2's messages, next encode user 1's messages by using the knowledge of user 2's codeword, and also use time-sharing between the two possible encoding orders. In the achievable scheme given in Theorem 8.1, user 1 first decodes its own message, and next uses the CAF scheme to help user 2, i.e., forms a compressed version of its own observation

and sends it to user 2. However, there are slight differences between the CAF used in the achievable scheme given in Theorem 8.1 and the original form of the CAF scheme in [80]. These differences originate from the secrecy concerns in our model, and are outlined in the following remark.

Remark 8.1 *We note that both the form of the probability distribution in (8.9) and the constraint in (8.10) in Theorem 8.1 are somewhat different than those of the classical CAF scheme in [80]. First, we condition the distribution of $\hat{Y}_1$ on V_1 to prevent the compressed version of Y_1 to leak any additional information regarding user 1's message on top of what user 2 already has through its own observation. The constraint in (8.10) also reflects this concern. Similar constraints on the distribution of $\hat{Y}_1$ and on the compression rate have appeared in [83], where these modifications are not due to secrecy constraints contrary to here. In [83], these are imposed to obtain higher rates for user 2 by removing user 1's private message from the compressed signal, whereas here, they are imposed not to let $\hat{Y}_1$ leak any additional information regarding user 1's message. Moreover, if we let user 1 compress its observation without erasing its own message from the observation, i.e., if we change the conditional distribution of $\hat{Y}_1$ to $p(\hat{y}_1|x_1, y_1)$, we can recover the constraint in [80] (see equations (29)-(31) in [83]).*

Remark 8.2 *If we disable the assistance of user 1 to user 2 by setting $X_1 = \hat{Y}_1 = \phi$, the channel model reduces to the broadcast channel with secrecy constraints, and the*

achievable equivocation region becomes

$$R_{e,1}^{BC} \leq I(V_1;Y_1) - I(V_1;Y_2|V_2) - I(V_1;V_2) \tag{8.11}$$

$$R_{e,2}^{BC} \leq I(V_2;Y_2) - I(V_2;Y_1|V_1) - I(V_1;V_2) \tag{8.12}$$

where we require the Markov chain $(V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2)$*. This result was derived in [64].*

Remark 8.3 *If we disable both cooperation between receivers by setting* $X_1 = \hat{Y}_1 = \phi$*, and also the confidential messages sent to user 1 by setting* $V_1 = \phi$*, the channel model reduces to the single-user eavesdropper channel, and the achievable equivocation rate for the second user becomes*

$$R_{e,2} \leq I(V_2;Y_2) - I(V_2;Y_1) \tag{8.13}$$

and the Markov chain $V_2 \rightarrow X \rightarrow (Y_1, Y_2)$ *is required by the probability distribution in (8.9). This is exactly the secrecy capacity of the single-user eavesdropper channel given in [3].*

Remark 8.4 *If we disable the confidential messages sent to user 1 by setting* $V_1 = \phi$*, the channel model reduces to a relay channel with secrecy constraints, and the achievable equivocation rate for the second user becomes*

$$R_{e,2} \leq I(V_2;Y_2,\hat{Y}_1|X_1) - I(V_2;Y_1|X_1) \tag{8.14}$$

subject to

$$I(\hat{Y}_1; Y_1|X_1) \leq I(\hat{Y}_1, X_1; Y_2) \tag{8.15}$$

and the corresponding joint distribution reduces to

$$p(v_2, x)p(x_1)p(\hat{y}_1|x_1, y_1)p(y_1, y_2|x, x_1) \tag{8.16}$$

Further, if we make the potentially suboptimal selection of $V_2 = X$*, the corresponding achievable secrecy rate and the constraint coincide with their counterparts found in [74, 76] for the relay channel.*

Remark 8.5 *By comparing the equivocation rates of the users in (8.6) and (8.8) and the equivocation rates of the users in the corresponding broadcast channel given in (8.11) and (8.12), we observe that the equivocation rate of user 1 may decrease depending on the information contained in* $\hat{Y}_1$ *and the equivocation rate of user 2 may increase depending on the channel conditions.*

Remark 8.6 *We will show in the next section, where we develop outer bounds for the rate-equivocation region, that if the channel of user 2 is degraded with respect to the channel of user 1 then* $R_{e,2} = 0$ *(see Remark 8.8), where degradedness is defined through the Markov chain* $X \to (X_1, Y_1) \to Y_2$*. Here, we show, as an interesting evaluation, that this achievable scheme cannot yield any positive secrecy rates in this*

case, as expected.

$$
\begin{aligned}
& I(V_2; Y_2, \hat{Y}_1 | X_1) - I(V_2; Y_1 | V_1, X_1) - I(V_1; V_2) \\
& \quad \leq I(V_2; Y_2, \hat{Y}_1, V_1 | X_1) - I(V_2; Y_1 | V_1, X_1) - I(V_1; V_2) && (8.17) \\
& \quad = I(V_2; Y_2, \hat{Y}_1 | V_1, X_1) + I(V_2; V_1 | X_1) - I(V_2; Y_1 | V_1, X_1) - I(V_1; V_2) && (8.18) \\
& \quad = I(V_2; Y_2, \hat{Y}_1 | V_1, X_1) - I(V_2; Y_1 | V_1, X_1) && (8.19) \\
& \quad \leq I(V_2; Y_2, \hat{Y}_1, Y_1 | V_1, X_1) - I(V_2; Y_1 | V_1, X_1) && (8.20) \\
& \quad = I(V_2; Y_2, Y_1 | V_1, X_1) + I(V_2; \hat{Y}_1 | V_1, X_1, Y_1, Y_2) - I(V_2; Y_1 | V_1, X_1) && (8.21) \\
& \quad = I(V_2; Y_2, Y_1 | V_1, X_1) - I(V_2; Y_1 | V_1, X_1) && (8.22) \\
& \quad = I(V_2; Y_2 | V_1, X_1, Y_1) && (8.23) \\
& \quad = 0 && (8.24)
\end{aligned}
$$

where in (8.19), we used the fact that X_1 *and* (V_1, V_2) *are independent in (8.22), we used the Markov chain* $(V_2, Y_2) \to (V_1, X_1, Y_1) \to \hat{Y}_1$ *which implies*

$$I(V_2; \hat{Y}_1 | V_1, X_1, Y_1, Y_2) = 0 \tag{8.25}$$

and in (8.24), we used the Markov chain $(V_1, V_2) \to X \to (X_1, Y_1) \to Y_2$ *which is due to the assumed degradedness.*

8.4 An Outer Bound

We now provide an outer bound for the rate-equivocation region. Our first outer bound in Theorem 8.2 uses auxiliary random variables. Next, in Theorem 8.3, we provide a simpler outer bound for user 2 using only the channel inputs and outputs, without employing any auxiliary random variables.

Theorem 8.2 *The rate-equivocation region of the CRBC lies in the union of the following rate tuples*

$$R_1 \leq I(V_1;Y_1|X_1) \tag{8.26}$$

$$R_2 \leq I(V_2;Y_2) \tag{8.27}$$

$$R_{e,1} \leq \min\left\{\tilde{R}_{e,1}, \bar{R}_{e,1}, R_1\right\} \tag{8.28}$$

$$R_{e,2} \leq \min\left\{\tilde{R}_{e,2}, \bar{R}_{e,2}, R_2\right\} \tag{8.29}$$

where

$$\tilde{R}_{e,1} = I(V_1;Y_1|U) - I(V_1;Y_2|U) \tag{8.30}$$

$$\tilde{R}_{e,2} = I(V_2;Y_2|U) - I(V_2;Y_1|U) \tag{8.31}$$

$$\bar{R}_{e,1} = I(V_1;Y_1|V_2) - I(V_1;Y_2|V_2) \tag{8.32}$$

$$\bar{R}_{e,2} = I(V_2;Y_2|V_1) - I(V_2;Y_1|V_1) \tag{8.33}$$

where the union is taken over all joint distributions satisfying the Markov chain

$$U \to (V_1, V_2) \to (X, X_1, Y_1) \to Y_2 \tag{8.34}$$

The proof of this theorem is given in Appendix 8.11.1.

The outer bounds on the equivocation rates given in Theorem 8.2 are reminiscent of the outer bound for the secrecy capacity of the discrete memoryless wiretap channel obtained in [3]. While the outer bound in [3] is tight for the wiretap channel, the outer bounds here for the CRBC are generally not tight. However, our outer bounds can be interpreted by referring to the outer bound in [3]. For example, user 1's equivocation rate is bounded by the minimum of three terms, see (8.28), where the first term, see (8.30), can be viewed as an outer bound for the secrecy capacity of the wiretap channel between the transmitter, user 1 (main receiver) and user 2 (eavesdropper), when one ignores the message sent to user 2, because this outer bound does not involve V_2. The second term, see (8.32), can be viewed similarly. This outer bound now considers the message sent to user 2, however, eliminates it by conditioning both mutual information terms in (8.32) on V_2.

Remark 8.7 *The bounds on the equivocation rates in Theorem 8.2 and those in [64], where the outer bounds are for the equivocation rates in a two-user broadcast channel with per-user secrecy constraints as in here, have the same expressions. The only difference between the two outer bounds is in the Markov chain over which the*

union is taken. The Markov chain in (8.34) contains the one in [64], which is

$$U \to (V_1, V_2) \to X \to (Y_1, Y_2) \tag{8.35}$$

which means that our outer bound here evaluates to a larger region than the one in [64]. This should be expected since the achievable rate-equivocation region here in our CRBC contains the achievable region in the broadcast channel.

We also provide a simpler outer bound for the equivocation rate of user 2 which does not involve any auxiliary random variables.

Theorem 8.3 *The equivocation rate of user 2 is bounded as follows*

$$R_{e,2} \leq \max_{p(x,x_1)} I(X; Y_2|X_1, Y_1) \tag{8.36}$$

The proof of this theorem is given in Appendix 8.11.2.

This outer bound is obtained by providing extra (i.e., side) information to user 2. In particular, to obtain the outer bound in Theorem 8.3, we consider a new channel where user 2 has access to user 1's observation. Thus, in this new channel, user 2's observation is improved as compared to the original channel. Consequently, an outer bound for the new channel also serves as an outer bound for the original channel.

Remark 8.8 *If the channel is degraded, then the equivocation rate of user 2 is zero,*

since

$$I(X;Y_2|X_1,Y_1)=0 \tag{8.37}$$

which follows from the Markov chain $X \to (X_1,Y_1) \to Y_2$ *which is a consequence of the degradedness.*

Remark 8.9 *We generally expect the outer bound in Theorem 8.3 to be loose because it essentially assumes that user 2 has a complete access to user 1's observation*[1] *whereas, in reality, user 2 has only limited information about user 1's observation, which it obtains through the cooperative link. However, if the link from user 1 to user 2 is strong enough, user 1 may be able to convey its observation to user 2 precisely in which case the outer bound in Theorem 8.3 can be close to the achievable rate obtained via the CAF scheme. For example, such a situation arises if the channel satisfies the following Markov chain*

$$X \to (X_1,Y_2) \to Y_1 \tag{8.38}$$

For such channels, by selecting $V_2=X, V_1=\hat{Y}_1=\phi$ *in the achievable scheme, we*

[1] In fact, this Sato-type [84] upper-bounding technique is used as a first step (before introducing noise correlation to tighten the upper bound) in finding the secrecy capacity of the MIMO wiretap channel [15–17, 21].

get the following equivocation rate for user 2

$$I(X;Y_2|X_1) - I(X;Y_1|X_1) = I(X;Y_2,Y_1|X_1) - I(X;Y_1|X_1) = I(X;Y_2|X_1,Y_1) \tag{8.39}$$

where the first equality is due to the Markov chain in (8.38). Hence, the outer bound in (8.36) gives the secrecy capacity for channels satisfying (8.38).

Remark 8.10 *Although we are able to provide a simple outer bound for the equivocation rate of user 2, that depends only on the channel inputs and outputs, finding such a simple outer bound for the equivocation rate of user 1 does not seem to be possible. One reason for this is that, user 1 can use its observation, i.e., Y_1, for encoding its input, i.e., X_1, and create correlation between its channel inputs and outputs across time. Consequently, this correlation cannot be accounted for without using auxiliary random variables. Another reason will be discussed in Remark 8.13.*

8.5 An Example: Gaussian CRBC

We now provide an example to show how the proposed achievable scheme can enlarge the secrecy region for a Gaussian broadcast channel. The channel outputs of a Gaussian CRBC are

$$Y_1 = X + Z_1 \tag{8.40}$$

$$Y_2 = X + X_1 + Z_2 \tag{8.41}$$

where $Z_1 \sim \mathcal{N}(0, N_1), Z_2 \sim \mathcal{N}(0, N_2)$ and are independent, $E[X^2] \leq P, E[X_1^2] \leq aP$. In this section, we assume that $N_2 > N_1$, i.e., user 1 has a stronger channel in the corresponding broadcast channel. Note that, in this case, if user 1 does not help user 2, e.g., in the corresponding broadcast channel, $R_{e,2} = 0$. We present two different achievable schemes for this channel where each one corresponds to a particular selection of the underlying random variables in Theorem 8.1 satisfying the probability distribution condition in (8.9). Proposition 8.1 assigns independent channel inputs for each user, whereas Proposition 8.2 uses a DPC scheme. For simplicity, we provide only the achievable equivocation region in the following propositions.

Proposition 8.1 *The following equivocation rates are achievable for all* $\alpha \in [0, 1]$

$$R_{e,1} \leq \frac{1}{2}\log\left(1 + \frac{\alpha P}{\bar{\alpha}P + N_1}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha P}{N_2}\right) \tag{8.42}$$

$$R_{e,2} \leq \frac{1}{2}\log\left(1 + \bar{\alpha}P\left(\frac{1}{\alpha P + N_2} + \frac{1}{N_1 + N_c}\right)\right) - \frac{1}{2}\log\left(1 + \frac{\bar{\alpha}P}{N_1}\right) \tag{8.43}$$

where $\bar{\alpha} = 1 - \alpha$ *and* N_c *is subject to*

$$N_c \geq \frac{N_2(\bar{\alpha}P + N_1) + P(\alpha\bar{\alpha}P + N_1)}{aP} \tag{8.44}$$

Proof: This achievable region can be obtained by selecting $V_1 \sim \mathcal{N}(0, \alpha P), V_2 \sim \mathcal{N}(0, \bar{\alpha}P)$, $X = V_1 + V_2$, $X_1 \sim \mathcal{N}(0, aP)$, $\hat{Y}_1 = Y_1 - V_1 + Z_c = V_2 + Z_1 + Z_c$ and $Z_c \sim \mathcal{N}(0, N_c)$, where V_1, V_2, X_1 and Z_c are independent. The rates are found by direct calculation of the expressions in Theorem 8.1 using the above selection of random variables. $\square$

This achievable region can be enlarged by introducing correlation between V_1, V_2. Since a joint encoding is performed at the transmitter, one of the users' signals can be treated as a non-causally known interference, and DPC [81] can be used. In the following proposition, the transmitter treats user 2's signal as a non-causally known interference.

Proposition 8.2 *The following equivocation rates are achievable for any γ and all $\alpha \in [0,1]$*

$$\begin{aligned} R_{e,1} \leq & \frac{1}{2}\log\left(1+\frac{(\bar{\alpha}\gamma+\alpha)^2 P}{(\alpha+\gamma^2\bar{\alpha})N_1+(\gamma-1)^2\alpha\bar{\alpha}P}\right)-\frac{1}{2}\log\left(1+\frac{\alpha P}{N_2}\right) \\ & -\frac{1}{2}\log\left(1+\gamma^2\frac{\bar{\alpha}}{\alpha}\right) \qquad (8.45) \\ R_{e,2} \leq & \frac{1}{2}\log\left(1+\frac{\bar{\alpha}P(N_1+N_c)+\bar{\alpha}(1-\gamma)^2P(\alpha P+N_2)}{(\alpha P+N_2)(N_1+N_c)}\right) \\ & -\frac{1}{2}\log\left(1+\frac{\alpha\bar{\alpha}(\gamma-1)^2P}{(\alpha+\gamma^2\bar{\alpha})N_1}\right)-\frac{1}{2}\log\left(1+\gamma^2\frac{\bar{\alpha}}{\alpha}\right) \qquad (8.46) \end{aligned}$$

where $\bar{\alpha}=1-\alpha$ and N_c is subject to

$$N_c \geq \frac{-\eta+\sqrt{\eta^2+4\theta\omega}}{2\theta} \qquad (8.47)$$

where

$$\theta = a(\alpha + \bar{\alpha}\gamma^2)P \tag{8.48}$$

$$\begin{aligned}\eta = &\left(\alpha + \gamma^2\bar{\alpha}\right) P\left[aN_1 + (1-\gamma)^2\bar{\alpha}P(a+\bar{\alpha})\right] \\ &- (P+N_2)\left[N_1(\alpha+\gamma^2\bar{\alpha}) + \alpha\bar{\alpha}(\gamma-1)^2P\right]\end{aligned} \tag{8.49}$$

$$\begin{aligned}\omega = &\left\{(P+N_2)\left[(1-\gamma)^2\bar{\alpha}P + N_1\right] - (1-\gamma)^2\bar{\alpha}^2P^2\right\} \\ &\times\left\{N_1\left(\alpha+\gamma^2\bar{\alpha}\right) + P\alpha\bar{\alpha}(\gamma-1)^2\right\}\end{aligned} \tag{8.50}$$

Proof: These equivocation rates are obtained by applying DPC for user 1. Let the channel input of the transmitter be $X = U_1 + U_2$ where $U_1 \sim \mathcal{N}(0, \alpha P), U_2 \sim \mathcal{N}(0, \bar{\alpha}P)$ and are independent. The auxiliary random variables are selected as $V_2 = U_2, V_1 = U_1 + \gamma U_2$, where for user 1, the signal of user 2 is treated as non-casually known interference at the transmitter. The channel output of user 1 is compressed as $\hat{Y}_1 = Y_1 - V_1 + Z_c = (1-\gamma)U_2 + Z_1 + Z_c$ where $Z_c \sim \mathcal{N}(0, N_c)$ is the compression noise. The channel input of user 1 is selected as $X_1 \sim \mathcal{N}(0, aP)$. Here, again, U_1, U_2, Z_c and X_1 are all independent. The rates are then found by direct calculation of the expressions in Theorem 8.1 using the above selection of random variables. $\square$

We note that, in both of the propositions above, $R_{e,2}$ is a monotonically decreasing function of N_c. Consequently, achievable $R_{e,2}$ depends on the quality of the cooperative link between the users. If this link gets better allowing user 1 to convey its observation in a finer form, user 2's secrecy increases. For illustrative purposes,

the rate regions given by Propositions 8.1 and 8.2 are evaluated for the parameters $P = 8, N_1 = 1, N_2 = 2$, and the corresponding plots are given in Figures 8.3 and 8.4. Note that since $N_2 > N_1$, if there was no cooperation between the users, user 2 could not have a positive secrecy rate. We observe from these figures that, thanks to the cooperation of the users, both users enjoy positive secrecy rates. However, we observe that a positive secrecy for user 2 comes at the expense of a decrease in the secrecy of user 1. In particular, for both propositions, maximum secrecy rate for user 2 is achieved when user 1 does not have any message itself and acts as a pure relay for user 2. Similarly, user 1 achieves the maximum secrecy rate when user 2 does not have any message.

We also note that the achievable secrecy rate regions for both Proposition 8.1 and Proposition 8.2 are monotonically increasing in a, i.e., the available power at user 1. In fact, for any given (P, N_1, N_2), there exist threshold values for a, denoted by $a_1^*(P, N_1, N_2)$ and $a_2^*(P, N_1, N_2)$, for Propositions 8.1 and 8.2, respectively, such that if $a \leq a_1^*(P, N_1, N_2)$ (resp. $a \leq a_2^*(P, N_1, N_2)$), Proposition 8.1 (resp. Proposition 8.2) cannot provide any positive secrecy rate for user 2, and if $a > a_1^*(P, N_1, N_2)$ (resp. $a > a_2^*(P, N_1, N_2)$), Proposition 8.1 (resp. Proposition 8.2) can provide a positive secrecy rate for user 2. Since the rate expressions involved in Propositions 8.1 and 8.2 are rather complicated, it does not seem that $a_j^*(P, N_1, N_2)$ admits a simple closed form expression. However, we numerically evaluated the threshold values for $(P = 8, N_1 = 1, N_2 = 2)$ (which is the parameter set that we use to obtain Figures 8.3 and 8.4) as $a_1^*(8, 1, 2) \approx 3.25$ and $a_2^*(8, 1, 2) \approx 1.25$. Thus, for $(P = 8, N_1 = 1, N_2 = 2)$, the minimum power required at user 1 to provide a

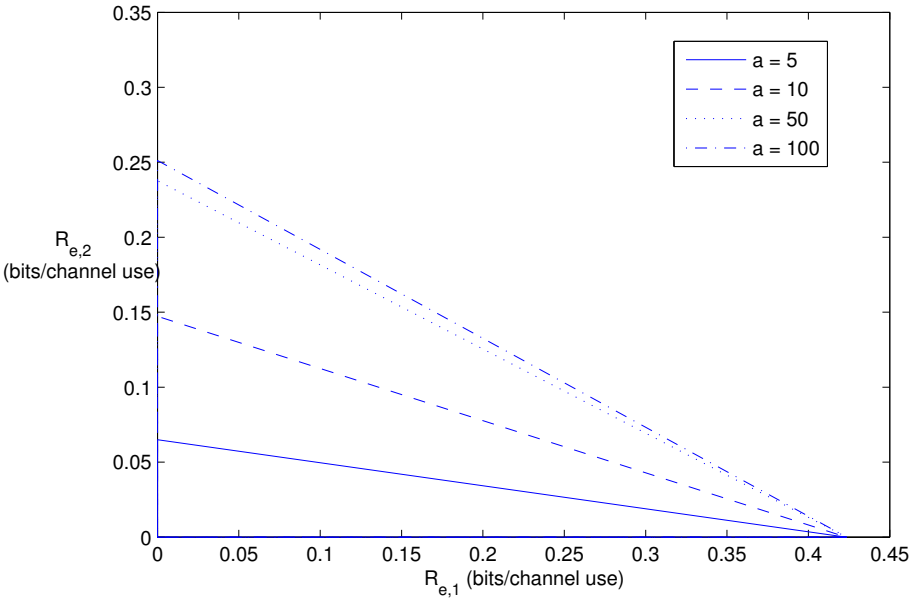

Figure 8.3: Achievable equivocation rate region for single-sided CRBC using Proposition 8.1 where V_1 and V_2 are independent. $P = 8, N_1 = 1, N_2 = 2$, i.e, user 2 has no secrecy rate in the underlying broadcast channel.

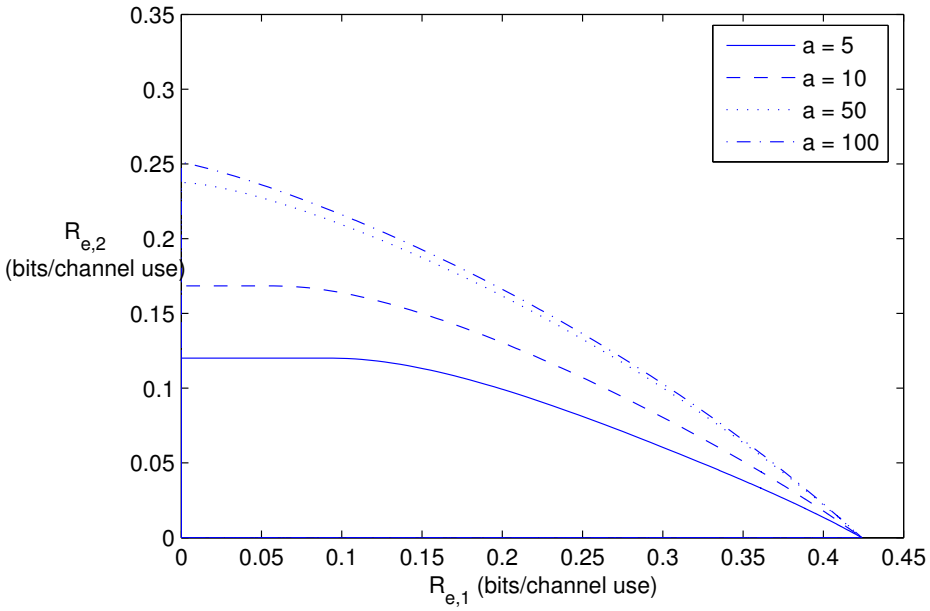

Figure 8.4: Achievable equivocation region for single-sided CRBC using Proposition 8.2 where V_1, V_2 are correlated, admitting a DPC interpretation. $P = 8, N_1 = 1, N_2 = 2$, i.e., user 2 has no secrecy rate in the underlying broadcast channel.

positive secrecy rate for user 2 by Proposition 8.2 is less than the minimum power required by Proposition 8.1. In fact, since Proposition 8.1 corresponds to a special case of Proposition 8.2, i.e., Proposition 8.1 can be recovered from Proposition 8.2 by setting $\gamma = 0$, in general, we have $a_2^*(P, N_1, N_2) \leq a_1^*(P, N_1, N_2)$.

Next, we note that, for both achievable schemes, as $a \to \infty$, the equivocation rate of user 2 approaches a limit. This is due to the fact that, as $a \to \infty$, the achievable equivocation rates are limited by the link between the transmitter and user 1. Moreover, as $a \to \infty$, user 1 can send its observation to user 2 perfectly. Thus, in this case, user 2 can be assumed to have a channel output of (Y_1, Y_2), which makes the channel of user 1 degraded with respect to the channel of user 2. Consequently, following the analysis carried out in Remark 8.9, we expect the outer bound in Theorem 8.3 to become tight as $a \to \infty$, which is stated in the next corollary.

Corollary 8.1 *As $a \to \infty$, the maximum achievable equivocation rate for user 2 becomes*

$$R_{e,2} = \frac{1}{2}\log\left(1 + P\left(\frac{1}{N_1} + \frac{1}{N_2}\right)\right) - \frac{1}{2}\log\left(1 + \frac{P}{N_1}\right) \tag{8.51}$$

The proof of this corollary is given in Appendix 8.11.3.

8.6 Joint Jamming and Relaying

The proposed achievability scheme and its application to Gaussian CRBC show us that user cooperation can enlarge the secrecy region. However, this achievability scheme and the Gaussian example provide us with only a limited picture of what can be achieved. In particular, the achievability scheme proposed in Section 8.3 is designed with the cooperating user (user 1) being the stronger of the two users in mind. Next, we want to explore what can be done when the cooperating user (user 1) is the weaker of the two users. In this case, without the cooperative link, user 1 cannot have a positive secrecy rate. Therefore, the first question to ask is, whether user 1 can have a positive secrecy rate by utilizing the cooperative link. The answer to this question is positive if user 1 uses the cooperative link to send a jamming signal to user 2. However, a more interesting question is whether both users can achieve positive secrecy simultaneously. The following theorem provides an achievable scheme, where user 1 performs a combination of jamming and relaying, to provide both users with positive secrecy rates.

Theorem 8.4 *The rate quadruples* $(R_1, R_2, R_{e,1}, R_{e,2})$ *satisfying*

$$\begin{aligned}
R_1 &\leq I(V_1; Y_1|X_1) && (8.52)\\
R_2 &\leq I(V_2; Y_2, \hat{Y}_1|U) && (8.53)\\
R_1 + R_2 &\leq I(V_1; Y_1|X_1) + I(V_2; Y_2, \hat{Y}_1|U) - I(V_1; V_2) && (8.54)\\
R_{e,1} &\leq R_1 && (8.55)\\
R_{e,1} &\leq \Big[I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, U) - I(V_1; V_2)\Big]^+ && (8.56)\\
R_{e,2} &\leq R_2 && (8.57)\\
R_{e,2} &\leq \Big[I(V_2; Y_2, \hat{Y}_1|U) - I(V_2; Y_1|V_1, X_1) - I(V_1; V_2)\Big]^+ && (8.58)
\end{aligned}$$

are achievable for any distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(u)p(x_1|u)p(\hat{y}_1|u, v_1, y_1)p(y_1, y_2|x, x_1) \tag{8.59}$$

subject to the following constraint

$$I(\hat{Y}_1; Y_1|X_1, V_1, U) \leq I(\hat{Y}_1, U; Y_2) \tag{8.60}$$

The proof of this theorem is given in Appendix 8.11.4.

We note that the achievable scheme given in Theorem 8.4 corresponds to the generalization of the achievable scheme given in Theorem 8.1 by using *channel pre-fixing* [3] at user 1. Channel pre-fixing refers to the construction of a hypothetical channel between the encoding scheme used at user 1 and the channel input of user

1. By means of this hypothetical channel, additional randomness can be introduced, and this randomness might be useful to improve the equivocation rates [3]. Besides channel pre-fixing, both achievable schemes use the same techniques, namely Marton's achievable scheme and random binning at the transmitter, and CAF scheme at user 1.

Remark 8.11 *In Theorem 8.4, U denotes the actual help signal, while the channel input X_1, which is correlated with U, may include an additional jamming attack. The intuition behind this achievable scheme is that, although user 2 should be able to decode U, it cannot decode the entire X_1. Therefore, since user 2 cannot decode and eliminate X_1 from Y_2, its channel becomes an attacked one, where decoding V_1 may be impossible. Therefore, in this scheme, user 1 first attacks user 2 to make its channel worse by associating U with many X_1s (hence, it confuses user 2), and then helps it to improve its secrecy rate.*

Remark 8.12 *We note that this achievable scheme is reminiscent of "cooperative jamming" [65]. In [65], the focus is on a two user MAC with an external eavesdropper, where one of the users attacks both the legitimate receiver and the eavesdropper, with the hope that it hurts the eavesdropper more than it hurts the legitimate receiver, and improves the secrecy of the legitimate receiver. In contrast, in our work, the relay (user 1) attacks user 2 to improve its own secrecy.*

8.7 Gaussian Example Revisited

Consider again the Gaussian CRBC, now with $N_1 > N_2$. The scheme proposed in Theorem 8.4 works as follows: user 1 divides X_1 into two parts. The first part carries the noise and the second part carries the bin index of $\hat{Y}_1$. Although Theorem 8.4 is valid for all cases, assume here that user 1 has large enough power. Then, the first part makes user 2's channel noisier than user 1's channel. This brings the situation to the case studied in Section 8.5. Consequently, we can now have a positive secrecy rate for user 1, and also provide a positive secrecy rate to user 2, by sending a compressed version of Y_1 to it, as in Section 8.5.

Proposition 8.3 *The following equivocation rates are achievable for all* $(\alpha, \beta) \in [0,1] \times [0,1]$

$$R_{e,1} \leq \frac{1}{2}\log\left(1+\frac{\alpha P}{\bar{\alpha}P+N_1}\right)-\frac{1}{2}\log\left(1+\frac{\alpha P}{a\bar{\beta}P+N_2}\right) \tag{8.61}$$

$$R_{e,2} \leq \frac{1}{2}\log\left(1+\bar{\alpha}P\left(\frac{1}{N_1+N_c}+\frac{1}{\alpha P+N_2+a\bar{\beta}P}\right)\right) - \frac{1}{2}\log\left(1+\frac{\bar{\alpha}P}{N_1}\right) \tag{8.62}$$

where $\bar{\alpha}=1-\alpha, \bar{\beta}=1-\beta$, *and* N_c *is subject to*

$$N_c \geq \frac{\bar{\alpha}P(\alpha P+N_2+a\bar{\beta}P)+N_1(P+N_2+a\bar{\beta}P)}{a\beta P} \tag{8.63}$$

Proof: This achievable region is obtained by selecting the random variables in Theorem 8.4 as $X = V_1 + V_2$ where $V_1 \sim \mathcal{N}(0,\alpha P), V_2 \sim \mathcal{N}(0,\bar{\alpha}P)$, $X_1 = U + Z_j$

where $U \sim \mathcal{N}(0, a\beta P), Z_j \sim \mathcal{N}(0, a\bar{\beta}P)$, $\hat{Y}_1 = Y_1 - V_1 + Z_c = V_2 + Z_1 + Z_c$ where $Z_c \sim \mathcal{N}(0, N_c)$. Moreover, V_1, V_2, U, Z_j, Z_c are all independent. Here, Z_j serves as the jamming signal, and U serves as the helper signal. User 1 first jams user 2 and makes its channel noisier than its own by using Z_j and then helps user 2 through sending a compressed version of its observation by using U. The rates are then found by direct calculation of the expressions in Theorem 8.4 using the above selection of random variables. $\square$

Moreover, as in Section 8.5, we can use DPC based schemes in this case also. The following proposition characterizes the DPC scheme for Theorem 8.4.

Proposition 8.4 *The following equivocation rates are achievable for any γ and for all $(\alpha, \beta) \in [0,1] \times [0,1]$*

$$R_{e,1} \leq \frac{1}{2}\log\left(1 + \frac{(\bar{\alpha}\gamma + \alpha)^2 P}{(\alpha + \gamma^2\bar{\alpha})N_1 + (\gamma-1)^2\alpha\bar{\alpha}P}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha P}{(a\bar{\beta}P + N_2)}\right) - \frac{1}{2}\log\left(1 + \gamma^2\frac{\bar{\alpha}}{\alpha}\right) \tag{8.64}$$

$$R_{e,2} \leq \frac{1}{2}\log\left(1 + \frac{\bar{\alpha}P(N_1+N_c) + \bar{\alpha}(1-\gamma)^2 P(\alpha P + a\bar{\beta}P + N_2)}{(\alpha P + a\bar{\beta}P + N_2)(N_1 + N_c)}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha\bar{\alpha}(\gamma-1)^2 P}{(\alpha + \gamma^2\bar{\alpha})N_1}\right) - \frac{1}{2}\log\left(1 + \gamma^2\frac{\bar{\alpha}}{\alpha}\right) \tag{8.65}$$

where $\bar{\alpha} = 1 - \alpha, \bar{\beta} = 1 - \beta$ and N_c is subject to

$$N_c \geq \frac{-\eta + \sqrt{\eta^2 + 4\theta\omega}}{2\theta} \tag{8.66}$$

where

$$\theta = a\beta(\alpha + \bar{\alpha}\gamma^2)P \tag{8.67}$$

$$\begin{aligned}\eta = &\left(\alpha + \gamma^2\bar{\alpha}\right) P\left[a\beta N_1 + (1-\gamma)^2\bar{\alpha}P(a\beta + \bar{\alpha})\right] \\ &- \left(P + a\bar{\beta}P + N_2\right)\left[N_1(\alpha + \gamma^2\bar{\alpha}) + \alpha\bar{\alpha}(\gamma-1)^2P\right]\end{aligned} \tag{8.68}$$

$$\begin{aligned}\omega = &\left[\left(P + a\bar{\beta} + N_2\right)\left[(1-\gamma)^2\bar{\alpha}P + N_1\right] - (1-\gamma)^2\bar{\alpha}^2P^2\right] \\ &\times \left[N_1\left(\alpha + \gamma^2\bar{\alpha}\right) + P\alpha\bar{\alpha}(\gamma-1)^2\right]\end{aligned} \tag{8.69}$$

Proof: All random variable selections are the same as in Proposition 8.2 except for X_1, U. Here, we choose $X_1 = Z_j + U$ and $U \sim \mathcal{N}(0, a\beta P), Z_j \sim \mathcal{N}(0, a\bar{\beta}P)$. U, Z_j are independent. $\square$

We first note that Propositions 8.3, 8.4 reduce to Propositions 8.1, 8.2, respectively, by simply selecting $\beta = 0$, i.e., no jamming. We provide a numerical example in Figures 8.5 and 8.6 for $P = 8, N_1 = 2, N_2 = 1$. Since $N_1 > N_2$, a positive secrecy rate for user 1 would not be possible if the cooperative link did not exist. However, if user 1 has enough power to make user 2's channel noisier by injecting Gaussian noise to it, user 1 can provide secrecy for itself. For user 1 to have positive secrecy, we need

$$a \geq \frac{N_1 - N_2}{P} \tag{8.70}$$

Otherwise, user 1 cannot have positive secrecy by using strategies employed in Propositions 8.3, 8.4. In addition, contrary to Section 8.5, we observe from Fig-

ures 8.5 and 8.6 that here DPC based schemes do not provide any gain with respect to the independent selection of V_1, V_2. Furthermore, we also apply Propositions 8.3 and 8.4 to the case where user 1 is stronger than user 2 by selecting the noise variances as $N_1 = 1, N_2 = 2$ as in Section 8.5 to show that propositions presented in this section cover the ones in Section 8.5.

We provide the corresponding graphs in Figures 8.7 and 8.8. Comparing Figures 8.3 (resp. 8.4) and 8.7 (resp. 8.8), we observe that even though the maximum secrecy rate of user 2 remains the same, the maximum secrecy rate of user 1 is improved significantly. This improvement comes, because through Propositions 8.3 and 8.4, user 1 jams the receiver of user 2.

Next, we examine Figures 8.3 and 8.7 in more detail. In Figure 8.3, for instance when $a = 100$, the largest $R_{e,2}$, which is about 0.25 bits/channel use, is obtained when $R_{e,1} = 0$. This corresponds to the case where user 1's rate and secrecy rate are set to zero. In this case, user 1 serves as a pure relay for user 2. The secrecy rate we obtain at this extreme is the same as [74–76]. At the other extreme, the largest $R_{e,1}$, which is about 0.42 bits/channel use, is obtained when $R_{e,2} = 0$. In this case, user 2 is just an eavesdropper in a single-user channel from the transmitter to user 1. The secrecy rate we obtain at this extreme is the same as [2, 3, 49]. Moreover, as we see from Figure 8.3, whenever user 1 helps user 2 to have positive secrecy, it needs to deviate from this extreme point. Thus, user 2's positive secrecy rates come at the expense of a decrease in user 1's secrecy rate. If we consider Figure 8.7, the largest $R_{e,2}$ is the same as that in Figure 8.3, which is again achieved when $R_{e,1} = 0$, i.e., when user 1 acts as a pure relay for user 2. However, in Figure 8.7,

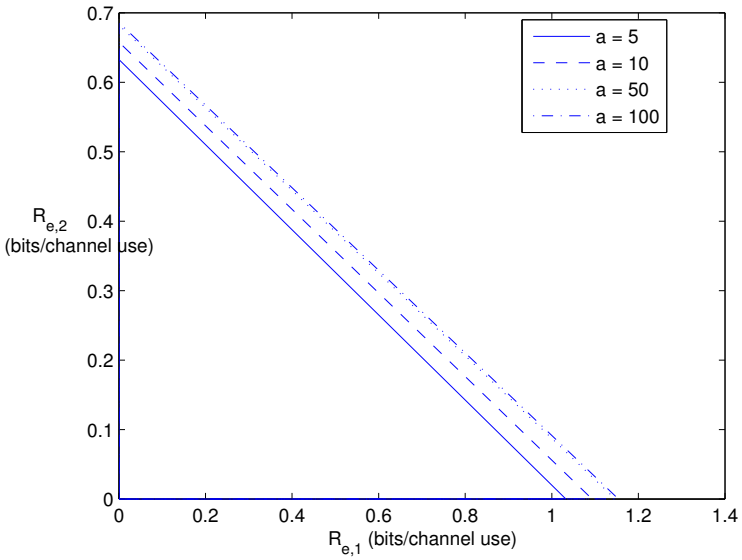

Figure 8.5: Achievable equivocation rate region using Proposition 8.3 where user 1 jams and relays, and V_1, V_2 are independent. $P = 8, N_1 = 2, N_2 = 1$, i.e., user 1 cannot have any positive secrecy in the underlying broadcast channel.

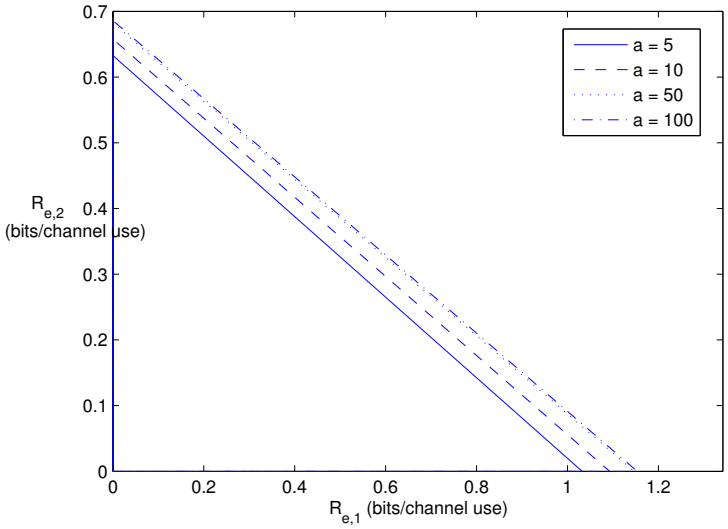

Figure 8.6: Achievable equivocation rate region using Proposition 8.4 where user 1 jams and relays, and V_1, V_2 are correlated, admitting a DPC interpretation. $P = 8, N_1 = 2, N_2 = 1$, i.e., user 1 cannot have any positive secrecy in the underlying broadcast channel.

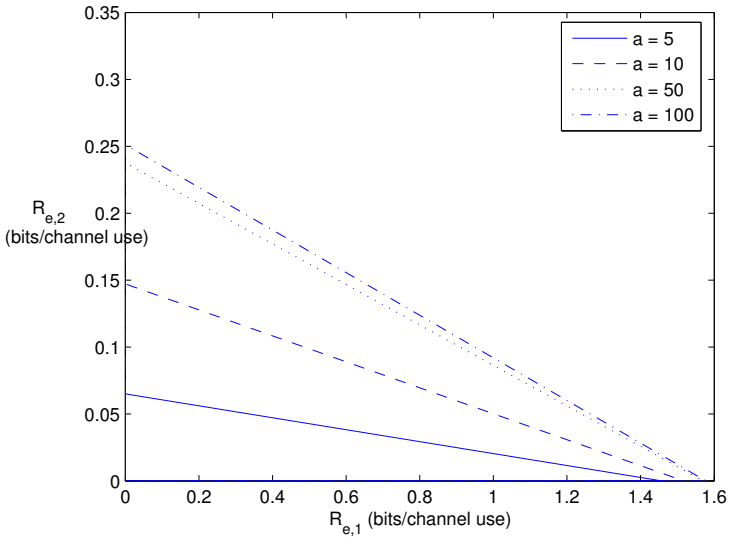

Figure 8.7: Achievable equivocation rate region using Proposition 8.3 where user 1 jams and relays, and V_1, V_2 are independent. $P = 8, N_1 = 1, N_2 = 2$, i.e., user 1's channel is stronger than user 2.

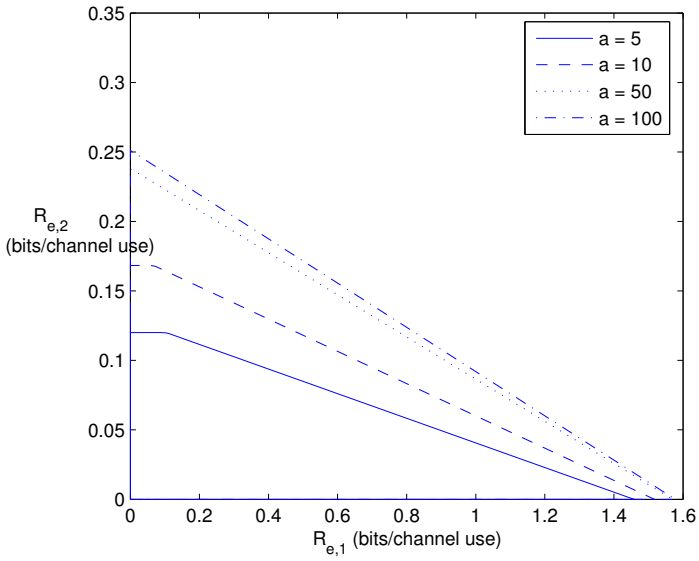

Figure 8.8: Achievable equivocation rate region using Proposition 8.4 where user 1 jams and relays, and V_1, V_2 are correlated, admitting a DPC interpretation. $P = 8, N_1 = 1, N_2 = 2$, i.e., user 1's channel is stronger than user 2.

user 1's maximum secrecy rate increases dramatically due to its jamming capabilities in Proposition 8.3. In Figure 8.7, user 1 achieves its maximum secrecy rate, which is about 1.58 bits/channel use, when it uses all of its power for jamming user 2's receiver and when the rate of user 2 is set to zero. We note that this rate is larger than that is achievable in the corresponding single-user eavesdropper channel from the transmitter to user 1, while user 2 is an eavesdropper. We observe from Figure 8.7 that when user 1 is able to jam and relay jointly, it can provide secrecy for user 2 while its own secrecy rate is still larger than that of the corresponding single-user eavesdropper channel. Thus, as opposed to the case where it can only relay, i.e., Proposition 8.1, both users enjoy secrecy in Proposition 8.3, while user 1 does not have to compromise from its own secrecy rate that is achievable in the underlying eavesdropper channel.

At first sight, this result may seem counterintuitive, because although user 1 spends some of its available power to jam user 2, user 2 still gets the same equivocation rate as if user 1 helps user 2 by using all its available power. However, this surprising result can be better understood by noting the fact that jamming and helping do not occur simultaneously, i.e., user 1 does not jam and help at the same time, instead, it uses time-sharing between jamming and relaying. In particular, Figure 8.7 clearly demonstrates the fact that user 1 uses time-sharing between two extreme operating points of Proposition 8.3 in order to provide a larger achievable secrecy rate region than the one in Figure 8.3. At one extreme operating point, user 1, to which no message is sent, acts as a pure relay for user 2, and at the other extreme operating point, user 1 acts as a pure jammer for user 2, to which no

message is sent. The same conclusion holds for Figure 8.8, i.e., Proposition 8.4, as well. However, in this case, at the extreme point where the maximum equivocation rate of user 2 is obtained, the equivocation rate of user 1 is not always zero, see the cases $a = 5, 10$ in Figures 8.4 and 8.8. In particular, Figure 8.9 shows the fact that user 1 employs time-sharing between two extreme operating points, where two extreme points, points A and B, are also noted.

Remark 8.13 *We are now ready to discuss why we could not find an outer bound for the equivocation rate of user 1 that relies only on the channel inputs and outputs. To understand this, we first examine the outer bound we found on the equivocation rate of user 2 in Theorem 8.3. This outer bound is obtained by giving the entire observation of user 1 to user 2 (i.e., $N_c = 0$). Hence, this is the best possible scenario as far as the channel of user 2 is concerned, and thus, it yields an outer bound. However, a similar approach cannot work for user 1, because although user 1 can have access to the observation of user 2, user 1 still has additional freedom (and opportunities) to increase its own secrecy rate by sending jamming signals over the cooperative link, as shown in this section. This is the main reason why we could not find a simple outer bound for user 1's secrecy rate using only the channel inputs/outputs.*

8.8 Two-sided Cooperation

In this section, we provide an achievable scheme for the CRBC with two-sided cooperation. In this case, each user can act as a relay for the other one; see Fig-

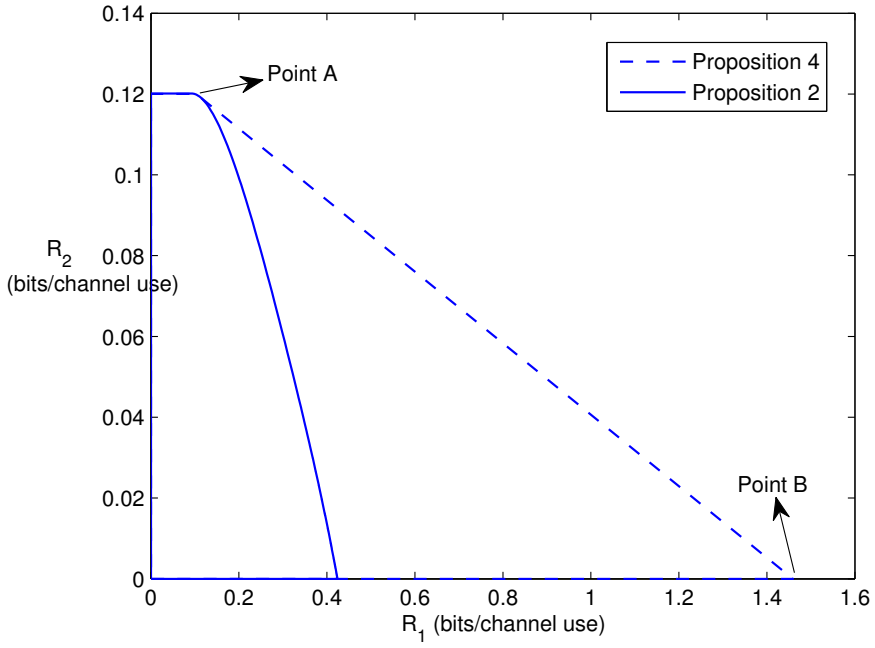

Figure 8.9: Achievable equivocation rate regions using Propositions 8.2 and 8.4 where user 1 jams and relays, and V_1, V_2 are correlated, admitting a DPC interpretation. $a = 5, P = 8, N_1 = 1, N_2 = 2$, i.e., user 1's channel is stronger than user 2.

ure 8.2. The corresponding channel consists of two message sets $w_1 \in \mathcal{W}_1, w_2 \in \mathcal{W}_2$, three input alphabets, one at the transmitter $x \in \mathcal{X}$, one at user 1 $x_1 \in \mathcal{X}_1$ and one at user 2 $x_2 \in \mathcal{X}_2$. The channel consists of two output alphabets denoted by $y_1 \in \mathcal{Y}_1, y_2 \in \mathcal{Y}_2$ at the two users. The channel is assumed to be memoryless and its transition probability distribution is $p(y_1, y_2|x, x_1, x_2)$.

A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two message sets as $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}$ and $\mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, an encoder at the transmitter which maps each pair $(w_1, w_2) \in (\mathcal{W}_1 \times \mathcal{W}_2)$ to a codeword $x^n \in \mathcal{X}^n$, a set of relay functions at user 1, $x_{1,i} = f_{1,i}(y_{1,1}, \ldots, y_{1,i-1})$,

$1 \leq i \leq n$, and a set of relay functions at user 2, $x_{2,i} = f_{2,i}(y_{2,1}, \ldots, y_{2,i-1})$, $1 \leq$

$i \leq n$, two decoders, one at user 1 and one at user 2 with the mappings $g_1 : \mathcal{Y}_1^n \rightarrow \mathcal{W}_1$, $g_2 : \mathcal{Y}_2^n \rightarrow \mathcal{W}_2$. Definitions for the error probability for this two-sided case are the same as in the single-sided case. The secrecy of the users is again measured by the equivocation rates which are $\frac{1}{n}H(W_1|Y_2^n, X_2^n)$ and $\frac{1}{n}H(W_2|Y_1^n, X_1^n)$. In this case, since user 2 has a channel input also, we condition the entropy rate of user 1's messages on this channel input.

A rate tuple $(R_1, R_2, R_{e,1}, R_{e,2})$ is said to be achievable if there exists a $(2^{nR_1}, 2^{nR_2}, n)$ code with $\lim_{n\rightarrow\infty} P_e^n = 0$, and

$$\lim_{n\rightarrow\infty} \frac{1}{n} H(W_1|Y_2^n, X_2^n) \geq R_{e,1}, \quad \lim_{n\rightarrow\infty} \frac{1}{n} H(W_2|Y_1^n, X_1^n) \geq R_{e,2} \tag{8.71}$$

The following theorem characterizes an achievable region for this channel model.

Theorem 8.5 *The rate tuples* $(R_1, R_2, R_{e,1}, R_{e,2})$ *satisfying*

$$R_1 \leq I(V_1; Y_1, \hat{Y}_2|X_1, U_2) \tag{8.72}$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|X_2, U_1) \tag{8.73}$$

$$R_1 + R_2 \leq I(V_1; Y_1, \hat{Y}_2|X_1, U_2) + I(V_2; Y_2, \hat{Y}_1|X_2, U_1) - I(V_1; V_2) \tag{8.74}$$

$$R_{e,1} \leq R_1 \tag{8.75}$$

$$R_{e,1} \leq \Big[I(V_1; Y_1, \hat{Y}_2|X_1, U_2) - I(V_1; Y_2, \hat{Y}_1|V_2, X_2, U_1) - I(V_1; V_2)\Big]^+ \tag{8.76}$$

$$R_{e,2} \leq R_2 \tag{8.77}$$

$$R_{e,2} \leq \Big[I(V_2; Y_2, \hat{Y}_1|X_2, U_1) - I(V_2; Y_1, \hat{Y}_2|V_1, X_1, U_2) - I(V_1; V_2)\Big]^+ \tag{8.78}$$

are achievable for any distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(u_1, x_1)p(\hat{y}_1|u_1, y_1)p(u_2, x_2)p(\hat{y}_2|u_2, y_2)p(y_1, y_2|x, x_1, x_2) \quad (8.79)$$

subject to the following constraints

$$I(\hat{Y}_1; Y_1|U_1, X_1, U_2) \leq I(\hat{Y}_1, U_1; Y_2|X_2) \quad (8.80)$$

$$I(\hat{Y}_2; Y_2|U_2, X_2, U_1) \leq I(\hat{Y}_2, U_2; Y_1|X_1) \quad (8.81)$$

The proof of this theorem is given in Appendix 8.11.5.

Similar to the achievable schemes given in Theorems 8.1 and 8.4, the achievable scheme in Theorem 8.5 also blends Marton's achievable scheme for broadcast channels [11], the random binning scheme of [3] to provide confidentiality, and the CAF scheme [80]. In particular, the transmitter uses Marton's achievable scheme and random binning, and each user employs a CAF-based cooperation scheme to help the other user. Similar to Theorem 8.4, in Theorem 8.5, channel pre-fixing is used as well. The main difference between the previous achievable schemes in Theorems 8.1, 8.4 and the achievable scheme in Theorem 8.5 comes from how CAF is performed as a cooperation strategy, and in particular, how compression is performed. Contrary to the previous achievable schemes given in Theorem 8.1 and 8.4, here users do not compress their observations after erasing their codewords from the observations; this is why we did not condition $\hat{Y}_1$ (resp. $\hat{Y}_2$) on V_1 (resp. V_2) in (8.79). In fact, they cannot remove their own codewords from their observations because

each user employs a sliding-window type decoding scheme, i.e., they should wait until the next block to decode their own codewords, whereas compression should be performed right after the reception of the previous block, at which time they have not yet decoded their own messages. However, we note that this achievable scheme also provides opportunities for jamming as did the achievable scheme provided in Section 8.6.

8.9 Gaussian Example for Two-sided Cooperation

The channel outputs of a Gaussian CRBC with two-sided cooperation are

$$Y_1 = X + X_2 + Z_1 \tag{8.82}$$

$$Y_2 = X + X_1 + Z_2 \tag{8.83}$$

where $Z_1 \sim \mathcal{N}(0, N_1), Z_2 \sim \mathcal{N}(0, N_2)$ and are independent, $E[X^2] \leq P$, $E[X_1^2] \leq a_1 P$, $E[X_2^2] \leq a_2 P$.

We present the following proposition which characterizes an achievable equivocation region.

Proposition 8.5 *The following equivocation rates are achievable for all* $(\alpha, \beta_1, \beta_2) \in$

$[0,1]^3$

$$R_{e,1} \leq \frac{1}{2}\log\left(1+\frac{\alpha P(N_1+a_2\bar{\beta}_2P+N_2+N_{c,2})}{\bar{\alpha}P(N_1+a_2\bar{\beta}_2P+N_2+N_{c,2})+(N_1+a_2\bar{\beta}_2P)(N_2+N_{c,2})}\right) - \frac{1}{2}\log\left(1+\alpha P\left(\frac{1}{a_1\bar{\beta}_1P+N_2}+\frac{1}{N_1+N_{c,1}}\right)\right) \tag{8.84}$$

$$R_{e,2} \leq \frac{1}{2}\log\left(1+\frac{\bar{\alpha}P(N_2+a_1\bar{\beta}_1P+N_2+N_{c,1})}{\alpha P(N_2+a_1\bar{\beta}_1P+N_1+N_{c,1})+(N_2+a_1\bar{\beta}_1P)(N_1+N_{c,1})}\right) - \frac{1}{2}\log\left(1+\alpha P\left(\frac{1}{a_2\bar{\beta}_2P+N_1}+\frac{1}{N_2+N_{c,2}}\right)\right) \tag{8.85}$$

where $\bar{\alpha}=1-\alpha, \bar{\beta}_1=1-\beta_1, \bar{\beta}_2=1-\beta_2$, *and* $N_{c,1}, N_{c,2}$ *are subject to*

$$N_{c,1} \geq \frac{-b_{11}+\sqrt{b_{11}^2+4a_{11}c_{11}}}{2a_{11}} \tag{8.86}$$

$$N_{c,2} \geq \frac{-b_{22}+\sqrt{b_{22}^2+4a_{22}c_{22}}}{2a_{22}} \tag{8.87}$$

and

$$a_{11} = a_1\beta_1P \tag{8.88}$$

$$b_{11} = P\big(P+a_1\beta_1(P+N_1)\big)-(P+N_1+a_2\bar{\beta}_2P)(P+N_2+a_1\bar{\beta}_1P) \tag{8.89}$$

$$c_{11} = (P+N_1+a_2\bar{\beta}_2P)\big(PN_1+(P+N_1)(N_2+a_1\bar{\beta}_1P)\big) \tag{8.90}$$

$$a_{22} = a_2\beta_2P \tag{8.91}$$

$$b_{22} = P\big(P+a_2\beta_2(P+N_2)\big)-(P+N_1+a_2\bar{\beta}_2P)(P+N_2+a_1\bar{\beta}_1P) \tag{8.92}$$

$$c_{22} = (P+N_2+a_1\bar{\beta}_1P)\big(PN_2+(P+N_2)(N_1+a_2\bar{\beta}_2P)\big) \tag{8.93}$$

Proof: This achievable region is obtained by selecting $X = V_1 + V_2$ where

$V_1 \sim \mathcal{N}(0, \alpha P)$, $V_2 \sim \mathcal{N}(0, \bar{\alpha} P)$ and are independent, $X_i = U_i + \tilde{Z}_i$ where $U_i \sim \mathcal{N}(0, a_i \beta_i P)$, $\tilde{Z}_i \sim \mathcal{N}(0, a_i \bar{\beta}_i P), i = 1, 2$ and independent, and $\hat{Y}_i = Y_i + Z_{c,i}$ where $Z_{c,i} \sim \mathcal{N}(0, N_{c,i}), i = 1, 2$ and are independent of all other random variables. Direct calculation of rates in Theorem 8.5 with these random variable selections yields the achievable region. $\square$

A numerical example is given in Figure 8.10 for the case $P = 8, N_1 = 1, N_2 = 2$. Comparing Figure 8.10 with Figures 8.7 and 8.8, we observe that user 2's secrecy rate improves significantly because now user 2 can jam user 1 to improve its own secrecy rate. We also observe that user 1's secrecy rate improves as well, compared to Section 8.7. The increase in user 1's secrecy in this two-sided case is due to the fact that user 2 now acts as a relay for user 1. However, when user 1 jams user 2 using all of its power, it limits the help that comes from user 2, hence Theorem 8.5 provides only a modest secrecy rate increase for user 1 on top of what Theorem 8.4 already provides.

8.10 Conclusions

In this chapter, we study the effects of cooperation on secrecy by considering the CRBC. We propose an achievable scheme relying on the CAF scheme and evaluate it for the Gaussian CRBC. This evaluation reveals that there is a synergy between user cooperation and secrecy, since both users can have secrecy in a Gaussian CRBC, although this is not possible when we remove the links between the receivers, i.e., without cooperation. It is worth noting that the synergy between user cooperation

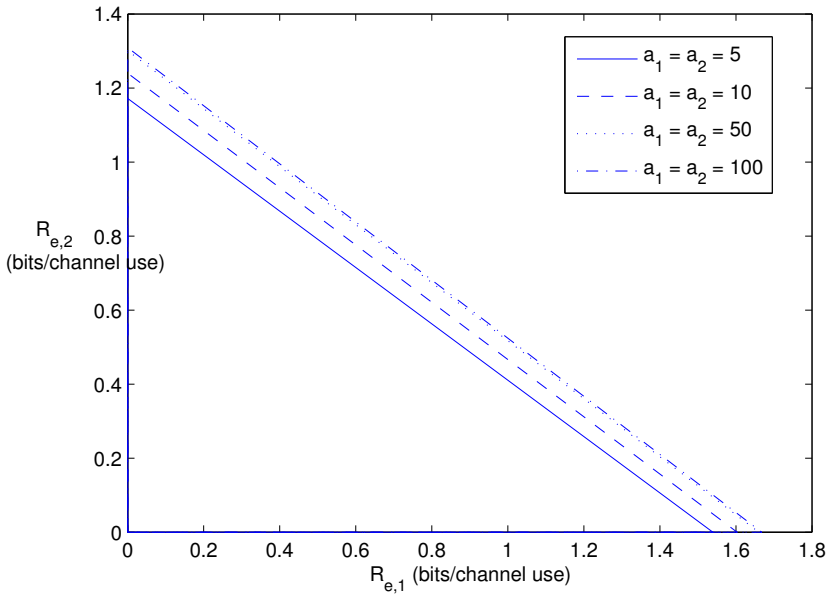

Figure 8.10: Achievable equivocation rate region using Proposition 8.5 where each user can jointly jam and relay. $P = 8, N_1 = 1, N_2 = 2$, i.e., user 2 cannot have any positive secrecy in the underlying broadcast channel.

and secrecy depends on the cooperative strategy used.

8.11 Appendix

8.11.1 Proof of Theorem 8.2

Here we prove the outer bound on the capacity-equivocation region of the CRBC given in Theorem 8.2 which closely follows the converse given in [3] and the outer

bound in [64]. First, define the following random variables

$$U_i = Y_1^{i-1} Y_{2,i+1}^n \tag{8.94}$$

$$V_{1,i} = W_1 U_i \tag{8.95}$$

$$V_{2,i} = W_2 U_i \tag{8.96}$$

which satisfy the following Markov chain

$$U_i \to (V_{1,i}, V_{2,i}) \to (X_i, X_{1,i}, Y_{1,i}) \to Y_{2,i} \tag{8.97}$$

but do not satisfy the following one

$$U_i \to (V_{1,i}, V_{2,i}) \to (X_i, X_{1,i}) \to (Y_{1,i}, Y_{2,i}) \tag{8.98}$$

because of the encoding function employed at user 1 which can generate correlation between $Y_{1,i}$ and $\left(Y_{1,i+1}^n, Y_{2,i+1}^n\right)$ through $X_{1,i+1}$ that cannot be resolved by conditioning on $(X_i, X_{1,i})$. For a similar discussion, the reader can refer to [85].

We start with the achievable rate of user 1.

$$
\begin{aligned}
nR_1 &= H(W_1) = I(W_1; Y_1^n) + H(W_1|Y_1^n) && (8.99)\\
&\leq I(W_1; Y_1^n) + \epsilon_n && (8.100)\\
&= \sum_{i=1}^{n} I(W_1; Y_{1,i}|Y_1^{i-1}) + \epsilon_n && (8.101)\\
&= \sum_{i=1}^{n} H(W_1|Y_1^{i-1}) - H(W_1|Y_1^{i-1}, Y_{1,i}) + \epsilon_n && (8.102)\\
&= \sum_{i=1}^{n} H(W_1|Y_1^{i-1}, X_{1,i}) - H(W_1|Y_1^{i-1}, Y_{1,i}) + \epsilon_n && (8.103)\\
&\leq \sum_{i=1}^{n} H(W_1|Y_1^{i-1}, X_{1,i}) - H(W_1|Y_1^{i-1}, Y_{1,i}, X_{1,i}) + \epsilon_n && (8.104)\\
&= \sum_{i=1}^{n} I(W_1; Y_{1,i}|Y_1^{i-1}, X_{1,i}) + \epsilon_n && (8.105)\\
&\leq \sum_{i=1}^{n} H(Y_{1,i}|X_{1,i}) - H(Y_{1,i}|Y_1^{i-1}, X_{1,i}, W_1) + \epsilon_n && (8.106)\\
&\leq \sum_{i=1}^{n} H(Y_{1,i}|X_{1,i}) - H(Y_{1,i}|Y_1^{i-1}, X_{1,i}, W_1, Y_{2,i+1}^n) + \epsilon_n && (8.107)\\
&= \sum_{i=1}^{n} I(V_{1,i}; Y_{1,i}|X_{1,i}) + \epsilon_n && (8.108)
\end{aligned}
$$

where (8.100) is due to Fano's lemma, (8.103) follows from the Markov chain $W_1 \rightarrow Y_1^{i-1} \rightarrow X_{1,i}$, (8.104), (8.106) and (8.107) are due to the fact that conditioning cannot increase entropy, and (8.108) follows from the definition of $V_{1,i}$ in (8.95).

Similarly, for the achievable rate of user 2, we have

$$\begin{aligned} nR_2 &\leq I(W_2; Y_2^n) + \epsilon_n && (8.109)\\ &= \sum_{i=1}^{n} I(W_2; Y_{2,i}|Y_{2,i+1}^n) + \epsilon_n && (8.110)\\ &= \sum_{i=1}^{n} H(Y_{2,i}|Y_{2,i+1}^n) - H(Y_{2,i}|Y_{2,i+1}^n, W_2) + \epsilon_n && (8.111)\\ &\leq \sum_{i=1}^{n} H(Y_{2,i}) - H(Y_{2,i}|Y_{2,i+1}^n, W_2, Y_1^{i-1}) + \epsilon_n && (8.112)\\ &\leq \sum_{i=1}^{n} I(V_{2,i}; Y_{2,i}) + \epsilon_n && (8.113) \end{aligned}$$

where (8.109) is due to Fano's lemma, (8.112) is due to the fact that conditioning cannot increase entropy, and (8.113) follows from the definition of $V_{2,i}$ given in (8.96).

We now derive the outer bounds on the equivocation rates starting with user 1.

$$\begin{aligned} nR_{e,1} &= H(W_1|Y_2^n) = H(W_1) - I(W_1; Y_2^n) && (8.114)\\ &= I(W_1; Y_1^n) - I(W_1; Y_2^n) + H(W_1|Y_1^n) && (8.115)\\ &\leq I(W_1; Y_1^n) - I(W_1; Y_2^n) + \epsilon_n && (8.116)\\ &= \sum_{i=1}^{n} I(W_1; Y_{1,i}|Y_1^{i-1}) - I(W_1; Y_{2,i}|Y_{2,i+1}^n) + \epsilon_n && (8.117)\\ &= \sum_{i=1}^{n} I(W_1, Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}) - I(Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_1)\\ &\quad - I(W_1, Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n) + I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n, W_1) + \epsilon_n && (8.118) \end{aligned}$$

where (8.116) is due to Fano's lemma. Using [3]

$$\sum_{i=1}^{n} I(Y_{2,i+1}^{n}; Y_{1,i}|Y_1^{i-1}, W_1) = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^{n}, W_1) \tag{8.119}$$

in (8.118), we obtain

$$\begin{aligned} nR_{e,1} &\leq \sum_{i=1}^{n} I(W_1, Y_{2,i+1}^{n}; Y_{1,i}|Y_1^{i-1}) - I(W_1, Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^{n}) + \epsilon_n & (8.120) \\ &= \sum_{i=1}^{n} I(W_1; Y_{1,i}|Y_1^{i-1}, Y_{2,i+1}^{n}) + I(Y_{2,i+1}^{n}; Y_{1,i}|Y_1^{i-1}) \\ &\quad - I(W_1; Y_{2,i}|Y_{2,i+1}^{n}, , Y_1^{i-1}) - I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^{n}) + \epsilon_n & (8.121) \end{aligned}$$

Now, using [3]

$$\sum_{i=1}^{n} I(Y_{2,i+1}^{n}; Y_{1,i}|Y_1^{i-1}) = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^{n}) \tag{8.122}$$

in (8.121), we obtain

$$\begin{aligned} nR_{e,1} &\leq \sum_{i=1}^{n} I(W_1; Y_{1,i}|Y_1^{i-1}, Y_{2,i+1}^{n}) - I(W_1; Y_{2,i}|Y_{2,i+1}^{n}, Y_1^{i-1}) + \epsilon_n & (8.123) \\ &= \sum_{i=1}^{n} I(W_1; Y_{1,i}|U_i) - I(W_1; Y_{2,i}|U_i) + \epsilon_n & (8.124) \\ &= \sum_{i=1}^{n} I(W_1, U_i; Y_{1,i}|U_i) - I(W_1, U_i; Y_{2,i}|U_i) + \epsilon_n & (8.125) \\ &= \sum_{i=1}^{n} I(V_{1,i}; Y_{1,i}|U_i) - I(V_{1,i}; Y_{2,i}|U_i) + \epsilon_n & (8.126) \end{aligned}$$

where (8.124) and (8.126) follow from the definitions of U_i and $V_{1,i}$ given in (8.94)

and (8.95), respectively. Similarly, we can use the preceding technique for user 2's equivocation rate as well after noting that

$$nR_{e,2} \leq H(W_2|Y_1^n, X_1^n) \leq H(W_2|Y_1^n) \tag{8.127}$$

which leads to

$$nR_{e,2} \leq \sum_{i=1}^{n} I(V_{2,i}; Y_{2,i}|U_i) - I(V_{2,i}; Y_{1,i}|U_i) + \epsilon_n \tag{8.128}$$

The other bounds on the equivocation rates can be derived as follows.

$$nR_{e,1} = H(W_1|Y_2^n) \leq H(W_1, W_2|Y_2^n) \tag{8.129}$$

$$= H(W_1|W_2, Y_2^n) + H(W_2|Y_2^n) \tag{8.130}$$

$$\leq H(W_1|W_2, Y_2^n) + \epsilon_n \tag{8.131}$$

$$= I(W_1; Y_1^n|W_2) - I(W_1; Y_2^n|W_2) + H(W_1|W_2, Y_1^n) + \epsilon_n \tag{8.132}$$

$$\leq I(W_1; Y_1^n|W_2) - I(W_1; Y_2^n|W_2) + \epsilon_n' \tag{8.133}$$

$$= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_2, Y_1^{i-1}) - I(W_1; Y_{2,i}|W_2, Y_{2,i+1}^n) + \epsilon_n' \tag{8.134}$$

$$= \sum_{i=1}^{n} I(W_1, Y_{2,i+1}^n; Y_{1,i}|W_2, Y_1^{i-1}) - I(W_1, Y_1^{i-1}; Y_{2,i}|W_2, Y_{2,i+1}^n) + \epsilon_n' \tag{8.135}$$

$$= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_2, Y_1^{i-1}, Y_{2,i+1}^n) - I(W_1; Y_{2,i}|W_2, Y_{2,i+1}^n, Y_1^{i-1}) + \epsilon_n' \tag{8.136}$$

$$= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_2, U_i) - I(W_1; Y_{2,i}|W_2, U_i) + \epsilon_n' \tag{8.137}$$

$$= \sum_{i=1}^{n} I(W_1, U_i; Y_{1,i}|W_2, U_i) - I(W_1, U_i; Y_{2,i}|W_2, U_i) + \epsilon_n' \tag{8.138}$$

$$= \sum_{i=1}^{n} I(V_{1,i}; Y_{1,i}|V_{2,i}) - I(V_{1,i}; Y_{2,i}|V_{2,i}) + \epsilon_n' \tag{8.139}$$

where (8.131) and (8.133) are due to Fano's lemma, and (8.135) and (8.136) are due to the following identities [3]

$$\sum_{i=1}^{n} I(Y_{2,i+1}^n; Y_{1,i}|W_1, W_2, Y_1^{i-1}) = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|W_1, W_2, Y_{2,i+1}^n) \tag{8.140}$$

$$\sum_{i=1}^{n} I(Y_{2,i+1}^n; Y_{1,i}|W_2, Y_1^{i-1}) = \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|W_2, Y_{2,i+1}^n) \tag{8.141}$$

respectively. Finally, (8.137) and (8.139) follow from the definitions of $U_i, V_{1,i}$ and $V_{2,i}$

given in (8.94), (8.95) and (8.96), respectively. Similarly, we can use this technique to bound user 2's equivocation rate after noting that $H(W_2|Y_1^n, X_1^n) \leq H(W_2|Y_1^n)$, which leads to

$$nR_{e,2} \leq H(W_2|Y_1^n, X_1^n) \leq H(W_2|Y_1^n) \leq \sum_{i=1}^{n} I(V_{2,i}; Y_{2,i}|V_{1,i}) - I(V_{2,i}; Y_{2,i}|V_{1,i}) + \epsilon_n' \tag{8.142}$$

To express the outer bounds obtained above in a single-letter form, we define $U = JU_J, V_1 = V_{1,J}, V_2 = V_{2,J}, X = X_J, X_1 = X_{1,J}, Y_1 = Y_{1,J}, Y_2 = Y_{2,J}$ where J is a random variable which is uniformly distributed over $\{1, \ldots, n\}$. Using these new definitions, we can reach the single-letter expressions given in Theorem 8.2, hence completing the proof.

8.11.2 Proof of Theorem 8.3

The proof is as follows.

$$
\begin{aligned}
R_{e,2} &\leq H(W_2|Y_1^n, X_1^n) && (8.143)\\
&\leq I(W_2; Y_2^n|X_1^n) - I(W_2; Y_1^n|X_1^n) + H(W_2|Y_2^n, X_1^n) && (8.144)\\
&\leq I(W_2; Y_2^n|X_1^n) - I(W_2; Y_1^n|X_1^n) + \epsilon_n && (8.145)\\
&\leq I(W_2; Y_2^n|X_1^n, Y_1^n) + \epsilon_n && (8.146)\\
&\leq I(X^n, W_2; Y_2^n|X_1^n, Y_1^n) + \epsilon_n && (8.147)\\
&= I(X^n; Y_2^n|X_1^n, Y_1^n) + \epsilon_n && (8.148)\\
&= \sum_{i=1}^{n} I(X^n; Y_{2,i}|X_1^n, Y_1^n, Y_2^{i-1}) + \epsilon_n && (8.149)\\
&\leq \sum_{i=1}^{n} H(Y_{2,i}|X_{1,i}, Y_{1,i}) - H(Y_{2,i}|X_1^n, Y_1^n, Y_2^{i-1}, X^n) + \epsilon_n && (8.150)\\
&= \sum_{i=1}^{n} H(Y_{2,i}|X_{1,i}, Y_{1,i}) - H(Y_{2,i}|X_{1,i}, Y_{1,i}, X_i) + \epsilon_n && (8.151)\\
&= \sum_{i=1}^{n} I(X_i; Y_{2,i}|X_{1,i}, Y_{1,i}) + \epsilon_n && (8.152)
\end{aligned}
$$

where (8.145) is due to Fano's lemma, (8.148) follows from the fact that given X^n, W_2 is independent of all other random variables, (8.150) is due to the fact that conditioning cannot increase entropy, and (8.151) follows from the Markov chains

$$
\begin{aligned}
(Y_{1,i}, Y_{2,i}) \rightarrow (X_i, X_{1,i}) \rightarrow (Y_1^{i-1}, Y_2^{i-1}, X^{i-1}, X_1^{i-1}) && (8.153)\\
Y_{2,i} \rightarrow (X_i, X_{1,i}, Y_{1,i}) \rightarrow (Y_{1,i+1}^n, X_{i+1}^n, X_{1,i+1}^n) && (8.154)
\end{aligned}
$$

Thus, after defining an independent random variable J, that is uniformly distributed over $\{1, \ldots, n\}$, and $X = X_J, X_1 = X_{1,J}, Y_1 = Y_{1,J}, Y_2 = Y_{2,J}$, we can obtain the single-letter expression in Theorem 8.3, completing the proof.

8.11.3 Proof of Corollary 8.1

In Propositions 8.1 and 8.2, if we take $a \to \infty$, then the secrecy rate in (8.51) can be shown to be achievable. As a notational remark, $H(\cdot)$ denotes the differential entropy in this section. We now compute an outer bound for $R_{e,2}$ using Theorem 8.3,

$$
\begin{aligned}
R_{e,2} &\leq I(X; Y_2|X_1, Y_1) && (8.155)\\
&= H(Y_2|X_1, Y_1) - H(Z_2|Z_1) && (8.156)\\
&\leq H(X + Z_2|Y_1) - H(Z_2) && (8.157)\\
&\leq H(X + Z_2 - \alpha Y_1) - \frac{1}{2}\log(2\pi e N_2) && (8.158)\\
&\leq \frac{1}{2}\log(2\pi e) E\left[(X + Z_2 - \alpha Y_1)^2\right] - \frac{1}{2}\log(2\pi e N_2) && (8.159)\\
&\leq \frac{1}{2}\log\left((1-\alpha)^2 P + \alpha^2 N_1 + N_2\right) - \frac{1}{2}\log(N_2) && (8.160)
\end{aligned}
$$

where in (8.157), we used the fact that conditioning cannot increase entropy and that $H(Z_2|Z_1) = H(Z_2)$ due to the independence of Z_1 and Z_2. Equation (8.158) is again due to the fact that conditioning cannot increase entropy, (8.159) comes from the fact that Gaussian distribution maximizes entropy subject to a power constraint, and (8.160) is obtained by using the power constraint on X. Finally, we note that

(8.160) is a valid outer bound for every α and if we select α as

$$\alpha = \frac{P}{P + N_1} \tag{8.161}$$

we get (8.51), completing the proof.

8.11.4 Proof of Theorem 8.4

The transmitter uses the joint encoding scheme of Marton [11] and user 1 uses a CAF scheme [80]. User 2 employs list decoding to find which $\hat{Y}_1$ is sent. Let $A_\epsilon^n(V_1)$ and $A_\epsilon^n(V_2)$ denote the sets of strongly typical i.i.d. length-n sequences of $\mathbf{v}_1$ and $\mathbf{v}_2$, respectively. Let $A_\epsilon^n\left(V_1|\mathbf{v}_2\right)$ (resp. $A_\epsilon^n\left(V_2|\mathbf{v}_1\right)$) denote the set of length-n sequences V_1 (resp. V_2) that are jointly typical with $\mathbf{v}_2$ (resp. $\mathbf{v}_1$). Furthermore, let $S_\epsilon^n(\mathbf{v}_1)$ (resp. $S_\epsilon^n(\mathbf{v}_2)$) denote the set of $\mathbf{v}_1$ (resp. $\mathbf{v}_2$) sequences for which $A_\epsilon^n\left(V_2|\mathbf{v}_1\right)$ (resp. $A_\epsilon^n\left(V_1|\mathbf{v}_2\right)$) are non-empty. Fix the probability distribution as

$$p(v_1, v_2)p(x|v_1, v_2)p(u, x_1)p(\hat{y}_1|u, v_1, y_1) \tag{8.162}$$

Codebook generation:

1. Select $2^{nR(V_i)}$ $\mathbf{v}_i$ sequences through

$$p(\mathbf{v}_i) = \begin{cases} \frac{1}{||S_\epsilon^n(\mathbf{v}_i)||}, & \text{if } \mathbf{v}_i \in S_\epsilon^n(\mathbf{v}_i) \\ 0, & \text{otherwise} \end{cases} \tag{8.163}$$

in an i.i.d. manner and index them as $\mathbf{v}_i(w_i, \tilde{w}_i, l_i)$ where $w_i \in \left\{1, \ldots, 2^{nR_i}\right\}$,

$\tilde{w}_i \in \{1, \ldots, 2^{n\tilde{R}_i}\}$ and $l_i \in \left\{1, \ldots, 2^{nL_i}\right\}$ for $i = 1, 2$. $R_i, \tilde{R}_i, L_i$ and $R(V_i)$ are related through

$$R(V_i) = R_i + \tilde{R}_i + L_i, \qquad i = 1, 2 \tag{8.164}$$

Furthermore, we set

$$L_1 + L_2 = I(V_1; V_2) + \epsilon \tag{8.165}$$

to ensure that for given pairs $(w_1, \tilde{w}_1)$ and $(w_2, \tilde{w}_2)$, we can find a jointly typical pair $(\mathbf{v}_1(w_1, \tilde{w}_1, l_1), \mathbf{v}_2(w_2, \tilde{w}_2, l_2))$ for some l_1, l_2.

2. For each (w_1, w_2), the transmitter randomly picks $(\tilde{w}_1, \tilde{w}_2)$ and finds a pair $(\mathbf{v}_1(w_1, \tilde{w}_1, l_1),$

   $\mathbf{v}_2(w_2, \tilde{w}_2, l_2))$ that is jointly typical. Such a pair exists with high probability due to (8.165). Then, given this pair of $(\mathbf{v}_1, \mathbf{v}_2)$, the transmitter generates its channel inputs through $\prod_{i=1}^{n} p(x_i|v_{1,i}, v_{2,i})$.

3. User 1 generates 2^{nR_0} length-n sequences $\mathbf{u}$ through $p(\mathbf{u}) = \prod_{i=1}^{n} p(u_i)$ and labels them as $\mathbf{u}(s_i)$ where $s_i \in \{1, \ldots, 2^{nR_0}\}$.

4. For each $\mathbf{u}(s_i)$, user 1 generates $2^{n\hat{R}}$ length-n sequences $\hat{\mathbf{y}}_1$ through $p(\hat{\mathbf{y}}_1|\mathbf{u}) = \prod_{i=1}^{n} p(\hat{y}_{1,i}|u_i)$ and indexes them as $\hat{\mathbf{y}}_1(z_i|s_i)$ where $z_i \in \{1, \ldots, 2^{n\hat{R}}\}$.

5. For each $\mathbf{u}(s_i)$, user 1 generates $2^{nR_0'}$ length-n sequences $\mathbf{x}_1$ through $p(\mathbf{x}_1|\mathbf{u}) = \prod_{i=1}^{n} p(x_{1,i}|u_i)$ and indexes them as $\mathbf{x}_1(t_i|s_i)$ where $t_i \in \{1, \ldots, 2^{nR_0'}\}$.

Partitioning:

- Partition $2^{n\hat{R}}$ into cells S_{s_i} where $s_i \in \{1, \ldots, 2^{nR_0}\}$.

Encoding:

The transmitter sends $\mathbf{x}$ corresponding to the pair (w_1, w_2). User 1 (relay) sends $\mathbf{x}_1(t_i|s_i)$ if the estimate of $\mathbf{y}_1(i-1)$, i.e., $\hat{z}_{i-1}$, falls into S_{s_i} and t_i is chosen randomly from $\{1, \ldots, 2^{nR_0'}\}$. The use of many $\mathbf{x}_1(t_i|s_i)$ for actual help signal $\mathbf{u}(s_i)$ aims to confuse user 2 and to decrease its decoding capability.

Decoding:

a. Decoding at user 1:

1. User 1 seeks a unique typical pair of $(\mathbf{y}_1(i), \mathbf{v}_1(w_{1,i}, \tilde{w}_{1,i}, l_i), \mathbf{x}_1(t_i|s_i))$ which can be achieved with vanishingly small error probability if

$$R(V_1) \leq I(V_1; Y_1|X_1) \tag{8.166}$$

2. User 1 decides that z_i is received if there exists a jointly typical pair $(\hat{\mathbf{y}}_1(z_i|s_i), \mathbf{y}_1(i), \mathbf{v}_1(w_{1,i}, \tilde{w}_{1,i}, l_i), \mathbf{x}_1(t_i|s_i))$ which can be guaranteed to occur if

$$\hat{R} \geq I(\hat{Y}_1; Y_1|U, X_1, V_1) \tag{8.167}$$

b. Decoding at user 2:

1. User 2 seeks a unique jointly typical pair of $(\mathbf{y}_2(i), \mathbf{u}(s_i))$ which can be found

with vanishingly small error probability if

$$R_0 \leq I(U;Y_2) \tag{8.168}$$

2. User 2 employs list decoding to decode $\hat{\mathbf{y}}_1(z_{i-1}|s_{i-1})$. It first calculates its ambiguity set as

$$\mathcal{L}\left(\hat{\mathbf{y}}_1(z_{i-1}|\hat{s}_{i-1})\right) = \{\hat{\mathbf{y}}_1(z_{i-1}|\hat{s}_{i-1}) : (\hat{\mathbf{y}}_1(z_{i-1}|\hat{s}_{i-1}), \mathbf{y}_2(i-1)) \text{ is jointly typical}\} \tag{8.169}$$

and takes its intersection with $S_{\hat{s}_i}$ which results in a unique and correct intersection point if

$$\hat{R} \leq I(\hat{Y}_1;Y_2|U) + R_0 \leq I(\hat{Y}_1,U;Y_2) \tag{8.170}$$

Equations (8.167) and (8.170) lead to the compression constraint in (8.60).

3. User 2 decides that $\mathbf{v}_2(w_{2,i-1},\tilde{w}_{2,i-1},l_{2,i-1})$ is received if there exists a unique jointly typical pair $(\mathbf{v}_2(w_{2,i-1},\tilde{w}_{2,i-1},l_{2,i-1}),\mathbf{y}_2(i-1),\hat{\mathbf{y}}_1(\hat{z}_{i-1}|\hat{s}_{i-1}))$, which can be found with vanishingly small error probability if

$$R(V_2) \leq I(V_2;Y_2,\hat{Y}_1|U) \tag{8.171}$$

Equivocation computation:

We now show that $R_{e,1}$ and $R_{e,2}$ satisfying (8.55)-(8.56) and (8.57)-(8.58) are achievable with the coding scheme presented. To this end, we treat several possible

cases separately. First, assume that

$$R_1 \geq I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, U) - I(V_1; V_2) \tag{8.172}$$

$$R_2 \geq I(V_2; Y_2, \hat{Y}_1|U) - I(V_2; Y_1|V_1, X_1) - I(V_1; V_2) \tag{8.173}$$

For this case, we select the total number of codewords, i.e., $R(V_i), i = 1, 2$, as

$$R(V_1) = I(V_1; Y_1|X_1) \tag{8.174}$$

$$R(V_2) = I(V_2; Y_2, \hat{Y}_1|U) \tag{8.175}$$

With this selection, we have

$$\tilde{R}_1 + L_1 \leq I(V_1; Y_2, \hat{Y}_1|V_2, U) + I(V_1; V_2) \tag{8.176}$$

$$\tilde{R}_2 + L_2 \leq I(V_2; Y_1|V_1, X_1) + I(V_1; V_2) \tag{8.177}$$

We start with user 1's equivocation rate,

$$H(W_1|Y_2^n) \geq H(W_1|Y_2^n, V_2^n, U^n, \hat{Y}_1^n) \tag{8.178}$$

$$= H(W_1, Y_2^n, V_2^n, \hat{Y}_1^n|U^n) - H(Y_2^n, V_2^n, \hat{Y}_1^n|U^n) \tag{8.179}$$

$$= H(V_1^n, W_1, Y_2^n, V_2^n, \hat{Y}_1^n|U^n) - H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n)$$

$$- H(Y_2^n, V_2^n, \hat{Y}_1^n|U^n) \tag{8.180}$$

$$= H(V_1^n|U^n) + H(W_1, Y_2^n, V_2^n, \hat{Y}_1^n|U^n, V_1^n) - H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n)$$

$$- H(Y_2^n, V_2^n, \hat{Y}_1^n|U^n) \tag{8.181}$$

$$\geq H(V_1^n|U^n) - I(V_1^n; Y_2^n, V_2^n, \hat{Y}_1^n|U^n) - H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n) \tag{8.182}$$

where each term will be treated separately. First term is

$$H(V_1^n|U^n) = H(V_1^n) = nR(V_1) = nI(V_1; Y_1|X_1) \tag{8.183}$$

where the first equality is due to the independence of U^n and V_1^n. The second equality follows from the fact that V_1^n can take $2^{nR(V_1)}$ values with equal probability. The third equality comes from our selection in (8.174). The second term of (8.182) can be bounded as

$$I(V_1^n; Y_2^n, V_2^n, \hat{Y}_1^n|U^n) \leq nI(V_1; Y_2, V_2, \hat{Y}_1|U) + n\epsilon_n \tag{8.184}$$

using the approach devised in Lemma 3 of [64]. To bound the last term in (8.182), we assume that user 2 is trying to decode V_1^n given the side information $W_1 = w_1$. Since

V_1^n can take less than $2^{n(I(V_1;Y_2,\hat{Y}_1|U,V_2)+I(V_1;V_2))}$ values (see (8.176)) given $W_1 = w_1$, user 2 can decode V_1^n with vanishingly small error probability as long as $W_1 = w_1$ is given. Consequently, the use of Fano's lemma yields

$$H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n) \leq \epsilon_n \tag{8.185}$$

Plugging (8.183), (8.184) and (8.185) into (8.182), we get

$$H(W_1|Y_2^n) \geq nI(V_1;Y_1|X_1) - nI(V_1;Y_2,\hat{Y}_1,V_2|U) - n\epsilon_n \tag{8.186}$$

$$= nI(V_1;Y_1|X_1) - nI(V_1;Y_2,\hat{Y}_1|V_2,U) - nI(V_1;V_2) - n\epsilon_n \tag{8.187}$$

where (8.187) follows from the independence of (V_1, V_2) and U, i.e., $I(V_1;V_2|U) = I(V_1;V_2)$. Similarly, we can bound equivocation of user 2 as follows,

$$H(W_2|Y_1^n, X_1^n) \geq H(W_2|Y_1^n, X_1^n, V_1^n) \tag{8.188}$$

$$= H(W_2, Y_1^n, V_1^n|X_1^n) - H(Y_1^n, V_1^n|X_1^n) \tag{8.189}$$

$$= H(W_2, V_2^n, Y_1^n, V_1^n|X_1^n) - H(V_2^n|W_2, Y_1^n, V_1^n, X_1^n) - H(Y_1^n, V_1^n|X_1^n) \tag{8.190}$$

$$= H(V_2^n|X_1^n) + H(W_2, Y_1^n, V_1^n|X_1^n, V_2^n) - H(V_2^n|W_2, Y_1^n, V_1^n, X_1^n)$$
$$- H(Y_1^n, V_1^n|X_1^n) \tag{8.191}$$

$$\geq H(V_2^n|X_1^n) - I(V_2^n;Y_1^n, V_1^n|X_1^n) - H(V_2^n|W_2, Y_1^n, V_1^n, X_1^n) \tag{8.192}$$

where the first term is

$$H(V_2^n|X_1^n) = H(V_2^n) = nR(V_2) = nI(V_2; Y_2, \hat{Y}_1|U) \tag{8.193}$$

where the first equality is due to the independence of V_2^n and X_1^n, the second equality comes from the fact that V_2^n can take $2^{nR(V_2)}$ values with equal probability and the last equality is a consequence of our choice in (8.175). The second term of (8.192) can be bounded as

$$I(V_2^n; Y_1^n, V_1^n|X_1^n) \leq nI(V_2; Y_1, V_1|X_1) + n\epsilon_n \tag{8.194}$$

following the approach of Lemma 3 of [64]. To bound the last term of (8.192), we assume that user 1 is trying to decode V_2^n given the side information $W_2 = w_2$. Since V_2^n can take at most $2^{n(I(V_2;Y_1|V_1,X_1)+I(V_2;V_1))}$ values (see (8.177)) given $W_2 = w_2$, user 1 can decode V_2^n with vanishingly small error probability as long as this side information is available. Consequently, the use of Fano's lemma yields

$$H(V_2^n|W_2, Y_1^n, V_1^n, X_1^n) \leq \epsilon_n \tag{8.195}$$

Plugging (8.193), (8.194) and (8.195) into (8.192), we get

$$H(W_2|Y_1^n, X_1^n) \geq nI(V_2; Y_2, \hat{Y}_1|U) - nI(V_2; Y_1, V_1|X_1) - n\epsilon_n \tag{8.196}$$

$$= nI(V_2; Y_2, \hat{Y}_1|U) - nI(V_2; Y_1|V_1, X_1) - nI(V_1; V_2) - n\epsilon_n \tag{8.197}$$

where (8.197) follows from the independence of (V_1, V_2) and X_1, i.e., $I(V_1; V_2|X_1) = I(V_1; V_2)$.

We have completed the equivocation calculation for the case described by (8.172)-(8.173). The proofs of other cases involve no different arguments besides decreasing the total number codewords in (8.174)-(8.175). For example, if

$$R_1 \leq I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, U) - I(V_1; V_2) \tag{8.198}$$

then we select the total number of codewords for user 1 as

$$R(V_1) = R_1 + I(V_1; Y_2, \hat{Y}_1|V_2, U) + I(V_1; V_2) \tag{8.199}$$

which is equivalent to saying that

$$\tilde{R}_1 + L_1 = I(V_1; Y_2, \hat{Y}_1|V_2, U) + I(V_1; V_2) \tag{8.200}$$

In this case, following the steps from (8.178) to (8.182), we can bound the equivocation of user 1 as follows,

$$H(W_1|Y_2^n) \geq H(V_1^n|U^n) - I(V_1^n; Y_2^n, V_2^n, \hat{Y}_1^n|U^n) - H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n) \tag{8.201}$$

where the first term is now

$$H(V_1^n|U^n) = H(V_1^n) = nR(V_1) = n(R_1 + I(V_1; Y_2, \hat{Y}_1|V_2, U) + I(V_1; V_2)) \quad (8.202)$$

where the first equality is due to the independence of V_1^n and U^n, the second equality is due to the fact that V_1^n can take at most $2^{nR(V_1)}$ values with equal probability and the last equality is a consequence of our choice in (8.199). An upper bound on the second term was already obtained in (8.184). The third term can also be shown to decay to zero as n goes to infinity considering the case that user 2 is decoding V_1^n using side information $W_1 = w_1$. Since V_1^n can take $2^{n(I(V_1;Y_2,\hat{Y}_1|V_2,U)+I(V_1;V_2))}$ values given $W_1 = w_1$, user 2 can decode V_2^n with vanishingly small error probability as long as this side information is available. Therefore, the use of Fano's lemma implies

$$H(V_1^n|W_1, Y_2^n, V_2^n, \hat{Y}_1^n, U^n) \leq \epsilon_n \quad (8.203)$$

Plugging (8.184),(8.202), (8.203) into (8.201), we get

$$\begin{aligned} H(W_1|Y_2^n) &\geq n(R_1 + I(V_1; Y_2, \hat{Y}_1|V_2, U) + I(V_1; V_2)) - I(V_1; Y_2, V_2, \hat{Y}_1|U) \\ &\quad - n\epsilon_n \quad (8.204) \\ &= nR_1 - n\epsilon_n \quad (8.205) \end{aligned}$$

where we used the fact that U and (V_1, V_2) are independent, i.e., $I(V_1; V_2|U) = I(V_1; V_2)$. The other cases leading to different equivocation rates can be proved

similarly, hence omitted.

8.11.5 Proof of Theorem 8.5

Fix the probability distribution as

$$p(v_1, v_2)p(x|v_1, v_2)p(u_1, x_1)p(\hat{y}_1|u_1, y_1)p(u_2, x_2)p(\hat{y}_2|u_2, y_2) \tag{8.206}$$

Codebook generation:

1. Select $2^{nR(V_i)}$ $\mathbf{v}_i$ sequences through

$$p(\mathbf{v}_i) = \begin{cases} \frac{1}{||S_\epsilon^n(\mathbf{v}_i)||}, & \text{if } \mathbf{v}_i \in S_\epsilon^n(\mathbf{v}_i) \\ 0, & \text{otherwise} \end{cases} \tag{8.207}$$

in an i.i.d. manner and index them as $\mathbf{v}_i(w_i, \tilde{w}_i, l_i)$ where $w_i \in \left\{1, \ldots, 2^{nR_i}\right\}$, $\tilde{w}_i \in \{1, \ldots, 2^{n\tilde{R}_i}\}$ and $l_i \in \left\{1, \ldots, 2^{nL_i}\right\}$ for $i = 1, 2$. $R_i, \tilde{R}_i, L_i$ and $R(V_i)$ are related through

$$R(V_i) = R_i + \tilde{R}_i + L_i, \qquad i = 1, 2 \tag{8.208}$$

Furthermore, we set

$$L_1 + L_2 = I(V_1; V_2) + \epsilon \tag{8.209}$$

to ensure that for given pairs $(w_1, \tilde{w}_1)$ and $(w_2, \tilde{w}_2)$, we can find a jointly typical

pair $(\mathbf{v}_1(w_1, \tilde{w}_1, l_1), \mathbf{v}_2(w_2, \tilde{w}_2, l_2))$ for some l_1, l_2.

2. For each (w_1, w_2), the transmitter randomly picks $(\tilde{w}_1, \tilde{w}_2)$ and finds a pair $(\mathbf{v}_1(w_1, \tilde{w}_1, l_1), \mathbf{v}_2(w_2, \tilde{w}_2, l_2))$ that is jointly typical. Such a pair exists with high probability due to (8.209). Then, given this pair of $(\mathbf{v}_1, \mathbf{v}_2)$, the transmitter generates its channel inputs through $\prod_{i=1}^{n} p(x_i|v_{1,i}, v_{2,i})$.

3. User j generates $2^{nR_{0,j}}$ length-n sequences $\mathbf{u}_j$ through $p(\mathbf{u}_j) = \prod_{i=1}^{n} p(u_{j,i})$ and labels them as $\mathbf{u}_j(s_{j,i})$ where $s_{j,i} \in \{1, \ldots, 2^{nR_{0,j}}\}$ where $j = 1, 2$.

4. For each $\mathbf{u}_j(s_{j,i})$, user j generates $2^{n\hat{R}_j}$ length-n sequences $\hat{\mathbf{y}}_j$ through $p(\hat{\mathbf{y}}_j|\mathbf{u}_j)$ $= \prod_{i=1}^{n} p(\hat{y}_{j,i}|u_{j,i})$ and indexes them as $\hat{\mathbf{y}}_j(z_{j,i}|s_{j,i})$ where $z_{j,i} \in \{1, \ldots, 2^{n\hat{R}_j}\}$, $j = 1, 2$.

5. For each $\mathbf{u}_j(s_{j,i})$, user j generates $2^{nR'_{0,j}}$ length-n sequences $\mathbf{x}_j$ through $p(\mathbf{x}_j|\mathbf{u}_j)$ $= \prod_{i=1}^{n} p(x_{j,i}|u_{j,i})$ and indexes them as $\mathbf{x}_j(t_{j,i}|s_{j,i})$ where $t_{j,i} \in \{1, \ldots, 2^{nR'_{0,j}}\}$, $j = 1, 2$.

Partitioning:

- Partition $2^{n\hat{R}_j}$ into cells $S_{s_{j,i}}$ where $s_{j,i} \in \{1, \ldots, 2^{nR_{0,j}}\}$, $j = 1, 2$.

Encoding:

The transmitter sends $\mathbf{x}$ corresponding to the pair (w_1, w_2). User j sends $\mathbf{x}_j(t_{j,i}|s_{j,i})$ if the estimate of $\mathbf{y}_j(i-1)$, i.e., $\hat{z}_{j,i-1}$, falls into $S_{s_{j,i}}$ and $t_{j,i}$ is chosen randomly from $\{1, \ldots, 2^{nR'_{0,j}}\}$. The use of many $\mathbf{x}_j(t_{j,i}|s_{j,i})$ for actual help signal $\mathbf{u}_j(s_{j,i})$ aims to confuse the other user and to decrease its decoding capability.

Decoding:

We only consider decoding at user 1. Final expressions regarding user 2 will follow due to symmetry.

1. User 1 seeks a unique jointly typical pair of $(\mathbf{y}_1(i), \mathbf{u}_2(s_{2,i}))$ which can be found with vanishingly small error probability if

$$R_{0,2} \leq I(U_2; Y_1|X_1) \tag{8.210}$$

2. User 1 decides on $\hat{\mathbf{y}}_1(z_{1,i}|s_{1,i})$ by looking for a jointly typical pair $(\hat{\mathbf{y}}_1(z_{1,i}|s_{1,i}), \mathbf{y}_1(i), \mathbf{u}_2(s_{2,i}), \mathbf{x}_1(t_{1,i}|s_{1,i}))$ which can be ensured to exist if

$$\hat{R}_1 \geq I(\hat{Y}_1; Y_1|U_1, U_2, X_1) \tag{8.211}$$

3. User 1 employs list decoding to decode $\hat{\mathbf{y}}_2(z_{2,i-1}|s_{2,i-1})$. It first calculates its ambiguity set as

$$\begin{aligned}&\mathcal{L}\left(\hat{\mathbf{y}}_2(z_{2,i-1}|\hat{s}_{2,i-1})\right)\\ &= \{\hat{\mathbf{y}}_2(z_{2,i-1}|\hat{s}_{2,i-1}) : (\hat{\mathbf{y}}_2(z_{2,i-1}|\hat{s}_{2,i-1}), \mathbf{y}_1(i-1)) \text{ is jointly typical}\}\end{aligned} \tag{8.212}$$

and then takes its intersection with $S_{\hat{s}_{2,i}}$ which results in a unique and correct intersection point if

$$\hat{R}_2 \leq I(\hat{Y}_2; Y_1|U_2, X_1) + R_{0,2} \leq I(\hat{Y}_2, U_2; Y_1|X_1) \tag{8.213}$$

4. User 1 decides that $\mathbf{v}_1(w_{1,i-1}, \tilde{w}_{1,i-1}, l_{1,i-1})$ is received if there exists a unique jointly typical pair $(\mathbf{v}_1(w_{1,i-1}, \tilde{w}_{1,i-1}, l_{1,i-1}), \mathbf{y}_1(i-1), \hat{\mathbf{y}}_2(\hat{z}_{2,i-1}|\hat{s}_{2,i-1}))$ which can be found with vanishingly small error probability if

$$R(V_1) \leq I(V_1; Y_1, \hat{Y}_2|X_1, U_2) \tag{8.214}$$

Equivocation computation:

Similar to the previous proofs, we treat each case separately. Due to symmetry, we only consider user 1. If the rate of user 1 is such that

$$R_1 \geq I(V_1; Y_1, \hat{Y}_2|X_1, U_2) - I(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1) - I(V_1; V_2) \tag{8.215}$$

then we select the total number of codewords as

$$R(V_1) = I(V_1; Y_1, \hat{Y}_2|X_1, U_2) \tag{8.216}$$

which implies that

$$\tilde{R}_1 + L_1 \leq I(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1) + I(V_1; V_2) \tag{8.217}$$

The equivocation rate can be bounded as follows,

$$H(W_1|Y_2^n, X_2^n) \geq H(W_1|Y_2^n, X_2^n, \hat{Y}_1^n, V_2^n, U_1^n) \tag{8.218}$$

$$= H(W_1, Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n) - H(Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n) \tag{8.219}$$

$$= H(W_1, V_1^n, Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n) - H(V_1^n|W_1, Y_2^n, \hat{Y}_1^n, V_2^n, X_2^n, U_1^n)$$
$$- H(Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n) \tag{8.220}$$

$$= H(V_1^n|X_2^n, U_1^n) + H(W_1, Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n, V_1^n)$$
$$- H(V_1^n|W_1, Y_2^n, \hat{Y}_1^n, V_2^n, X_2^n, U_1^n) - H(Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n) \tag{8.221}$$

$$\geq H(V_1^n|X_2^n, U_1^n) - I(V_1^n; Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n)$$
$$- H(V_1^n|W_1, Y_2^n, \hat{Y}_1^n, V_2^n, X_2^n, U_1^n) \tag{8.222}$$

We treat each term in (8.222) separately. The first term is

$$H(V_1^n|X_2^n, U_1^n) = H(V_1^n) = nR(V_1) = nI(V_1; Y_1, \hat{Y}_2|X_1, U_2) \tag{8.223}$$

where the first equality is due to the independence of V_1^n and (X_2^n, U_1^n), the second equality follows from the fact that V_1^n can take $2^{nR(V_1)}$ values with equal probability and the last equality is due to our choice in (8.216). The second term of (8.222) can be bounded as

$$I(V_1^n; Y_2^n, \hat{Y}_1^n, V_2^n|X_2^n, U_1^n) \leq nI(V_1; Y_2, \hat{Y}_1, V_2|X_2, U_1) + n\epsilon_n \tag{8.224}$$

following Lemma 3 of [64]. To bound the last term of (8.222), we consider the case

that user 2 is trying to decode V_1^n given the side information $W_1 = w_1$. Since V_1^n can take $2^{n(I(V_1;Y_2,\hat{Y}_1|X_2,V_2,U_1)+I(V_1;V_2))}$ values at most, user 2 can decode V_1^n with vanishingly small error probability as long as this side information is available. Hence, the use of Fano's lemma yields

$$H(V_1^n|W_1, Y_2^n, \hat{Y}_1^n, V_2^n, X_2^n, U_1^n) \leq \epsilon_n \tag{8.225}$$

Plugging (8.223), (8.224), (8.225) into (8.222), we get

$$H(W_1|Y_2^n, X_2^n) \geq nI(V_1; Y_1, \hat{Y}_2|X_1, U_2) - nI(V_1; Y_2, \hat{Y}_1, V_2|X_2, U_1) - n\epsilon_n \tag{8.226}$$

$$= nI(V_1; Y_1, \hat{Y}_2|X_1, U_2) - nI(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1) - nI(V_1; V_2) - n\epsilon_n \tag{8.227}$$

where (8.227) follows from the independence of (X_2, U_1) and (V_1, V_2).

For the other case, i.e., if the rate of user 1 is such that

$$R_1 \leq I(V_1; Y_1, \hat{Y}_2|X_1, U_2) - I(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1) - I(V_1; V_2) \tag{8.228}$$

we select the total number of codewords as

$$R(V_1) = R_1 + I(V_1; Y_2, \hat{Y}_1|X_2, V_2, U_1) + I(V_1; V_2) \tag{8.229}$$

and following the same lines of computation, we can show that

$$H(W_1|Y_2^n, X_2^n) \geq nR_1 - n\epsilon_n \tag{8.230}$$

completing the proof.

Chapter 9

Cooperative Secrecy in Multiple Access Channels with Generalized Feedback

9.1 Introduction

In this chapter, we consider the effects of user cooperation on the simultaneous secrecy of multiple users against each other, in a multiple access channel with generalized feedback (MAC-GF), where users can cooperate via the feedback signals (see Figure 9.1). Similar to the CRBC, in the MAC-GF also, users cooperate, although, they do not trust each other and consider each other as an eavesdropper. Our goal is to understand how cooperation and secrecy interact within this channel model.

We note that MAC-GF has been studied from a secrecy perspective in [86, 87], however, our work differs significantly from these previous works. In [86, 87] feedback signals, which are available at the transmitters, are not used in the encoding functions, i.e., the users are not allowed to cooperate. In this work, we allow users to utilize their overheard information in their encoding functions, and study the effects of this cooperation on secrecy.

In this chapter, we present two achievable schemes which are based on the CAF strategy [80]. CAF has been used before in the context of increasing rates

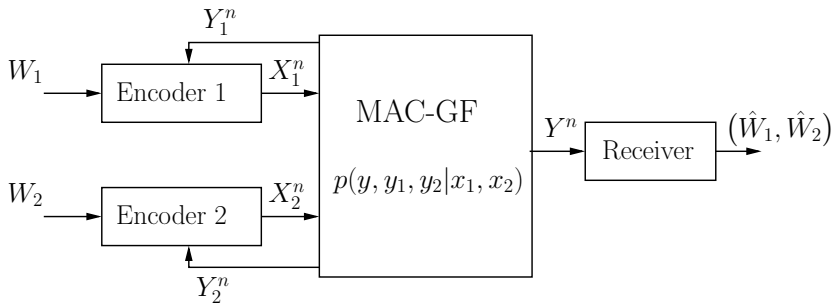

Figure 9.1: The MAC-GF channel model.

in MAC-GF [88, 89]; here we use CAF to provide secrecy to cooperating users, and determine achievable equivocation rates. We also present outer bounds on the achievable equivocation rates. The outer bounds we derive depend only on the channel inputs and outputs, and hence are easily computable. Finally, we present numerical results for Gaussian MAC-GF.

9.2 Channel Model and Definitions

The two-user MAC-GF (see Figure 9.1) consists of two input alphabets $\mathcal{X}_1, \mathcal{X}_2$ and three output alphabets $\mathcal{Y}, \mathcal{Y}_1, \mathcal{Y}_2$. The channel is memoryless and is characterized by $p(y, y_1, y_2|x_1, x_2)$.

A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two message sets $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}, \mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, two encoder functions

$$x_{1,i} = f_1\left(w_1, y_{1,1}, \ldots, y_{1,i-1}\right), \qquad i = 1, \ldots, n$$

$$x_{2,i} = f_2\left(w_2, y_{2,1}, \ldots, y_{2,i-1}\right), \qquad i = 1, \ldots, n$$

and a decoder function $g : \mathcal{Y} \to \mathcal{W}_1 \times \mathcal{W}_2$. The probability of error is defined as

$P_e^n = \Pr\left(g(Y^n) \neq (W_1, W_2)\right)$.

The secrecy of each user is measured by the normalized entropy of its message conditioned on the random variables available at the other user, the other user's observation, channel input and message, i.e.,

$$\frac{1}{n}H(W_1|Y_2^n, X_2^n, W_2) \quad \text{and} \quad \frac{1}{n}H(W_2|Y_1^n, X_1^n, W_1)$$

which will hereafter be called equivocation rates. A rate tuple $(R_1, R_2, R_{e,1}, R_{e,2})$ is said to be achievable if there exists a $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n}H(W_1|Y_2^n, X_2^n, W_2) \geq R_{e,1} \tag{9.1}$$

$$\lim_{n\to\infty} \frac{1}{n}H(W_2|Y_1^n, X_1^n, W_1) \geq R_{e,2} \tag{9.2}$$

Remark 9.1 *We note that our coding scheme is different than those in previous works [86, 87], which also considered secrecy in MAC-GF. In [86, 87], the encoding functions are restricted to be of the form*

$$f_i : \mathcal{W}_i \to \mathcal{X}_i^n, \qquad i = 1, 2$$

i.e., the feedback signals that are available at the transmitters are not utilized in the encoding functions.

9.3 Achievable Schemes

We present our first achievable scheme in the following theorem. In this achievable scheme, even though both users receive feedback signals in the MAC-GF, only one of them, user 1, utilizes the feedback signal in its encoding function and sends a compressed version of its observation to the main receiver. This achievable scheme is based on CAF strategy [80].

Theorem 9.1 *Rate tuples* $(R_1, R_2, R_{e,1}, R_{e,2})$ *satisfying*

$$R_1 \leq I(X_1; Y, \hat{Y}_1 | U, X_2) \tag{9.3}$$

$$R_2 \leq I(X_2; Y, \hat{Y}_1 | U, X_1) \tag{9.4}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, \hat{Y}_1 | U) \tag{9.5}$$

$$R_{e,1} \leq \min\left\{R_1' - I(X_1; Y_2, \hat{Y}_1 | U, X_2), R_1\right\} \tag{9.6}$$

$$R_{e,2} \leq \min\left\{R_2' - I(X_2; Y_1 | U, X_1), R_2\right\} \tag{9.7}$$

where the pairs (R_1', R_2') *belong to*

$$\mathcal{C}_1(R_1, R_2) = \left\{ \begin{array}{rcl} R_1 & \leq & R_1' \\ R_2 & \leq & R_2' \\ R_1' & \leq & I(X_1; Y, \hat{Y}_1 | U, X_2) \\ R_2' & \leq & I(X_2; Y, \hat{Y}_1 | U, X_1) \\ R_1' + R_2' & \leq & I(X_1, X_2; Y, \hat{Y}_1 | U) \end{array} \right\} \tag{9.8}$$

are achievable for any distribution of the form

$$p(u)p(x_1|u)p(\hat{y}_1|u,x_1,y_1)p(x_2)p(y,y_1,y_2|x_1,x_2) \tag{9.9}$$

subject to the constraint

$$I(\hat{Y}_1;Y_1|U,X_1) \leq I(U,\hat{Y}_1;Y) \tag{9.10}$$

The achievable scheme in Theorem 9.1 corresponds to a special case of the achievable scheme given in Theorem 9.2.

Remark 9.2 *The achievable region given in Theorem 9.1 can be enlarged by using the channel prefixing technique introduced in [3]. In Theorem 9.1, we did not use channel prefixing for the clarity of presentation. If we want to use it, we need to replace all occurrences of X_1 (resp. X_2) with V_1 (resp. V_2), and change the joint distribution in (9.9) to $p(u)p(v_1|u)p(x_1|v_1)p(\hat{y}_1|u,v_1,y_1)p(v_2)p(x_2|v_2)\ p(y,y_1,y_2|x_1,x_2)$.*

Remark 9.3 *In (9.9), we condition $\hat{Y}_1$ on X_1 because user 1's feedback signal can be correlated with X_1. The conditioning on X_1 in (9.10) is for the same reason as well. By these conditionings, we implicitly assume that, if the feedback signal of user 1 has a self-interference term, user 1 cancels it out. If user 1 does not want to cancel it out hoping that this may increase the achievable region, then the pdf in (9.9) and the constraint in (9.10) should be replaced with $p(\hat{y}_1|u,y_1)$ and $I(\hat{Y}_1;Y_1|U) \leq I(U,\hat{Y}_1;Y)$, respectively. Both choices are optional, and neither of them provides an achievable region that includes the one provided by the other. For a similar discussion, please*

see Remark 2 of [83].

Remark 9.4 *If we disable user cooperation via setting $U = \hat{Y}_1 = \phi$, the achievable rate region for the pairs (R_1, R_2) reduce to the capacity region of the MAC [22].*

Remark 9.5 *If we set $U = X_1 = \hat{Y}_1 = Y_2 = \phi$, then the channel becomes a wire-tap channel, and the achievable rate region reduces to*

$$R_2 \leq I(X_2; Y) \tag{9.11}$$

$$R_{e,2} \leq \min\{I(X_2; Y) - I(X_2; Y_1), R_2\} \tag{9.12}$$

which, after channel prefixing, becomes the same as the one in [3].

Remark 9.6 *If we disable the assistance of user 1 by setting $U = \hat{Y}_1 = \phi$, then we have the following achievable region*

$$R_1 \leq I(X_1; Y|X_2) \tag{9.13}$$

$$R_2 \leq I(X_2; Y|X_1) \tag{9.14}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y) \tag{9.15}$$

$$R_{e,1} \leq \min\{R_1' - I(X_1; Y_2|X_2), R_1\} \tag{9.16}$$

$$R_{e,2} \leq \min\{R_2' - I(X_2; Y_1|X_1), R_2\} \tag{9.17}$$

where the pairs (R_1', R_2') *belong to*

$$\left\{ \begin{array}{rcl} R_1 & \leq & R_1' \\ R_2 & \leq & R_2' \\ R_1' & \leq & I(X_1; Y|X_2) \\ R_2' & \leq & I(X_2; Y|X_1) \\ R_1' + R_2' & \leq & I(X_1, X_2; Y) \end{array} \right\} \tag{9.18}$$

for any distribution of the form

$$p(x_1)p(x_2)p(y, y_1, y_2|x_1, x_2) \tag{9.19}$$

which, after channel prefixing, becomes the same as the one in [86], where feedback signals are not utilized in the encoding functions.

Remark 9.7 *If we disable the confidential messages of user 1 by setting* $U = X_1$*, the channel model becomes a relay channel with secrecy constraints, and the achievable region reduces to*

$$R_2 \leq I(X_2; Y, \hat{Y}_1|X_1) \tag{9.20}$$

$$R_{e,2} \leq \min\left\{ I(X_2; Y, \hat{Y}_1|X_1) - I(X_2; Y_1|X_1), R_2 \right\} \tag{9.21}$$

for any distribution

$$p(x_1)p(\hat{y}_1|x_1, y_1)p(x_2)p(y, y_1, y_2|x_1, x_2) \tag{9.22}$$

subject to the constraint

$$I(\hat{Y}_1; Y_1|X_1) \leq I(X_1, \hat{Y}_1; Y) \tag{9.23}$$

which was proposed in [74].

We state our second achievable scheme in the following theorem. In this achievable scheme, both users utilize the feedback signals they receive in their encoding functions, and send compressed versions of their observations to the main receiver.

Theorem 9.2 *Rate tuples* $(R_1, R_2, R_{e,1}, R_{e,2})$ *satisfying*

$$R_1 \leq I(X_1; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2, X_2) \tag{9.24}$$

$$R_2 \leq I(X_2; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2, X_1) \tag{9.25}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2) \tag{9.26}$$

$$R_{e,1} \leq \min\left\{R_1' - I(X_1; Y_2, \hat{Y}_1|U_1, U_2, X_2), R_1\right\} \tag{9.27}$$

$$R_{e,2} \leq \min\left\{R_2' - I(X_2; Y_1, \hat{Y}_2|U_1, U_2, X_1), R_2\right\} \tag{9.28}$$

where the pairs (R_1', R_2') *belong to*

$$\mathcal{C}_2\left(R_1, R_2\right) = \left\{ \begin{array}{rcl} R_1 & \leq & R_1' \\ R_2 & \leq & R_2' \\ R_1' & \leq & I(X_1; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2, X_2) \\ R_2' & \leq & I(X_2; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2, X_1) \\ R_1' + R_2' & \leq & I(X_1, X_2; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2) \end{array} \right\} \tag{9.29}$$

are achievable for any distribution of the form

$$p(u_1)p(x_1|u_1)p(\hat{y}_1|u_1,x_1,y_1)p(u_2)p(x_2|u_2)p(\hat{y}_2|u_2,x_2,y_2)p(y,y_1,y_2|x_1,x_2) \tag{9.30}$$

subject to the constraints

$$I(\hat{Y}_1;Y_1|U_1,X_1) \leq I(U_1,\hat{Y}_1;Y|U_2) \tag{9.31}$$

$$I(\hat{Y}_2;Y_2|U_2,X_2) \leq I(U_2,\hat{Y}_2;Y|U_1) \tag{9.32}$$

$$\begin{aligned} I(\hat{Y}_1;Y_1|U_1,X_1)+I(\hat{Y}_2;Y_2|U_2,X_2) \leq{}& I(U_1,U_2;Y)+I(\hat{Y}_1;Y|U_1,U_2) \\ &+ I(\hat{Y}_2;Y|U_1,U_2) \end{aligned} \tag{9.33}$$

The proof of Theorem 9.2 is given in Appendix 9.7.1.

Remark 9.8 *Remarks 9.2 and 9.3 apply to Theorem 9.2, as well. As in Remark 9.3, if users do not want to cancel their own signals out from their observations while compressing, the conditioning of $\hat{Y}_1$ (resp. $\hat{Y}_2$) on X_1 (resp. X_2) and conditionings on the left hand sides of inequalities (9.31), (9.32), (9.33) on X_1, X_2 should be removed.*

Remark 9.9 *In Theorem 9.2, the receiver jointly decodes U_1, U_2 which, as seen in (9.33), results in a sum constraint on the qualities of the observations sent to the receiver.*

Remark 9.10 *If we set $U_2 = \hat{Y}_2 = \phi$ in Theorem 9.2, we recover Theorem 9.1.*

9.4 Outer Bound

We now present an outer bound on the equivocation rates. This outer bound depends only on the channel inputs and outputs, and hence is computable.

Theorem 9.3 *The equivocation rate pairs* $(R_{e,1}, R_{e,2})$ *are contained in the union of*

$$R_{e,1} \leq I(X_1, Y_1; Y|X_2, Y_2) \tag{9.34}$$

$$R_{e,2} \leq I(X_2, Y_2; Y|X_1, Y_1) \tag{9.35}$$

where the union is over all $p(x_1, x_2)$.

This bound is obtained by considering the best possible scenario for each user, e.g., the bound for user 1 assumes that user 2's observation is made available to the main receiver. The proof of Theorem 9.3 is given in Appendix 9.7.2.

9.5 Gaussian Channels

A Gaussian MAC-GF may be described by [86]:

$$Y_{1,i} = X_{1,i} + X_{2,i} + Z_{1,i} \tag{9.36}$$

$$Y_{2,i} = X_{1,i} + X_{2,i} + Z_{2,i} \tag{9.37}$$

$$Y_i = X_{1,i} + X_{2,i} + Z_i \tag{9.38}$$

where $Z_{1,i} \sim \mathcal{N}(0, N_1), Z_{2,i} \sim \mathcal{N}(0, N_2), Z_i \sim \mathcal{N}(0, N)$ and are all i.i.d. In addition, we have the following power constraints

$$\frac{1}{n}\sum_{i=1}^{n} E[X_{1,i}^2] \leq P_1 \tag{9.39}$$

$$\frac{1}{n}\sum_{i=1}^{n} E[X_{2,i}^2] \leq P_2 \tag{9.40}$$

In Section 9.5.1, we present results on degraded channels. This section is designed to identify cases where the use of feedback signals in the encoding, i.e., cooperation, is needed for positive secrecy rates. In Section 9.5.2, we present achievable regions for Gaussian channels with some particular selections for random variables involved in Theorems 9.1, 9.2.

9.5.1 Degraded Channels and Implications

We first note that, for a given channel $p(y, y_1, y_2|x_1, x_2)$, depending on whether the feedback signals are used in the encoding or not, we obtain different n-letter joint distributions $p(w_1, w_2, x_1^n, x_2^n, y_1^n, y_2^n, y^n)$, and observe different characteristics. In this section, we focus on MAC-GFs where the feedback signals are not used in the encoding functions, e.g., [86, 87]. For such channels, we have the following outer bound.

Theorem 9.4 *The equivocation rate pairs $(R_{e,1}, R_{e,2})$ of MAC-GFs where feedback*

signals are not used in the encoding functions, are contained in the union of

$$R_{e,1} \leq I(X_1; Y|X_2, Y_2) \tag{9.41}$$

$$R_{e,2} \leq I(X_2; Y|X_1, Y_1) \tag{9.42}$$

where the union is over all $p(x_1, x_2) = p(x_1)p(x_2)$.

The proof of this theorem is similar to the proof of Theorem 9.3, and hence, is omitted. Motivated with this outer bound, we define degradedness.

Definition 9.1 *If the channel satisfies the Markov chain* $X_1 \rightarrow (X_2, Y_2) \rightarrow Y$ *(resp.* $X_2 \rightarrow (X_1, Y_1) \rightarrow Y$*), then it is said to be type-I (resp. type-II) degraded.*

Theorem 9.4 together with Definition 9.1 implies the following.

Corollary 9.1 *If the channel is type-I (resp. type-II) degraded, then we have* $R_{e,1} = 0$ *(resp.* $R_{e,2} = 0$*).*

Corollary 9.1 can be specialized to degraded Gaussian channels.

Corollary 9.2 *For Gaussian channels with* $Z = Z_1 + Z'$ *(resp.* $Z = Z_2 + Z'$*), we have* $R_{e,2} = 0$ *(resp.* $R_{e,1} = 0$*) where* $Z' \sim \mathcal{N}(0, N')$ *and independent of* Z_1, Z_2.

The following lemma is from [86].

Lemma 9.1 *All channels having the same marginal distributions*

$$p(y_1|x_1, x_2), p(y_2|x_1, x_2), p(y|x_1, x_2) \tag{9.43}$$

as the original channel have the same capacity-equivocation regions.

We are now ready to consider the broader class of stochastically degraded channels.

Definition 9.2 *A channel is said to be stochastically type-I degraded, if its conditional marginal distribution $p(y|x_1, x_2)$ is the same as that of a type-I degraded channel, i.e., there exists a distribution $p'(y|y_2, x_2)$ which satisfies*

$$p(y|x_1, x_2) = \sum_{y_2} p(y_2|x_1, x_2)p'(y|y_2, x_2) \tag{9.44}$$

Stochastically type-II degradedness is defined similarly.

Using Lemma 9.1, we have the following corollary.

Corollary 9.3 *If a channel is stochastically type-I (resp. type-II) degraded, then we have $R_{e,1} = 0$ (resp. $R_{e,2} = 0$).*

In Gaussian MAC-GFs, stochastically degradedness is characterized by receiver noise variances, as stated next.

Corollary 9.4 *For Gaussian channels, if $N_1 < N$ (resp. $N_2 < N$), then $R_{e,2} = 0$ (resp. $R_{e,1} = 0$).*

This corollary follows from Lemma 9.1 and Theorem 9.4.

To sum up, in this section we showed that, for Gaussian MAC-GF, if the feedback signals are not utilized in the encoding functions and if $N_1 < N$ (resp. $N_2 < N$), then $R_{e,1} = 0$ (resp. $R_{e,2} = 0$). However, if the feedback signals are utilized in the encoding functions, then we may have positive secrecy rates for both users as will be shown next.

9.5.2 Achievable Schemes for Gaussian Channels

We now provide achievable regions for Gaussian MAC-GF. The following propositions characterize achievable regions using Theorems 9.1, 9.2 with certain selections for the involved random variables. We define $\mathrm{C}(x) = \frac{1}{2}\log(1+x)$.

Proposition 9.1 *For any $\bar{\alpha} = 1-\alpha \in [0,1]$, rate tuples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying*

$$R_1 \leq R_1' \leq C\left(\bar{\alpha}\frac{P_1}{N}\right) \tag{9.45}$$

$$R_2 \leq R_2' \leq C\left(P_2\frac{N+N_1+N_c}{N\left(N_1+N_c\right)}\right) \tag{9.46}$$

$$R_1' + R_2' \leq C\left(\bar{\alpha}\frac{P_1}{N} + P_2\frac{N+N_1+N_c}{N\left(N_1+N_c\right)} + \frac{\bar{\alpha}P_1P_2}{N(N_1+N_c)}\right) \tag{9.47}$$

$$R_{e,1} \leq \min\left\{R_1' - C\left(\bar{\alpha}\frac{P_1}{N_2}\right), R_1\right\} \tag{9.48}$$

$$R_{e,2} \leq \min\left\{R_2' - C\left(\frac{P_2}{N_1}\right), R_2\right\} \tag{9.49}$$

are achievable, subject to the constraint

$$N_c \geq \frac{-\beta + \sqrt{\beta^2 + 4\theta\gamma}}{2\theta} \tag{9.50}$$

where

$$\theta = \alpha P_1$$

$$\beta = P_2\left[(2\alpha-1)P_1 - N - N_1\right] - N_1\left[(1-2\alpha)P_1 + N\right]$$

$$\gamma = \left(P_2+N_1\right)\left[N_1\left(\bar{\alpha}P_1 + P_2 + N\right) + P_2\left(\bar{\alpha}P_1 + N\right)\right]$$

Proof: This region is obtained via direct calculation of the rates in Theorem 9.1 with the following selection of the random variables: $X_2 \sim \mathcal{N}(0, P_2), U \sim \mathcal{N}(0, \alpha P_1)$, $U' \sim \mathcal{N}(0, \bar{\alpha} P_1)$ and $X_1 = U + U'$. $\hat{Y}_1 = Y_1 - X_1 + Z_c = X_2 + Z_1 + Z_c$ where Z_c is the compression noise with distribution $Z_c \sim \mathcal{N}(0, N_c)$. X_2, U', Z_c are all independent. $\square$

Proposition 9.2 *For any* $\left(\bar{\alpha} = 1 - \alpha, \bar{\beta} = 1 - \beta\right) \in [0,1] \times [0,1]$, *rate tuples* $(R_1, R_2, R_{e,1}, R_{e,2})$ *satisfying*

$$R_1 \leq R_1' \leq C\left(\bar{\alpha} P_1 \frac{N + N_2 + N_{c,2}}{N\left(N_2 + N_{c,2}\right)}\right) \tag{9.51}$$

$$R_2 \leq R_2' \leq C\left(\bar{\beta} P_2 \frac{N + N_1 + N_{c,1}}{N(N_1 + N_{c,1})}\right) \tag{9.52}$$

$$\begin{aligned} R_1' + R_2' \leq C\Bigg(&\bar{\alpha} P_1 \frac{N + N_2 + N_{c,2}}{N(N_2 + N_{c,2})} + \bar{\beta} P_2 \frac{N + N_1 + N_{c,1}}{N(N_1 + N_{c,1})} \\ &+ \bar{\alpha}\bar{\beta} P_1 P_2 \frac{N + N_1 + N_{c,1} + N_2 + N_{c,2}}{N(N_1 + N_{c,1})(N_2 + N_{c,2})}\Bigg) \end{aligned} \tag{9.53}$$

$$R_{e,1} \leq \min\left\{R_1' - C\left(\bar{\alpha}\frac{P_1}{N_2}\right), R_1\right\} \tag{9.54}$$

$$R_{e,2} \leq \min\left\{R_2' - C\left(\bar{\beta}\frac{P_2}{N_1}\right), R_2\right\} \tag{9.55}$$

are achievable, subject to the constraints

$$\frac{-\beta_1 + \sqrt{\beta_1^2 + 4\theta_1\gamma_1}}{2\theta_1} \leq N_{c,1} \tag{9.56}$$

$$\frac{-\beta_2 + \sqrt{\beta_2^2 + 4\theta_2\gamma_2}}{2\theta_2} \leq N_{c,2} \tag{9.57}$$

$$\left(1 + \frac{P_2 + N_1}{N_{c,1}}\right)\left(1 + \frac{P_1 + N_2}{N_{c,2}}\right) \leq (1 + \omega_1)(1 + \omega_2)\left(1 + \frac{\alpha P_1 + \beta P_2}{\bar{\alpha} P_1 + \bar{\beta} P_2 + N}\right) \tag{9.58}$$

where

$$\theta_1 = \alpha P_1$$

$$\theta_2 = \beta P_2$$

$$\beta_1 = \alpha P_1(\bar{\beta}P_2 + N_1) + (\bar{\beta}P_2)^2 - (P_2 + N_1)(\bar{\beta}P_2 + \bar{\alpha}P_1 + N)$$

$$\beta_2 = \beta P_2(\bar{\alpha}P_1 + N_2) + (\bar{\alpha}P_1)^2 - (P_1 + N_2)(\bar{\alpha}P_1 + \bar{\beta}P_2 + N)$$

$$\gamma_1 = (P_2 + N_1)\left((\bar{\alpha}P_1 + N)(\bar{\beta}P_2 + N_1) + \bar{\beta}P_2N_1\right)$$

$$\gamma_2 = (P_1 + N_2)\left((\bar{\beta}P_2 + N)(\bar{\alpha}P_1 + N_2) + \bar{\alpha}P_1N_2\right)$$

$$\omega_1 = \frac{(\bar{\alpha}P_1)^2}{\bar{\alpha}P_1(\bar{\beta}P_2 + N + N_2 + N_{c,2}) + (\bar{\beta}P_2 + N)(N_2 + N_{c,2})}$$

$$\omega_2 = \frac{\left(\bar{\beta}P_2\right)^2}{\bar{\beta}P_2(\bar{\alpha}P_1 + N + N_1 + N_{c,1}) + (\bar{\alpha}P_1 + N)(N_1 + N_{c,1})}$$

Proof: This region is obtained via direct calculation of the rates in Theorem 9.2 with the following selection of the random variables: $X_2 = U_2 + U_2'$ where $U_2 \sim \mathcal{N}(0, \beta P_2), U_2' \sim \mathcal{N}(0, \bar{\beta}P_2)$; $X_1 = U_1 + U_1'$ where $U_1 \sim \mathcal{N}(0, \alpha P_1)$, $U_1' \sim \mathcal{N}(0, \bar{\alpha}P_1)$; $\hat{Y}_1 = Y_1 - X_1 + Z_{c,1} = X_2 + Z_1 + Z_{c,1}$ where $Z_{c,1}$ is the compression noise with distribution $Z_{c,1} \sim \mathcal{N}(0, N_{c,1})$ $\hat{Y}_2 = Y_2 - X_2 + Z_{c,2} = X_1 + Z_2 + Z_{c,2}$ where $Z_{c,2}$ is the compression noise with distribution $Z_{c,2} \sim \mathcal{N}(0, N_{c,2})$; and $U_1, U_1', U_2, U_2', Z_{c,1}, Z_{c,2}$ are all independent. $\square$

Graphical illustrations of Propositions 9.1, 9.2 are given in Figures 9.2, 9.3, 9.4. In all these figures, we use $P_1 = P_2 = 50$. In Figure 9.2, equivocation regions are plotted for $N_1 = 0.75, N_2 = 1.25, N = 1$. Since $N_1 < N$, if cooperation is not allowed for this channel, we have $R_{e,2} = 0$. Due to user cooperation, we have a

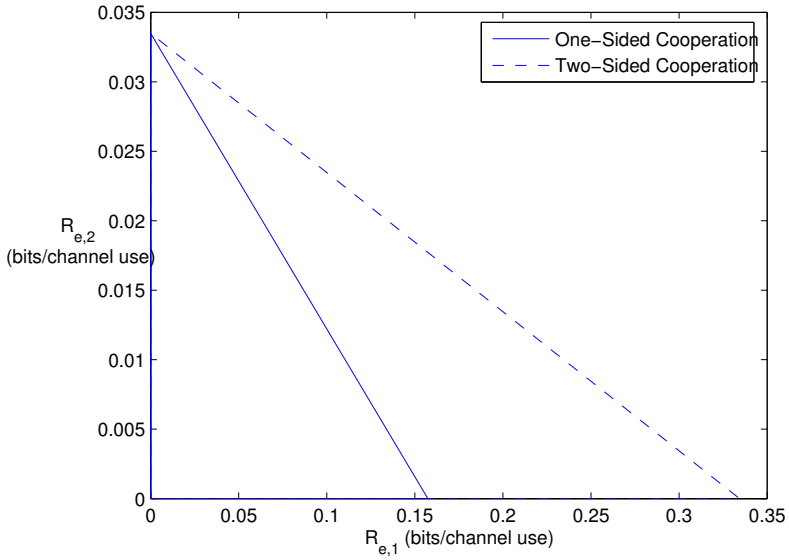

Figure 9.2: The equivocation regions given in Propositions 9.1,9.2.

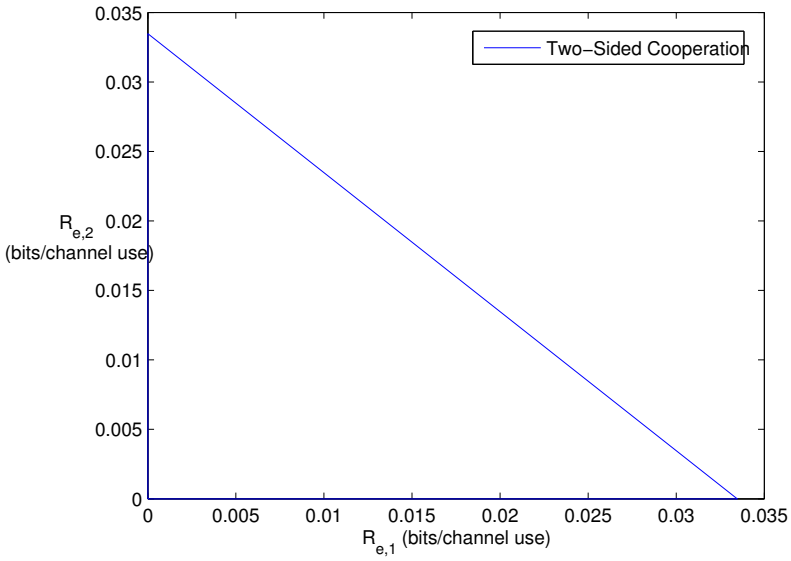

Figure 9.3: The equivocation region given in Proposition 9.2.

positive secrecy rate for user 2. If Proposition 9.1 (i.e., one-sided cooperation) is used, then we provide a positive secrecy rate for user 2 at the expense of the secrecy of user 1. However, if Proposition 9.2 (i.e., two-sided cooperation) is used, then user 2 can have positive secrecy without any cost, i.e., without any decrease in the secrecy of user 1. For both propositions, maximum secrecy rate for user 2 is achieved if user 1 does not transmit any confidential messages and acts as a relay for user 2. In Proposition 9.1, the maximum secrecy for user 1 is achieved when user 1 does not help user 2, and in Proposition 9.2, the maximum secrecy for user 1 is achieved when user 2 does not transmit any confidential messages and acts as a relay for user 1.

Secondly, we consider a case where neither user can achieve positive secrecy rates without cooperation, i.e., $N_1 < N, N_2 < N$. We select the parameters as $N_1 = 0.75, N_2 = 0.75, N = 1$. As we see in Figure 9.3, both users are able to have positive secrecy rates through cooperation. Again, in this case as well, the maximum secrecy rate for each user is obtained when the other user acts as a pure relay.

Finally, we consider a system with $N_1 = 1.25, N_2 = 1.25, N = 1$, where we can have positive secrecy rates for both users without cooperation. We observe from Figure 9.4 that user cooperation increases the achievable secrecy rates.

9.6 Conclusions

In this chapter, we consider MAC-GF to study the effects of cooperation on secrecy. In particular, we provide an achievable secrecy rate region by using a CAF-scheme

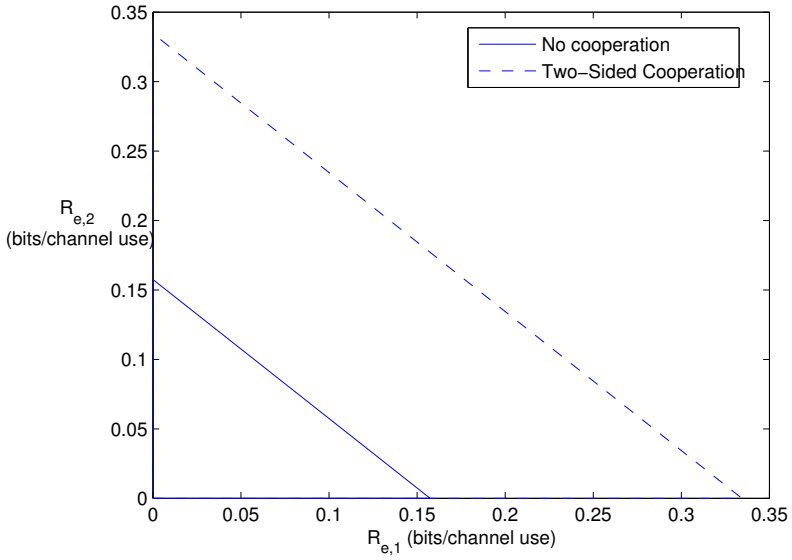

Figure 9.4: Comparison of equivocation regions with and without cooperation.

and evaluate this achievable scheme for some Gaussian channels. Through numerical illustrations, we show that, thanks to cooperation, both users can have secure communication with the receiver, although this is not possible if users are not allowed to cooperate. Hence, similar to the broadcast setting we study in the previous chapter, for the multiple access setting also, there is a synergy between user cooperation and secrecy in the sense that user cooperation can improve secrecy. We finally note that this synergy can be created only by using an appropriate cooperation strategy.

9.7 Appendix

9.7.1 Proof of Theorem 9.2

We now prove Theorem 9.2. We again show the achievability in two parts. First, we show that any rate pair (R_1, R_2) satisfying (9.24)-(9.26) subject to the constraints in

(9.31)-(9.33) are achievable. Then we show that for any rate pair (R_1, R_2), equivocation rates (R_1', R_2') in (9.27)-(9.28) are achievable. Fix the probability distribution

$$p(u_1)p(x_1|u_1)p(\hat{y}_1|u_1,x_1,y_1)p(u_2)p(x_2|u_2)p(\hat{y}_2|u_2,x_2,y_2)p(y,y_1,y_2|x_1,x_2) \quad (9.59)$$

Codebook generation:

User 1:

- Generate $2^{nR_{0,1}}$ $\mathbf{u}_1$ through $p(\mathbf{u}_1) = \prod_{i=1}^{n} p(u_{1,i})$ and index them as $\mathbf{u}_1(s_{1,i})$ where $s_{1,i} \in \left\{1, \ldots, 2^{nR_{0,1}}\right\}$.
- For each $\mathbf{u}_1(s_{1,i})$, generate 2^{nR_1} $\mathbf{x}_1$ through $p(\mathbf{x}_1|\mathbf{u}_1) = \prod_{i=1}^{n} p(x_{1,i}|u_{1,i})$ and index them as $\mathbf{x}_1(w_{1,i}|s_{1,i})$ where $w_{1,i} \in \left\{1, \ldots, 2^{nR_1}\right\}$.
- For each $\mathbf{u}_1(s_{1,i})$, generate $2^{n\hat{R}_1}$ $\hat{\mathbf{y}}_1$ through $p(\hat{\mathbf{y}}_1|\mathbf{u}_1) = \prod_{i=1}^{n} p(\hat{y}_{1,i}|u_{1,i})$ and index them as $\hat{\mathbf{y}}_1(z_{1,i}|s_{1,i})$ where $z_{1,i} \in \left\{1, \ldots, 2^{n\hat{R}_1}\right\}$.

User 2:

User 2 generates its own codebook through the same steps wasuser 1, only difference is that all of the subscripts 1 should be replaced with 2.

Partitioning:

User 1 partitions $2^{n\hat{R}_1}$ into $2^{nR_{0,1}}$ cells and user 2 partitions $2^{n\hat{R}_2}$ into $2^{nR_{0,2}}$ cells.

Encoding:

- User 1, upon receiving $\mathbf{y}_1(i-1)$, decides on which $z_{1,i-1}$ is received by looking for a jointly typical pair $(\hat{\mathbf{y}}_1(z_{1,i-1}|s_{1,i-1}), \mathbf{y}_1(i-1), \mathbf{x}_1(w_{1,i-1}|s_{1,i-1}), \mathbf{u}_1(s_{1,i-1}))$ which is ensured to occur if the constraint

$$I(\hat{Y}_1; Y_1|X_1, U_1) \leq \hat{R}_1 \tag{9.60}$$

is satisfied. Assume $\hat{z}_{1,i-1}$ falls into $S_{s_{1,i}}$, then user 1 sends $\mathbf{x}_1(w_{1,i}|s_{1,i})$.

- User 2, upon receiving $\mathbf{y}_2(i-1)$, decides on which $z_{2,i-1}$ is received by looking for a jointly typical pair $(\hat{\mathbf{y}}_2(z_{2,i-1}|s_{2,i-1}), \mathbf{y}_2(i-1), \mathbf{x}_2(w_{2,i-1}|s_{2,i-1}), \mathbf{u}_2(s_{2,i-1}))$ which is ensured to occur if the constraint

$$I(\hat{Y}_2; Y_2|X_2, U_2) \leq \hat{R}_2 \tag{9.61}$$

is satisfied. Assume $\hat{z}_{2,i-1}$ falls into $S_{s_{2,i}}$, then user 2 sends $\mathbf{x}_2(w_{2,i}|s_{2,i})$.

Decoding:

- Receiver first decodes $(\mathbf{u}_1(s_{1,i}), \mathbf{u}_2(s_{2,i}))$ jointly which can be done with vanishingly small error probability if

$$R_{0,1} \leq I(U_1; Y|U_2) \tag{9.62}$$

$$R_{0,2} \leq I(U_2; Y|U_1) \tag{9.63}$$

$$R_{0,1} + R_{0,2} \leq I(U_1, U_2; Y) \tag{9.64}$$

- Receiver list decodes $\hat{\mathbf{y}}_1(z_{1,i-1})$ and $\hat{\mathbf{y}}_2(z_{2,i-1})$, separately. It first forms its ambiguity set for $z_{1,i-1}$ as

$$\begin{aligned}&\mathcal{L}(z_{1,i-1})\\&= \{z_{1,i-1} : (\hat{\mathbf{y}}_1(z_{1,i-1}|s_{1,i-1}), \mathbf{y}(i), \mathbf{u}_1(s_{1,i-1}), \mathbf{u}_2(s_{2,i-1})) \text{ is jointly typical}\}\end{aligned} \tag{9.65}$$

and intersects with $S_{s_{1,i}}$ which has the correct and unique intersection point if

$$\hat{R}_1 \leq R_{0,1} + I(\hat{Y}_1; Y|U_1, U_2) \tag{9.66}$$

Similarly, to decode $z_{2,i-1}$ reliably, we need the following condition

$$\hat{R}_2 \leq R_{0,2} + I(\hat{Y}_2; Y|U_1, U_2) \tag{9.67}$$

- Receiver finally decodes $w_{1,i-1}$ and $w_{2,i-1}$ jointly which can be done with vanishingly small error probability if

$$R_1 \leq I(X_1; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2, X_2) \tag{9.68}$$

$$R_2 \leq I(X_2; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2, X_1) \tag{9.69}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, \hat{Y}_1, \hat{Y}_2|U_1, U_2) \tag{9.70}$$

Compression constraints:

As of now, we described encoding and decoding procedures. Before starting the equivocation calculations, we derive the compression constraints given in (9.31), (9.32) and (9.33). First, using (9.60) (resp. (9.61)) in (9.66) (resp. 9.67), we get

$$I(\hat{Y}_1; Y_1|X_1, U_1) \leq R_{0,1} + I(\hat{Y}_1; Y|U_1, U_2) \tag{9.71}$$

$$I(\hat{Y}_2; Y_2|X_2, U_2) \leq R_{0,2} + I(\hat{Y}_2; Y|U_1, U_2) \tag{9.72}$$

Next, using (9.62) and (9.63) in the equations above, we get

$$I(\hat{Y}_1; Y_1|X_1, U_1) \leq I(U_1, \hat{Y}_1; Y|U_2) \tag{9.73}$$

$$I(\hat{Y}_2; Y_2|X_2, U_2) \leq I(U_2, \hat{Y}_2; Y|U_1) \tag{9.74}$$

Finally, the last constraint in (9.33) can be obtained as follows

$$\begin{aligned} &I(\hat{Y}_1; Y_1|X_1, U_1) + I(\hat{Y}_2; Y_2|X_2, U_2) \\ &\quad \leq R_{0,1} + R_{0,2} + I(\hat{Y}_1; Y|U_1, U_2) + I(\hat{Y}_2; Y|U_1, U_2) && (9.75) \\ &\quad \leq I(U_1, U_2; Y) + I(\hat{Y}_1; Y|U_1, U_2) + I(\hat{Y}_2; Y|U_1, U_2) && (9.76) \end{aligned}$$

where we used (9.64).

Equivocation computation:

We now compute the equivocation rates. Since the computation of user 2's equivocation rate follows from the symmetry, we only present the computation for

user 1. We assume that the following

$$R_1' - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \geq 0 \tag{9.77}$$

otherwise the equivocation rate is zero. The cases

$$R_1' - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \leq R_1 \quad \text{and} \quad R_1' - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \geq R_1 \tag{9.78}$$

will be treated separately. First assume that

$$R_1' - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \leq R_1 \tag{9.79}$$

is satisfied for any admissible R_1'. In this case, we expand the codebook as follows: Generate $2^{nR_1'}$ $\mathbf{x}_1$ for each $\mathbf{u}_1(s_{1,i})$ and index them as $\mathbf{x}_1(\tilde{w}_{1,i}|s_{1,i})$ where

$$\tilde{w}_{1,i} = (w_{1,i}, l_i) \tag{9.80}$$

and $w_{1,i} \in \left\{1, \ldots, 2^{nR_1}\right\}, \quad l_i \in \left\{1, \ldots, 2^{n(R_1'-R_1)}\right\}$. Start with the definition

$$
\begin{aligned}
nR_{e,1} &\geq H(W_1|Y_2^n, X_2^n, W_2) && (9.81)\\
&= H(W_1|Y_2^n, X_2^n) && (9.82)\\
&\geq H(W_1|Y_2^n, U_1^n, U_2^n, X_2^n, \hat{Y}_1^n) && (9.83)\\
&= H(W_1, Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n) - H(Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n) && (9.84)\\
&= H(X_1^n, W_1, Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n) - H(X_1^n|W_1, Y_2^n, \hat{Y}_1^n, U_1^n, U_2^n, X_2^n)\\
&\quad - H(Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n) && (9.85)\\
&= H(X_1^n|U_1^n, U_2^n, X_2^n) + H(W_1, Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n, X_1^n)\\
&\quad - H(X_1^n|W_1, Y_2^n, \hat{Y}_1^n, U_1^n, U_2^n, X_2^n) - H(Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n) && (9.86)\\
&\geq H(X_1^n|U_1^n, U_2^n, X_2^n) - I(X_1^n; Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n)\\
&\quad - H(X_1^n|W_1, Y_2^n, \hat{Y}_1^n, U_1^n, U_2^n, X_2^n) && (9.87)
\end{aligned}
$$

where (9.82) is due to the Markov chain $W_2 \to (X_2^n, Y_2^n) \to W_1$ and (9.83) follows from the fact that conditioning cannot increase entropy. Each term in (9.87) will be treated separately. The first term in (9.87) can be expressed as

$$H(X_1^n|U_1^n, U_2^n, X_2^n) = H(X_1^n|U_1^n) = nR_1' \tag{9.88}$$

where the first equality is due to the fact that X_1^n and (X_2^n, U_2^n) are independent, and the second one follows from the fact that given $U_1^n = \mathbf{u}_1$, X_1^n can take $2^{nR_1'}$

values with equal probability. The second term in (9.87) can be bounded as

$$I(X_1^n; Y_2^n, \hat{Y}_1^n | U_1^n, U_2^n, X_2^n) \leq nI(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) + \epsilon_n \tag{9.89}$$

because of the fact that the channel is memoryless and the codewords are generated in an i.i.d. manner. To bound the last term in (9.87), assume that user 2 is trying to decode X_1^n using $Y_2^n, \hat{Y}_1^n, W_1$ as side information. Since given $W_1 = w_1$, X_1^n can take $2^{n(R_1' - R_1)} \leq 2^{nI(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2)}$ values, user 1 can reliably decode X_1^n, hence we have

$$H(X_1^n | W_1, Y_2^n, \hat{Y}_1^n, U_1^n, U_2^n, X_2^n) \leq \epsilon_n \tag{9.90}$$

due to Fano's lemma. Therefore, we have

$$R_{e,1} \leq R_1' - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \tag{9.91}$$

as an achievable equivocation rate if (9.79) is satisfied.

Now assume that there exists at least one R_1' in the achievable region such that

$$R_1' - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \geq R_1 \tag{9.92}$$

is satisfied. In this case, generate $2^{n\left(R_1 + I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2)\right)}$ $\mathbf{x}_1$ for each $\mathbf{u}_1(s_{1,i})$ and

index them as $\mathbf{x}_1(\tilde{w}_{1,i}|s_{1,i})$ where

$$\tilde{w}_{1,i} = (w_{1,i}, l_i) \tag{9.93}$$

and $w_{1,i} \in \left\{1, \ldots, 2^{nR_1}\right\}, l_i \in \left\{1, \ldots, 2^{n(I(X_1;Y_2|U_1,U_2,X_2)}\right\}$. Using previous analysis, we have

$$\begin{aligned} nR_{e,1} \geq & H(X_1^n|U_1^n, U_2^n, X_2^n) - I(X_1^n; Y_2^n, \hat{Y}_1^n|U_1^n, U_2^n, X_2^n) \\ & - H(X_1^n|W_1, Y_2^n, \hat{Y}_1^n, U_1^n, U_2^n, X_2^n) \end{aligned} \tag{9.94}$$

where the first term is

$$H(X_1^n|U_1^n, U_2^n, X_2^n) = H(X_1^n|U_1^n) = nR_1 + nI(X_1; Y_2, \hat{Y}_1|U_1, U_2, X_2) \tag{9.95}$$

where the first equality is due to the fact that X_1^n is independent of (U_2^n, X_2^n) and the second equality is due to the fact that given $U_1^n = \mathbf{u}_1$, X_1^n can take $2^{n\left(R_1 + I(X_1;Y_2,\hat{Y}_1|U_1,U_2,X_2)\right)}$ values with equal probability. Moreover, the last term in (9.94) can be bounded as

$$H(X_1^n|W_1, Y_2^n, \hat{Y}_1^n, U_1^n, U_2^n, X_2^n) \leq \epsilon_n \tag{9.96}$$

because user 2 can decode X_1^n using its observation and side information W_1 due to the fact that given $W_2 = w_2$, X_1^n can take $2^{nI(X_1;Y_2,\hat{Y}_1|U_1,U_2,X_2)}$ values. Therefore, we

have

$$R_{e,1} \leq R_1 + I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) = R_1 \tag{9.97}$$

as an achievable equivocation rate if (9.92) is satisfied.

9.7.2 Proof of Theorem 9.3

We now prove Theorem 9.3. We start with the first user as follows

$$\begin{aligned}
nR_{e,1} &= H(W_1 | Y_2^n, X_2^n, W_2) && (9.98)\\
&= H(W_1 | Y_2^n, X_2^n) && (9.99)\\
&= H(W_1 | X_2^n) - I(W_1; Y_2^n | X_2^n) && (9.100)\\
&= I(W_1; Y^n | X_2^n) - I(W_1; Y_2^n | X_2^n) + H(W_1 | Y_2^n, X_2^n) && (9.101)\\
&\leq I(W_1; Y^n | X_2^n) - I(W_1; Y_2^n | X_2^n) + \epsilon_n && (9.102)\\
&\leq I(W_1; Y^n | Y_2^n, X_2^n) + \epsilon_n && (9.103)\\
&\leq I(X_1^n, W_1; Y^n | Y_2^n, X_2^n) + \epsilon_n && (9.104)\\
&= I(X_1^n; Y^n | Y_2^n, X_2^n) + I(W_1; Y^n | Y_2^n, X_2^n, X_1^n) + \epsilon_n && (9.105)\\
&= I(X_1^n; Y^n | Y_2^n, X_2^n) + \epsilon_n && (9.106)\\
&= \sum_{i=1}^{n} I(Y_i; X_1^n | Y_2^n, X_2^n, Y^{i-1}) + \epsilon_n && (9.107)\\
&= \sum_{i=1}^{n} H(Y_i | Y_2^n, X_2^n, Y^{i-1}) - H(Y_i | Y_2^n, X_2^n, X_1^n, Y^{i-1}) + \epsilon_n && (9.108)\\
&\leq \sum_{i=1}^{n} H(Y_i | Y_{2,i}, X_{2,i}) - H(Y_i | Y_2^n, X_2^n, X_1^n, Y^{i-1}, Y_{1,i}) + \epsilon_n && (9.109)
\end{aligned}$$

where (9.98) is due to the Markov chain $W_2 \to (X_2^n, Y_2^n) \to W_1$, (9.102) is due to Fano's lemma, (9.106) is due to the fact that given X_1^n, W_1 is independent of all other terms, and (9.109) follows from the fact that conditioning cannot increase entropy. Now, consider the following Markov chains

$$\left(Y^{i-1}, X_2^{i-1}, X_1^{i-1}\right) \to (X_{1,i}, X_{2,i}, Y_{1,i}, Y_{2,i}) \to Y_i \tag{9.110}$$

$$\left(Y_{i+1}^n, X_{2,i+1}^n, X_{1,i+1}^n\right) \to (X_{1,i}, X_{2,i}, Y_{1,i}, Y_{2,i}) \to Y_i \tag{9.111}$$

where the first one is due to the memoryless property of the channel and the second one is due to the fact that correlation induced between current output, i.e., Y_i, and future inputs, i.e., $\left(X_{2,i+1}^n, X_{1,i+1}^n\right)$ can be resolved by conditioning on $(Y_{1,i}, Y_{2,i})$. Hence, using these two Markov chains, we have

$$nR_{e,1} \leq \sum_{i=1}^{n} H(Y_i|Y_{2,i}, X_{2,i}) - H(Y_i|Y_{2,i}, X_{2,i}, X_{1,i}, Y_{1,i}) + \epsilon_n \tag{9.112}$$

$$= \sum_{i=1}^{n} I(X_{1,i}, Y_{1,i}; Y_i|Y_{2,i}, X_{2,i}) + \epsilon_n \tag{9.113}$$

Similarly, we can obtain the following bound for the second user

$$nR_{e,2} \leq \sum_{i=1}^{n} I(X_{2,i}, Y_{2,i}; Y_i|Y_{1,i}, X_{1,i}) + \epsilon_n \tag{9.114}$$

These bounds can be single-letterized to obtain the bounds in Theorem 9.3; completing the proof.

Chapter 10

On Compound Wiretap Channels

10.1 Introduction

In this chapter, we study the compound wiretap channel. The compound wiretap channel can be defined in two alternative yet equivalent forms: The compound wiretap channel consists of a user and an eavesdropper, where there are a finite number of channel states determining the channel transition probability distribution, see Figure 10.1. The channel state is fixed during the entire transmission and known at the receivers, but not at the transmitter. The goal of the transmitter is to ensure a perfect secrecy rate irrespective of the channel state realization. In the second equivalent description, see Figure 10.2, the compound wiretap channel consists of a group of users and a group of eavesdroppers, where the transmitter sends a common confidential message to the users while keeping all eavesdroppers ignorant of this message. Regarding each channel state as a user and eavesdropper pair, the equivalence of two definitions is clear. In this chapter, we adopt the second interpretation.

The compound wiretap channel is first studied in [90, 91], which consider the parallel wiretap channel with two sub-channels where each sub-channel is wiretapped by a different eavesdropper. Recent works on compound wiretap channels are [24, 25, 38, 54, 92–94]. Reference [92] studies the fading wiretap channel with many

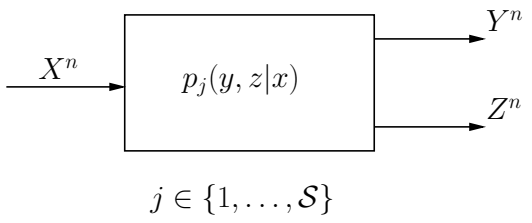

Figure 10.1: The compound wiretap channel defined in terms of channel uncertainty.

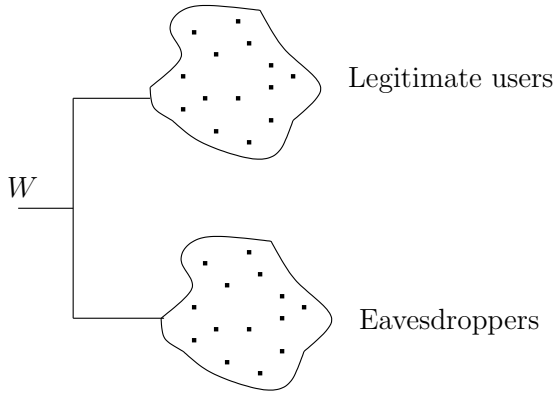

Figure 10.2: The compound wiretap channel defined in terms multicasting a common confidential message.

receivers, [24, 25, 54] consider the transmission of a common confidential message to many legitimate receivers in the presence of a single eavesdropper. Reference [38] considers the general discrete memoryless compound wiretap channel and provides inner and outer bounds for the secrecy capacity. Moreover, [38] establishes the secrecy capacity of the degraded compound wiretap channel as well as its degraded Gaussian MIMO instance. Another work on the compound wiretap channel is [94] where the secrecy capacity of a class of non-degraded Gaussian parallel compound wiretap channels is established.

A recent work [93] studies the two-user one-eavesdropper compound wiretap channel, and obtains a lower bound for its secrecy capacity. The achievable scheme

in [93] uses indirect decoding [13] and Marton's inner bound for discrete memoryless broadcast channels [11]. This lower bound is the best achievable secrecy rate for the two-user one-eavesdropper case. In particular, it provides a strictly better achievable secrecy rate than the previous achievable secrecy rate in [38], which corresponds to an extension of the Csiszar-Korner achievable scheme in [3] to a compound setting.

Here, we first provide a new achievable scheme which is potentially better than this best known lower bound in [93], i.e., the secrecy rate our scheme can provide is always as large as the secrecy rate that the achievable scheme in [93] can provide. Similar to [93], our achievable scheme also uses indirect decoding [13] and Marton's inner bound [11]. However, the difference between our achievable scheme and the one in [93] comes from the equivocation computation. In particular, at a certain step of the equivocation computation in [93], joint conditional entropy of two random variables is upper bounded by conditional individual entropies, and the proof is concluded. Here, we compute the equivocation rate without using this potentially loose outer bound, which gives us a potentially better achievable scheme than the one in [93].

We next consider the two-user one-eavesdropper Gaussian MIMO compound wiretap channel and obtain an achievable secrecy rate for it by using DPC [12] in the achievable scheme we already provided. We address the tightness of the resulting achievable secrecy rate by showing that it can achieve at least half of the secrecy capacity. We also consider a special class of two-user one-eavesdropper Gaussian MIMO compound wiretap channels, where the eavesdropper is degraded with respect to one of the two users. We obtain the secrecy capacity of these channels.

10.2 Channel Model and Definitions

We study the two-user one-eavesdropper discrete memoryless compound wiretap channel, see Figure 10.3, with a transition probability $p(y_1, y_2, z|x)$ where $x \in \mathcal{X}$ is the channel input, $y_j \in \mathcal{Y}_j$ is the jth user's observation, and $z \in \mathcal{Z}$ is the eavesdropper's observation. We consider the scenario where the transmitter sends a common confidential message to both users, which needs to be kept perfectly secret from the eavesdropper.

An $(n, 2^{nR})$ code for this channel consists of one message set $\mathcal{W} = \{1, \ldots, 2^{nR}\}$, one encoder at the transmitter $f_n : \mathcal{W} \to \mathcal{X}^n$, and one decoder at each user $g_{j,n} : \mathcal{Y}_j^n \to \mathcal{W},\ j = 1, 2$. The probability of error is defined as

$$P_{e,n} = \max_{j=1,2} \Pr\left[g_{j,n}(f_n(W)) \neq W\right] \tag{10.1}$$

where W is a uniformly distributed random variable in $\mathcal{W}$. We measure the secrecy of the message W by its equivocation rate at the eavesdropper $(1/n)H(W|Z^n)$ [2, 3].

A perfect secrecy rate R is said to be achievable if there exists an $(n, 2^{nR})$ code which has $\lim_{n\to\infty} P_{e,n} = 0$, and

$$\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) = 0 \tag{10.2}$$

The secrecy capacity C_S is defined to be the supremum of all achievable perfect secrecy rates.

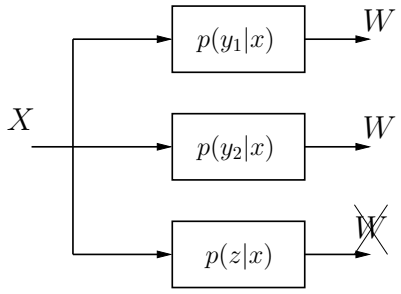

Figure 10.3: The compound wiretap channel with two legitimate users and a single eavesdropper.

10.3 An Achievable Secrecy Rate

Here, we revisit the existing achievability results for two-user one-eavesdropper discrete memoryless compound wiretap channels, and provide a potentially higher achievable secrecy rate than the best known achievable secrecy rate given in [93]. The first achievable scheme for discrete memoryless compound wiretap channels is proposed in [38]. This achievable scheme can be viewed as an extension of the Csiszar-Korner achievable scheme for discrete memoryless wiretap channels [3] to compound wiretap channels. The achievable secrecy rate in [38] is stated in the following theorem.

Theorem 10.1 ([38, Theorem 1]) *The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded as follows*

$$C_S \geq \max_{U \to X \to (Y_1, Y_2, Z)} \min_{j=1,2} I(U; Y_j) - I(U; Z) \tag{10.3}$$

This inner bound is strictly improved in [93], where a new achievable scheme is proposed by using indirect decoding [13] and Marton's achievable scheme for discrete memoryless broadcast channels [11]. This achievable secrecy rate is stated in the following theorem.

Theorem 10.2 ([93, Theorem 1]) *The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded by the maximum of R satisfying*

$$R \leq I(V_0, V_1; Y_1) - I(V_0, V_1; Z) \tag{10.4}$$

$$R \leq I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \tag{10.5}$$

for some (V_0, V_1, V_2) such that $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$, and

$$I(V_1, V_2; Z|V_0) + I(V_1; V_2|V_0) \leq I(V_1; Z|V_0) + I(V_2; Z|V_0) \tag{10.6}$$

We now provide a new achievable secrecy rate for two-user one-eavesdropper discrete memoryless compound wiretap channels. This new achievable scheme is similar to the achievable scheme given in Theorem 10.2 in terms of the techniques used. In particular, this new achievable scheme also uses indirect decoding [13] and Marton's inner bound for discrete memoryless broadcast channels [11]. The only new ingredient in the achievable scheme we provide here as compared to the achievable scheme in Theorem 10.2 is the way we compute the equivocation rate. In particular, while computing the equivocation rate in the proof of Theorem 10.2,

one needs to show the following

$$\lim_{n\to\infty} \frac{1}{n} H(V_1^n, V_2^n | W, V_0^n, Z^n) = 0 \tag{10.7}$$

To this end, [93] first considers the following bound

$$\frac{1}{n} H(V_1^n, V_2^n | W, V_0^n, Z^n) \leq \frac{1}{n} H(V_1^n | W, V_0^n, Z^n) + \frac{1}{n} H(V_2^n | W, V_0^n, Z^n) \tag{10.8}$$

and shows that each term on the right hand side of (10.8) vanishes as $n \to \infty$. The upper bound in (10.8) might result in potential suboptimality in the achievable secrecy rate given in Theorem 10.2 as compared to the achievable secrecy rate that can be obtained by directly showing (10.7) without any recourse to the bound in (10.8). The corresponding new achievable secrecy rate, obtained by showing (10.7) without using the bound in (10.8), is given in the following theorem.

Theorem 10.3 *The secrecy capacity of the two-user one-eavesdropper discrete memoryless compound wiretap channel is lower bounded by the maximum of R satisfying*

$$R \leq I(V_0, V_1; Y_1) - I(V_0, V_1; Z) \tag{10.9}$$

$$R \leq I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \tag{10.10}$$

$$\begin{aligned} 2R \leq\ & I(V_0, V_1; Y_1) + I(V_0, V_2; Y_2) - 2I(V_0; Z) - I(V_1, V_2; Z | V_0) \\ & - I(V_1; V_2 | V_0) \end{aligned} \tag{10.11}$$

for some (V_0, V_1, V_2) such that $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$.

The proof of this theorem is given in Appendix 10.6.1. We note that the achievable secrecy rate given in Theorem 10.3 has one more rate constraint than the achievable secrecy rate given in Theorem 10.2, while both achievable secrecy rates have two rate constraints (10.9)-(10.10) in common. On the other hand, the new achievable secrecy rate in Theorem 10.3 does not have the constraint in (10.6) that Theorem 10.2 has. We next obtain a potentially looser version of the achievable secrecy rate in Theorem 10.3, which will be useful to compare the achievable secrecy rates in Theorems 10.2 and 10.3. This potentially looser version of the achievable secrecy rate given in Theorem 10.3 is stated in the following corollary.

Corollary 10.1 *The secrecy capacity of the two-user one-eavesdropper compound wiretap channel is lower bounded as follows*

$$C_S \geq \max\left\{R_S^{12}, R_S^{21}\right\} \tag{10.12}$$

for some (V_0, V_1, V_2) *such that* $(V_0, V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2, Z)$*, and* R_S^{12}, R_S^{21} *are given by*

$$R_S^{12} = \min\{I(V_0, V_1; Y_1) - I(V_0, V_1; Z), I(V_0, V_2; Y_2) - I(V_0; Z) - I(V_2; Z, V_1|V_0)\} \tag{10.13}$$

$$R_S^{21} = \min\{I(V_0, V_1; Y_1) - I(V_0; Z) - I(V_1; Z, V_2|V_0), I(V_0, V_2; Y_2) - I(V_0, V_2; Z)\} \tag{10.14}$$

The proof of Corollary 10.1 is given in Appendix 10.6.2. We now compare the potentially looser version of Theorem 10.3 given in Corollary 10.1 with Theorem 10.2

to show that the achievable secrecy rate in Theorem 10.3 is potentially higher than the one in Theorem 10.2. We note that the constraint in (10.6) implies

$$0 \leq I(V_1; Z|V_0) + I(V_2; Z|V_0) - I(V_1; V_2|V_0) - I(V_1, V_2; Z|V_0) \tag{10.15}$$

$$= I(V_2; Z|V_0) - I(V_1; V_2|V_0) - I(V_2; Z|V_0, V_1) \tag{10.16}$$

$$= I(V_2; Z|V_0) - I(V_2; Z, V_1|V_0) \tag{10.17}$$

$$= -I(V_2; V_1|V_0, Z) \tag{10.18}$$

which is equivalent to

$$I(V_2; V_1|V_0, Z) = 0 \tag{10.19}$$

Consider a random variable triple (V_0, V_1, V_2) such that it satisfies $(V_0, V_1, V_2) \rightarrow X \rightarrow (Y_1, Y_2, Z)$ and (10.6). Due to (10.19), we have

$$R_S^{12} = R_S^{21} = \min\{I(V_0, V_1; Y_1) - I(V_0, V_1; Z), I(V_0, V_2; Y_2) - I(V_0, V_2; Z)\} \tag{10.20}$$

which is the achievable secrecy rate in Theorem 10.2. Thus, for any random variable triple (V_0, V_1, V_2) satisfying (10.6), both the new achievable secrecy rate in Corollary 10.1, hence in Theorem 10.3, and the achievable secrecy rate in Theorem 10.2 are equal. However, since the new achievable secrecy rate in Theorem 10.3 does not have the constraint, i.e., restriction, in (10.6), it is potentially higher than the achievable secrecy rate in Theorem 10.2.

10.4 Gaussian MIMO Compound Wiretap Channel

We consider the two-user one-eavesdropper Gaussian MIMO compound wiretap channel which is defined by

$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{N}_1 \tag{10.21}$$

$$\mathbf{Y}_2 = \mathbf{X} + \mathbf{N}_2 \tag{10.22}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{10.23}$$

where the channel input $\mathbf{X}$, a $t \times 1$ vector, is subject to a covariance constraint as

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{10.24}$$

and $\mathbf{S}$ is a positive semi-definite matrix, i.e., $\mathbf{S} \succeq \mathbf{0}$. The noise covariance matrices of the Gaussian random vectors $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$, $t \times 1$ vectors, are denoted by $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2, \mathbf{\Sigma}_Z$, respectively, where we assume $\mathbf{\Sigma}_1 \succ \mathbf{0}, \mathbf{\Sigma}_2 \succ \mathbf{0}, \mathbf{\Sigma}_Z \succ \mathbf{0}$. We remark that the Gaussian MIMO compound wiretap channel defined in (10.21)-(10.23) actually corresponds to a special case of the more general form of the Gaussian MIMO compound wiretap channel given by

$$\mathbf{Y}_j = \mathbf{H}_j\mathbf{X} + \mathbf{N}_j, \quad j = 1, 2 \tag{10.25}$$

$$\mathbf{Z} = \mathbf{H}_Z\mathbf{X} + \mathbf{N}_Z \tag{10.26}$$

However, using the rather straightforward analysis given in Section 7.1 of [19], the results we obtain for the channel model in (10.21)-(10.23) can be extended to the most general form of the Gaussian MIMO compound wiretap channel in (10.25)-(10.26). Thus, here, we restrict our attention to the channel model in (10.21)-(10.23). Another remark about the channel model is the way we impose the power constraint on the channel input $\mathbf{X}$. We note that the covariance constraint in (10.24) subsumes the more common total power constraint $E\left[\mathbf{X}^{\top}\mathbf{X}\right] \leq P$, in that both inner and outer bounds proved for the covariance constraint in (10.24) can be extended to the case where the channel input $\mathbf{X}$ is subject to a total power constraint; see Lemma 1 and Corollary 1 in [4]. Thus, without loss of generality, we consider only the covariance constraint in (10.24).

We now present an achievable secrecy rate for the two-user one-eavesdropper Gaussian MIMO compound wiretap channel in (10.21)-(10.23) given in the following theorem.

Theorem 10.4 *The secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel $C_S(\mathbf{S})$ is lower bounded by the maximum of R satisfying*

$$R = \max\left\{R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2), R_S^{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)\right\} \tag{10.27}$$

for some positive semi-definite matrices $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2$ such that $\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$,

and $R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ *is given by*

$$R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = \min\{R_{S1}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)\} \tag{10.28}$$

where $R_{S1}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ *are*

$$R_{S1}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_1|}{|\mathbf{K}_2 + \mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|} \tag{10.29}$$

$$\begin{aligned} R_{S2}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = {} & \frac{1}{2}\log\frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_1|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|} \\ & + \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{10.30}$$

Moreover, $R_S^{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ *can be obtained from* $R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ *by swapping the indices* 1 *and* 2.

Theorem 10.4 can be obtained from Corollary 10.1 by choosing (V_0, V_1, V_2) to be jointly Gaussian with a specific correlation structure. V_0, to which the covariance matrix $\mathbf{K}_0$ is allotted, can be viewed as the common part, and is decoded by both users. V_1 (resp. V_2) can be thought of as a private message that is directed to only the first (resp. second) user, the second (resp. first) user does not bother to decode. V_1, V_2 are encoded using DPC [12]. Thus, depending on the encoding order used in DPC, we get a different achievable secrecy rate. For example, $R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ comes from encoding V_1 first, then using DPC for V_2. The details of the proof of Theorem 10.4 can be found in Appendix 10.6.3.

We next note the following special case of Theorem 10.4.

Corollary 10.2 *The secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel $C_S(\mathbf{S})$ is lower bounded by the maximum of R satisfying*

$$R = \max\left\{R_S^{12}(\mathbf{K}_1, \mathbf{K}_2), R_S^{21}(\mathbf{K}_1, \mathbf{K}_2)\right\} \tag{10.31}$$

for some positive semi-definite matrices $\mathbf{K}_1, \mathbf{K}_2$ such that

$$\mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S} \tag{10.32}$$

and $R_S^{12}(\mathbf{K}_1, \mathbf{K}_2)$ is given by

$$R_S^{12}(\mathbf{K}_1, \mathbf{K}_2) = \min\{R_{S1}^{12}(\mathbf{K}_1, \mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_1, \mathbf{K}_2)\} \tag{10.33}$$

where $R_{S1}^{12}(\mathbf{K}_1, \mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_1, \mathbf{K}_2)$ are

$$R_{S1}^{12}(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_1|}{|\mathbf{K}_2 + \mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|} \tag{10.34}$$

$$R_{S2}^{12}(\mathbf{K}_1, \mathbf{K}_2) = \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.35}$$

Moreover, $R_S^{21}(\mathbf{K}_1, \mathbf{K}_2)$ can be obtained from $R_S^{12}(\mathbf{K}_1, \mathbf{K}_2)$ by swapping the indices 1 *and* 2.

This corollary can be obtained by setting $\mathbf{K}_0 = \phi$ in Theorem 10.4. We next assess the tightness of the inner bound in Corollary 10.2. To this end, we introduce the following simple outer bound on the secrecy capacity of the two-user one-eavesdropper

Gaussian MIMO compound wiretap channel.

Lemma 10.1 *The secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel is upper bounded as follows*

$$C_S(\mathbf{S}) \leq \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \tag{10.36}$$

where $C_{Sj}(\mathbf{S}),\ j = 1, 2,$ *is given by*

$$C_{Sj}(\mathbf{S}) = \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_j|}{|\mathbf{\Sigma}_j|} - \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.37}$$

We note that $C_{Sj}(\mathbf{S})$ is the secrecy capacity of the Gaussian MIMO wiretap channel between the jth user and the eavesdropper. If one wants to multicast a common confidential message to both users, one cannot transmit at a higher rate than the secrecy capacity of the wiretap channel between the jth user and the eavesdropper for $j = 1, 2$. This observation proves Lemma 10.1. We now provide the following theorem which assesses the tightness of the achievable secrecy rate in Corollary 10.2 in terms of the outer bound in Lemma 10.1.

Theorem 10.5 *The secrecy capacity* $C_S(\mathbf{S})$ *of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel satisfies*

$$\frac{1}{2} \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \leq C_S(\mathbf{S}) \leq \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \tag{10.38}$$

The proof of Theorem 10.5 is given in Appendix 10.6.4. In the proof of this theorem,

we use the achievable secrecy rate in Corollary 10.2 and the channel enhancement technique [4]. Hence, Theorem 10.5 states that using Corollary 10.2, one can get an achievable secrecy rate R such that

$$\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \leq 2R \tag{10.39}$$

which, in turn, implies that $C_S(\mathbf{S}) \leq 2R$ using Lemma 10.1. Thus, the achievable secrecy rate given in Corollary 10.2 achieves at least half of the secrecy capacity. We note that there are two possible directions that might improve this result. The first one is to consider the more general form of Corollary 10.2 given in Theorem 10.4. This might lead to higher achievable secrecy rates. The second possible improvement is to find better outer bounds for the secrecy capacity of the Gaussian MIMO compound wiretap channel. The outer bound in Lemma 10.1 seems to be loose. In general, we do not expect the secrecy capacity of a Gaussian MIMO compound wiretap channel to be the minimum of the secrecy capacities of the underlying wiretap channels. However, still, there might be cases that the outer bound in Lemma 10.1 is tight. To give an example, assume that the eavesdropper is degraded with respect to the second user, i.e., we have $\mathbf{X} \to \mathbf{Y}_2 \to \mathbf{Z}$, which is equivalent to

$$\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z \tag{10.40}$$

The secrecy capacity of a Gaussian MIMO compound wiretap channel satisfying (10.40) is given by the following theorem.

Theorem 10.6 *The secrecy capacity region of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel satisfying (10.40) is given by*

$$C_S(\mathbf{S}) = \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \tag{10.41}$$

The proof of Theorem 10.6 is given in Appendix 10.7. Theorem 10.6 states that if the eavesdropper is degraded with respect to one of the two users, the secrecy capacity of the two-user one-eavesdropper Gaussian MIMO compound wiretap channel is equal to the minimum of the secrecy capacities of the underlying two Gaussian MIMO wiretap channels.

10.5 Conclusions

In this chapter, we study two-user one-eavesdropper compound wiretap channels and obtain a lower bound for their secrecy capacity. We show that this lower bound is potentially better than all existing lower bounds. We also study the two-user one-eavesdropper Gaussian MIMO compound wiretap channel by providing a DPC-based achievable secrecy rate. Finally, we discuss the tightness of this achievable rate for the Gaussian MIMO channel.

10.6 Appendix

10.6.1 Proof of Theorem 10.3

We fix a random variable tuple (V_0, V_1, V_2, X) such that

$$p(v_0, v_1, v_2, x, y_1, y_2, z) = p(v_0, v_1, v_2)p(x|v_0, v_1, v_2)p(y_1, y_2, z|x) \tag{10.42}$$

Codebook generation:

- Generate $2^{n(R+\tilde{R}_0)}$ length-n $\mathbf{v}_0$ sequences through $p(\mathbf{v}_0) = \prod_{i=1}^{n} p(v_{0,i})$. Index them as $\mathbf{v}_0(w, \tilde{w}_0)$ where $W \in \{1, \ldots, 2^{nR}\}$, and $\tilde{W}_0 \in \{1, \ldots, 2^{n\tilde{R}_0}\}$.

- For each $\mathbf{v}_0$ sequence and $j \in \{1, 2\}$, generate $2^{n(\tilde{R}_j+L_j)}$ length-n $\mathbf{v}_j$ sequences through $p(\mathbf{v}_j|\mathbf{v}_0) = \prod_{i=1}^{n} p(v_{j,i}|v_{0,i})$. Index them as $\mathbf{v}_j(w, \tilde{w}_0, \tilde{w}_j, l_j)$ where $\tilde{W}_j \in \{1, \ldots, 2^{n\tilde{R}_j}\}, L_j \in \{1, \ldots, 2^{nL_j}\}$.

Encoding:

If $W = w$ is to be transmitted, randomly pick $(\tilde{w}_0, \tilde{w}_1, \tilde{w}_2)$. Then, find an (l_1, l_2) pair such that

$$(V_0^n(w, \tilde{w}_0), V_1^n(w, \tilde{w}_0, \tilde{w}_1, l_1), V_2^n(w, \tilde{w}_0, \tilde{w}_2, l_2)) \tag{10.43}$$

is jointly typical. Finally, generate the channel input X^n through $\prod_{i=1}^{n} p(x_i|v_{1,i}, v_{2,i})$.

Selection of $\tilde{R}_0, \tilde{R}_1, \tilde{R}_2, L_1, L_2$:

We select the rates $\tilde{R}_0, \tilde{R}_1, \tilde{R}_2, L_2$ as follows

$$\tilde{R}_0 = I(V_0; Z) - \epsilon \tag{10.44}$$

$$\tilde{R}_1 + \tilde{R}_2 = I(V_1, V_2; Z|V_0) - 2\epsilon \tag{10.45}$$

$$L_1 + L_2 = I(V_1; V_2|V_0) + \epsilon \tag{10.46}$$

$$\tilde{R}_1 + L_1 \leq I(V_1; Z, V_2|V_0) \tag{10.47}$$

$$\tilde{R}_2 + L_2 \leq I(V_2; Z, V_1|V_0) \tag{10.48}$$

Probability of error analysis:

- Since we have $L_1 + L_2 > I(V_1; V_2|V_0)$, encoding, i.e., to find an (l_1, l_2) pair such that (10.43) is jointly typical, can be accomplished with vanishingly small probability of error.

- The jth user decodes W through (V_0^n, V_j^n), which can be accomplished with vanishingly small probability of error if we have

$$R + \tilde{R}_0 + \tilde{R}_j + L_j < I(V_0, V_j; Y_j), \ j = 1, 2 \tag{10.49}$$

Equivocation computation:

We now show that this coding scheme satisfies the perfect secrecy requirement in

(10.2). To this end, consider the following

$$H(W|Z^n) = H(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2|Z^n) - H(\tilde{W}_0, \tilde{W}_1, \tilde{W}_2|Z^n, W) \tag{10.50}$$

$$= H(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2) - I(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2; Z^n)$$

$$- H(\tilde{W}_0, \tilde{W}_1, \tilde{W}_2|Z^n, W) \tag{10.51}$$

The first term in (10.51) is

$$H(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2) = n(R + \tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2) \tag{10.52}$$

where we used the fact that $(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2)$ are independent and uniformly distributed random variables. The second term in (10.51) is

$$I(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2; Z^n) \leq I(V_0^n, V_1^n, V_2^n; Z^n) \tag{10.53}$$

$$\leq nI(V_0, V_1, V_2; Z) + n\gamma_{1n} \tag{10.54}$$

where $\gamma_{1n} \to 0$ as $n \to \infty$. Equation (10.53) is due to the Markov chain

$$(W, \tilde{W}_0, \tilde{W}_1, \tilde{W}_2) \to (V_0^n, V_1^n, V_2^n) \to Z^n \tag{10.55}$$

and (10.54) can be proved by following Lemma 8 [2]. We next consider the third

term in (10.51)

$$H(\tilde{W}_0, \tilde{W}_1, \tilde{W}_2|Z^n, W) = H(\tilde{W}_0|Z^n, W) + H(\tilde{W}_1, \tilde{W}_2|Z^n, W, \tilde{W}_0) \tag{10.56}$$

$$= H(\tilde{W}_0|Z^n, W) + H(\tilde{W}_1, \tilde{W}_2|Z^n, W, \tilde{W}_0, V_0^n) \tag{10.57}$$

Since $\tilde{R}_0 < I(V_0; Z)$, given $W = w$, the eavesdropper can decode $\tilde{W}_0$ through V_0^n. Thus, for the first term in (10.57), we have

$$H(\tilde{W}_0|Z^n, W) \leq n\gamma_{2n} \tag{10.58}$$

due to Fano's lemma, where $\gamma_{2n} \to 0$ as $n \to \infty$. Since $\tilde{R}_1, \tilde{R}_2, L_1, L_2$ are selected to satisfy (see (10.45)-(10.48))

$$\tilde{R}_1 + L_1 \leq I(V_1; Z, V_2|V_0) \tag{10.59}$$

$$\tilde{R}_2 + L_2 \leq I(V_2; Z, V_1|V_0) \tag{10.60}$$

$$\tilde{R}_1 + \tilde{R}_2 + L_1 + L_2 \leq I(V_1, V_2; Z|V_0) + I(V_1; V_2|V_0) \tag{10.61}$$

the eavesdropper can decode $(\tilde{W}_1, \tilde{W}_2)$ by looking for the unique jointly typical tuple

$$(V_0^n(w_0, \tilde{w}_0), V_1^n(w_0, \tilde{w}_0, \tilde{w}_1, l_1), V_2^n(w_0, \tilde{w}_0, \tilde{w}_2, l_2), Z^n) \tag{10.62}$$

Thus, for the second term in (10.57), we have

$$H(\tilde{W}_1, \tilde{W}_2 | Z^n, W, \tilde{W}_0, V_0^n) \leq n\gamma_{3n} \tag{10.63}$$

due to Fano's lemma, where $\gamma_{3n} \to 0$ as $n \to \infty$. Using (10.52), (10.54), (10.57)-(10.63) in (10.51), we get

$$\begin{aligned} H(W|Z^n) &\geq nR + n(\tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2) - nI(V_0, V_1, V_2; Z) \\ &\quad - n(\gamma_{1n} + \gamma_{2n} + \gamma_{3n}) \qquad (10.64) \\ &= nR - n3\epsilon - n(\gamma_{1n} + \gamma_{2n} + \gamma_{3n}) \qquad (10.65) \end{aligned}$$

where (10.65) follows from (10.44)-(10.45). Hence, taking $\epsilon \to 0$, and $n \to \infty$ yields

$$\lim_{n\to\infty} \frac{1}{n} I(W; Z^n) = 0 \tag{10.66}$$

which completes the equivocation computation.

Thus, we have shown that for a given (V_0, V_1, V_2, X) such that the Markov chain $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$ holds, the perfect secrecy rate R is achievable if the conditions in (10.44)-(10.49) are satisfied for some $\tilde{R}_1, \tilde{R}_2, L_1, L_2$. Finally, Fourier-Motzkin elimination can be used to remove the terms $\tilde{R}_1, \tilde{R}_2, L_1, L_2$ from the inequalities in (10.44)-(10.49), which results in the inequalities given in Theorem 10.3.

10.6.2 Proof of Corollary 10.1

We first show the achivability of R_S^{12} for a given random variable triple (V_0, V_1, V_2) satisfying $(V_0, V_1, V_2) \to X \to (Y_1, Y_2, Z)$. Let us define a, b as follows

$$a = I(V_0, V_1; Y_1) - I(V_0, V_1; Z) \tag{10.67}$$

$$b = I(V_0, V_2; Y_2) - I(V_0, V_2; Z) \tag{10.68}$$

Using (10.67)-(10.68) in (10.9)-(10.11), we have that

$$R = \min \left\{ a, b, \frac{a + b - I(V_1; V_2 | V_0, Z)}{2} \right\} \tag{10.69}$$

is an achievable secrecy rate. Since we have

$$R \geq \min \{a, b - I(V_1; V_2 | V_0, Z)\} \tag{10.70}$$

and

$$b - I(V_1; V_2 | V_0, Z) = I(V_0, V_2; Z) - I(V_0; Z) - I(V_2; Z, V_1 | V_0) \tag{10.71}$$

the achievability of R_S^{12} follows. Using the symmetry, the achievability of R_S^{21} for the same given random variable triple (V_0, V_1, V_2) can be shown as well; completing the proof.

10.6.3 Proof of Theorem 10.4

We first prove the achievability of the secrecy rate $R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ in Theorem 10.4 by computing the achievable secrecy rate R_S^{12} given in Corollary 10.1 for a particular selection of V_0, V_1, V_2. As it will be clear soon, this specific selection corresponds to the dirty-paper coding scheme proposed in [12]. We first define the independent Gaussian random vectors $\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2$ with covariance matrices $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2$, where $\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$. We set V_0, V_1, V_2 as follows

$$V_0 = \mathbf{U}_0 \tag{10.72}$$

$$V_1 = \mathbf{U}_1 + \mathbf{U}_0 \tag{10.73}$$

$$V_2 = \mathbf{U}_2 + \mathbf{A}\mathbf{U}_1 + \mathbf{U}_0 \tag{10.74}$$

where $\mathbf{A} = \mathbf{K}_2 \left[\mathbf{K}_2 + \mathbf{\Sigma}_2\right]^{-1}$ is the precoding matrix for the second user to suppress the interference originating from $\mathbf{U}_1$ [12]. Furthermore, we set the channel input $\mathbf{X} = \mathbf{U}_0 + \mathbf{U}_1 + \mathbf{U}_2$. We first compute the first term in (10.13) as follows

$$R_{S1}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) = I(V_0, V_1; \mathbf{Y}_1) - I(V_0, V_1; \mathbf{Z}) \tag{10.75}$$

$$= I(\mathbf{U}_0, \mathbf{U}_1; \mathbf{U}_0 + \mathbf{U}_1 + \mathbf{U}_2 + \mathbf{N}_1) - I(\mathbf{U}_0, \mathbf{U}_1; \mathbf{U}_0 + \mathbf{U}_1 + \mathbf{U}_2 + \mathbf{N}_Z) \tag{10.76}$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_1|}{|\mathbf{K}_2 + \mathbf{\Sigma}_1|} - \frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|} \tag{10.77}$$

where we used the definitions of $\mathbf{U}_0, \mathbf{U}_1, \mathbf{U}_2$ given in (10.72)-(10.74). We next compute the second term in (10.13). To this end, we note the following identity

$$
\begin{aligned}
& I(V_2; \mathbf{Y}_2|V_0) - I(V_2; \mathbf{Z}, V_1|V_0) \\
&= I(\mathbf{U}_2 + \mathbf{A}\mathbf{U}_1; \mathbf{U}_1 + \mathbf{U}_2 + \mathbf{N}_2) - I(\mathbf{U}_2 + \mathbf{A}\mathbf{U}_1; \mathbf{U}_1 + \mathbf{U}_2 + \mathbf{N}_Z, \mathbf{U}_1) && (10.78) \\
&= I(\mathbf{U}_2 + \mathbf{A}\mathbf{U}_1; \mathbf{U}_1 + \mathbf{U}_2 + \mathbf{N}_2) - I(\mathbf{U}_2 + \mathbf{A}\mathbf{U}_1; \mathbf{U}_1) - I(\mathbf{U}_2; \mathbf{U}_2 + \mathbf{N}_Z) && (10.79) \\
&= \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - I(\mathbf{U}_2; \mathbf{U}_2 + \mathbf{N}_Z) && (10.80) \\
&= \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (10.81)
\end{aligned}
$$

where (10.80) is due to Theorem 1 of [12]. We now compute the second term in (10.13)

$$
\begin{aligned}
R_{S2}^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2) &= I(V_0, V_2; \mathbf{Y}_2) - I(V_0; \mathbf{Z}) - I(V_2; \mathbf{Z}, V_1|V_0) && (10.82) \\
&= [I(V_0; \mathbf{Y}_2) - I(V_0; \mathbf{Z})] + [I(V_2; \mathbf{Y}_2|V_0) - I(V_2; \mathbf{Z}, V_1|V_0)] && (10.83) \\
&= [I(V_0; \mathbf{Y}_2) - I(V_0; \mathbf{Z})] + \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (10.84) \\
&= \frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{K}_0 + \mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{K}_1 + \mathbf{K}_2 + \mathbf{\Sigma}_Z|} \\
&\quad + \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (10.85)
\end{aligned}
$$

where (10.84) comes from (10.81). Thus, we have shown the achievability of $R_S^{12}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ for a given covariance matrix triple $(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$. Following the same analysis, we can show the achievability of $R_S^{21}(\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2)$ for the same covariance matrices $\mathbf{K}_0, \mathbf{K}_1, \mathbf{K}_2$ as well. This completes the proof.

10.6.4 Proof of Theorem 10.5

The upper bound in (10.38) comes from the upper bound in Theorem 10.1. Thus, we need to prove the lower bound. For that purpose, we use Corollary 10.2. We first consider the following maximization

$$\max_{\substack{\mathbf{0}\preceq\mathbf{K}_j,\ j=1,2\\ \mathbf{K}_1+\mathbf{K}_2\preceq\mathbf{S}}} R_S^{12}(\mathbf{K}_1,\mathbf{K}_2) = \max_{\substack{\mathbf{0}\preceq\mathbf{K}_j,\ j=1,2\\ \mathbf{K}_1+\mathbf{K}_2\preceq\mathbf{S}}} \min\{R_{S1}^{12}(\mathbf{K}_1,\mathbf{K}_2), R_{S2}^{12}(\mathbf{K}_1,\mathbf{K}_2)\} \tag{10.86}$$

This maximization can be put into the following alternative form

$$\begin{aligned} \max \quad & a \\ \text{s.t.} \quad & R_{S1}^{12}(\mathbf{K}_1,\mathbf{K}_2) \geq a \\ & R_{S2}^{12}(\mathbf{K}_1,\mathbf{K}_2) \geq a \end{aligned} \tag{10.87}$$

where the maximization should be taken with respect to $a, \mathbf{K}_1, \mathbf{K}_2$, and $\mathbf{K}_1, \mathbf{K}_2$ are positive semi-definite matrices such that $\mathbf{K}_1 + \mathbf{K}_2 \preceq \mathbf{S}$. The Lagrangian for the maximization in (10.87) is given by

$$\begin{aligned} \mathcal{L}(\mathbf{K}_1,\mathbf{K}_2) = a + \lambda(R_{S1}^{12}(\mathbf{K}_1,\mathbf{K}_2) - a) + \mu(R_{S2}^{12}(\mathbf{K}_1,\mathbf{K}_2) - a) + \text{tr}(\mathbf{K}_1\mathbf{M}_1) \\ + \text{tr}(\mathbf{K}_2\mathbf{M}_2) + \text{tr}((\mathbf{S} - \mathbf{K}_1 - \mathbf{K}_2)\mathbf{M}_S) \end{aligned} \tag{10.88}$$

where $\lambda \geq 0, \mu \geq 0$, $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_S$ are positive semi-definite matrices. Let the maximizer of this optimization problem be $a^*, \mathbf{K}_1^*, \mathbf{K}_2^*$. The necessary KKT conditions

are given by

$$\frac{\partial \mathcal{L}(\mathbf{K}_1, \mathbf{K}_2)}{\partial a}\Big|_{a=a^*} = 0 \tag{10.89}$$

$$\nabla_{\mathbf{K}_1} \mathcal{L}(\mathbf{K}_1, \mathbf{K}_2)\big|_{\mathbf{K}_1=\mathbf{K}_1^*} = \mathbf{0} \tag{10.90}$$

$$\nabla_{\mathbf{K}_2} \mathcal{L}(\mathbf{K}_1, \mathbf{K}_2)\big|_{\mathbf{K}_2=\mathbf{K}_2^*} = \mathbf{0} \tag{10.91}$$

$$\lambda(R_{S1}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) - a^*) = 0 \tag{10.92}$$

$$\mu(R_{S2}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) - a^*) = 0 \tag{10.93}$$

$$\mathrm{tr}(\mathbf{K}_1^* \mathbf{M}_1) = 0 \tag{10.94}$$

$$\mathrm{tr}(\mathbf{K}_2^* \mathbf{M}_2) = 0 \tag{10.95}$$

$$\mathrm{tr}((\mathbf{S} - \mathbf{K}_1^* - \mathbf{K}_2^*)\mathbf{M}_S) = 0 \tag{10.96}$$

The first condition in (10.89) implies $\lambda + \mu = 1$. From now on, we set $\mu = \bar{\lambda} = 1 - \lambda$. The second and third KKT conditions in (10.90) and (10.91) yield

$$\lambda(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 = \lambda(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{10.97}$$

$$\bar{\lambda}(\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} - \bar{\lambda}(\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_2 = \lambda(\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} - \lambda(\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_1 \tag{10.98}$$

The KKT conditions in (10.94), (10.95), (10.96) yield

$$\mathbf{K}_1^* \mathbf{M}_1 = \mathbf{M}_1 \mathbf{K}_1^* = \mathbf{0} \tag{10.99}$$

$$\mathbf{K}_2^* \mathbf{M}_2 = \mathbf{M}_2 \mathbf{K}_2^* = \mathbf{0} \tag{10.100}$$

$$(\mathbf{S} - \mathbf{K}_1^* - \mathbf{K}_2^*)\mathbf{M}_S = \mathbf{M}_S(\mathbf{S} - \mathbf{K}_1^* - \mathbf{K}_2^*) = \mathbf{0} \tag{10.101}$$

We treat cases $\lambda = 0, \lambda = 1, 0 < \lambda < 1$ separately.

$\underline{\lambda = 0}$: In this case, the conditions in (10.97) and (10.98) reduce to

$$\mathbf{M}_1 = \mathbf{M}_S \tag{10.102}$$

$$(\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \mathbf{M}_2 = (\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_1 \tag{10.103}$$

Furthermore, achievable secrecy rate is given by

$$R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) = \frac{1}{2}\log\frac{|\mathbf{K}_2^* + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2^* + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.104}$$

We now enhance the second user's channel as

$$(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_2)^{-1} = (\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \mathbf{M}_2 \tag{10.105}$$

This new noise covariance matrix $\tilde{\mathbf{\Sigma}}_2$ has some important properties which are given in the following lemma.

Lemma 10.2 *We have the following facts.*

- $\tilde{\mathbf{\Sigma}}_2 \preceq \mathbf{\Sigma}_2$
- $\tilde{\mathbf{\Sigma}}_2 \preceq \mathbf{\Sigma}_Z$
- $(\mathbf{S} + \tilde{\mathbf{\Sigma}}_2)(\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2)^{-1} = (\mathbf{S} + \mathbf{\Sigma}_Z)(\mathbf{K}_2 + \mathbf{\Sigma}_Z)^{-1}$

- $(\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2)^{-1}\tilde{\mathbf{\Sigma}}_2 = (\mathbf{K}_2 + \mathbf{\Sigma}_2)^{-1}\mathbf{\Sigma}_2$

The proof of this lemma is given in Appendix 10.6.5. We are now ready to complete the part of the proof for $\lambda = 0$. To this end, we consider the following Gaussian MIMO wiretap channel

$$\tilde{\mathbf{Y}}_2 = \mathbf{X} + \tilde{\mathbf{N}}_2 \tag{10.106}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{10.107}$$

where the covariance matrix of the Gaussian noise vector $\tilde{\mathbf{N}}_2$ is $\tilde{\mathbf{\Sigma}}_2$. We have $\tilde{\mathbf{\Sigma}}_2 \preceq \mathbf{\Sigma}_Z$, i.e., this wiretap channel is degraded, and its secrecy capacity $\tilde{C}_{S2}(\mathbf{S})$ is [21]

$$\tilde{C}_{S2} = \frac{1}{2}\log\frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.108}$$

Furthermore, we have

$$\begin{aligned}
\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} &\leq C_{S2}(\mathbf{S}) && (10.109)\\
&\leq \tilde{C}_{S2}(\mathbf{S}) && (10.110)\\
&= \frac{1}{2}\log\frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (10.111)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (10.112)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (10.113)\\
&= R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) && (10.114)
\end{aligned}$$

where (10.112) is due to the third part of Lemma 10.2, and (10.113) comes from the fourth part of Lemma 10.2.

$\underline{\lambda = 1:}$ In this case, the conditions in (10.97) and (10.98) reduce to

$$(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 = (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{10.115}$$

$$(\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 = (\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_2 \tag{10.116}$$

Furthermore, the achievable secrecy rate is given by

$$R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) = \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_Z|} \tag{10.117}$$

We now enhance the first user's channel as follows

$$(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = (\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 \tag{10.118}$$

This new noise covariance matrix $\tilde{\mathbf{\Sigma}}_1$ has some important properties which are given in the following lemma.

Lemma 10.3 *We have the following facts.*

- $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_1$
- $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_Z$
- $(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1$
- $(\mathbf{S} + \tilde{\mathbf{\Sigma}}_1)(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = (\mathbf{S} + \mathbf{\Sigma}_Z)(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1}$

- $(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1}\tilde{\mathbf{\Sigma}}_1 = (\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1}\mathbf{\Sigma}_Z$

- $(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1}(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1) = (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1)$.

The proof of this lemma is given in Appendix 10.6.6. We are now ready to complete the part of the proof for the case $\lambda = 1$. To this end, we consider the following Gaussian MIMO wiretap channel

$$\tilde{\mathbf{Y}}_1 = \mathbf{X} + \tilde{\mathbf{N}}_1 \tag{10.119}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{10.120}$$

where the covariance matrix of the Gaussian random vector $\tilde{\mathbf{N}}_1$ is $\tilde{\mathbf{\Sigma}}_1$. We have $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_Z$, i.e., the channel is degraded, and its secrecy capacity $\tilde{C}_{S1}(\mathbf{S})$ is [21]

$$\tilde{C}_{S1}(\mathbf{S}) = \frac{1}{2}\log\frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_1|}{|\tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.121}$$

We have

$$\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \leq C_{S1}(\mathbf{S}) \tag{10.122}$$

$$\leq \tilde{C}_{S1}(\mathbf{S}) \tag{10.123}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_1|}{|\tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.124}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1|}{|\tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.125}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1|}{|\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_Z|} \tag{10.126}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}_2^* + \mathbf{\Sigma}_Z|} \tag{10.127}$$

$$= R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) \tag{10.128}$$

where (10.125), (10.126) and (10.127) are due to the fourth, fifth and sixth parts of Lemma 10.3, respectively.

$\underline{0 < \lambda < 1:}$ In this case, the KKT conditions in (10.97) and (10.98) remain to be the same. The achievable secrecy rate in this case is given by

$$R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) = R_{S1}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) = R_{S2}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) \tag{10.129}$$

We enhance both legitimate users' channels as follows

$$\lambda(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = \lambda(\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1 \tag{10.130}$$

$$\bar{\lambda}(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_2)^{-1} = \bar{\lambda}(\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \mathbf{M}_2 \tag{10.131}$$

We now present the following lemma which lists the important properties of these new noise covariance matrices $\tilde{\mathbf{\Sigma}}_1, \tilde{\mathbf{\Sigma}}_2$.

Lemma 10.4 *We have the following facts.*

- $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_1, \tilde{\mathbf{\Sigma}}_2 \preceq \mathbf{\Sigma}_2$
- $\lambda(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = \lambda(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1$
- $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_Z, \tilde{\mathbf{\Sigma}}_2 \preceq \mathbf{\Sigma}_Z$

- $$\tilde{\mathbf{\Sigma}}_1 \begin{cases} \preceq \tilde{\mathbf{\Sigma}}_2 & \text{if } \lambda < 0.5 \\ = \tilde{\mathbf{\Sigma}}_2 & \text{if } \lambda = 0.5 \\ \succeq \tilde{\mathbf{\Sigma}}_2 & \text{if } \lambda > 0.5 \end{cases}$$

- $(\mathbf{S} + \tilde{\mathbf{\Sigma}}_1)(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = (\mathbf{S} + \mathbf{\Sigma}_Z)(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1}$

- $(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1}(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1) = (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1)$

- $(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_2)^{-1}\tilde{\mathbf{\Sigma}}_2 = (\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1}\mathbf{\Sigma}_2$

The proof of this lemma is given in Appendix 10.6.7. We are now ready to complete the part of the proof for $0 < \lambda < 1$. We first consider $0 < \lambda \leq 0.5$. We introduce the following Gaussian MIMO wiretap channel

$$\tilde{\mathbf{Y}}_2 = \mathbf{X} + \tilde{\mathbf{N}}_2 \tag{10.132}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{10.133}$$

where the covariance matrix of the Gaussian random vector $\tilde{\mathbf{N}}_2$ is $\tilde{\mathbf{\Sigma}}_2$. Since $\tilde{\mathbf{\Sigma}}_2 \preceq \mathbf{\Sigma}_Z$, i.e., the channel is degraded, its secrecy capacity $\tilde{C}_{S2}(\mathbf{S})$ is given by

$$\tilde{C}_{S2}(\mathbf{S}) = \frac{1}{2}\log\frac{|\mathbf{S} + \tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.134}$$

We have

$$\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \leq C_{S2}(\mathbf{S}) \tag{10.135}$$

$$\leq \tilde{C}_{S2}(\mathbf{S}) \tag{10.136}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S}+\tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.137}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S}+\tilde{\mathbf{\Sigma}}_2|}{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_2|} + \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.138}$$

$$\leq \frac{1}{2}\log\frac{|\mathbf{S}+\tilde{\mathbf{\Sigma}}_1|}{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|} + \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.139}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|}{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|} + \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.140}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1|}{|\mathbf{K}_2^*+\mathbf{\Sigma}_1|} + \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.141}$$

$$\begin{aligned} &= \left[\frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1|}{|\mathbf{K}_2^*+\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}\right] \\ &\quad + \left[\frac{1}{2}\log\frac{|\mathbf{K}_2^*+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \end{aligned} \tag{10.142}$$

$$= R_{S1}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) + R_{S2}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) \tag{10.143}$$

$$= 2R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) \tag{10.144}$$

where (10.139) comes from the fact that

$$\frac{|\mathbf{A}+\mathbf{B}|}{|\mathbf{A}|} \geq \frac{|\mathbf{A}+\mathbf{B}+\mathbf{\Delta}|}{|\mathbf{A}+\mathbf{\Delta}|} \tag{10.145}$$

for $\mathbf{A} \succ \mathbf{0}, \mathbf{B} \succeq \mathbf{0}, \mathbf{\Delta} \succeq \mathbf{0}$, and $\tilde{\mathbf{\Sigma}}_1 \preceq \tilde{\mathbf{\Sigma}}_2$, (10.140) comes from the fifth part of Lemma 10.4, (10.141) is due to the sixth and seventh parts of Lemma 10.4.

We now consider the case $0.5 > \lambda$. To this end, we first introduce the following

Gaussian MIMO wiretap channel

$$\tilde{\mathbf{Y}}_1 = \mathbf{X} + \tilde{\mathbf{N}}_1 \tag{10.146}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{10.147}$$

where the covariance matrix of the Gaussian random vector $\tilde{\mathbf{N}}_1$ is $\tilde{\mathbf{\Sigma}}_1$. Since $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_Z$, i.e., the channel is degraded, its secrecy capacity $\tilde{C}_{S1}(\mathbf{S})$ is given by [21]

$$\tilde{C}_{S1}(\mathbf{S}) = \frac{1}{2}\log\frac{|\mathbf{S}+\tilde{\mathbf{\Sigma}}_1|}{|\tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.148}$$

We have

$$\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \le C_{S1}(\mathbf{S}) \tag{10.149}$$

$$\le \tilde{C}_{S1}(\mathbf{S}) \tag{10.150}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S}+\tilde{\mathbf{\Sigma}}_1|}{|\tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.151}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|}{|\tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.152}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|}{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|} + \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|}{|\tilde{\mathbf{\Sigma}}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.153}$$

$$\le \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|}{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1|} + \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_2|}{|\tilde{\mathbf{\Sigma}}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.154}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1|}{|\mathbf{K}_2^*+\mathbf{\Sigma}_1|} + \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.155}$$

$$= \left[\frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1|}{|\mathbf{K}_2^*+\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}\right] + \left[\frac{1}{2}\log\frac{|\mathbf{K}_2^*+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{K}_2^*+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}\right] \tag{10.156}$$

$$= R_{S1}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) + R_{S2}^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) \tag{10.157}$$

$$= 2R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) \tag{10.158}$$

where (10.152) comes from the fifth part of Lemma 10.4, (10.154) comes from (10.145) and the fact that $\tilde{\mathbf{\Sigma}}_2 \preceq \tilde{\mathbf{\Sigma}}_1$, and (10.155) is due to the sixth and seventh parts of Lemma 10.4. Thus, in view of (10.114), (10.128), (10.144), (10.158), we showed that

$$\min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \leq 2R_S^{12}(\mathbf{K}_1^*, \mathbf{K}_2^*) \tag{10.159}$$

which completes the proof of this theorem.

10.6.5 Proof of Lemma 10.2

The first two statements of Lemma 10.2 are rather straightforward to show. We now show the third statement. For that purpose, we note that

$$(\mathbf{S} - \mathbf{K}_2)\mathbf{M}_1 = (\mathbf{S} - \mathbf{K}_1 - \mathbf{K}_2)\mathbf{M}_1 \tag{10.160}$$

$$= (\mathbf{S} - \mathbf{K}_1 - \mathbf{K}_2)\mathbf{M}_S \tag{10.161}$$

$$= \mathbf{0} \tag{10.162}$$

where (10.160) is due to (10.99), (10.161) comes from (10.102), and (10.162) is due to (10.101). Furthermore, we note that the new noise covariance matrix satisfies

$$(\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2)^{-1} = (\mathbf{K}_2 + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_1 \tag{10.163}$$

which is a consequence of (10.103) and (10.105). Equations (10.162) and (10.163) imply

$$(\mathbf{S} - \mathbf{K}_2)(\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2)^{-1} = (\mathbf{S} - \mathbf{K}_2)(\mathbf{K}_2 + \mathbf{\Sigma}_Z)^{-1} \tag{10.164}$$

which implies which is the desired identity, i.e.,

$$(\mathbf{S} + \mathbf{\Sigma}_2)(\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2)^{-1} = (\mathbf{S} + \mathbf{\Sigma}_Z)(\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_Z)^{-1} \tag{10.165}$$

We now consider the fourth item in the lemma as follows

$$\begin{aligned}
(\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2)^{-1}\tilde{\mathbf{\Sigma}}_2 &= \mathbf{I} - (\mathbf{K}_2 + \tilde{\mathbf{\Sigma}}_2)^{-1}\mathbf{K}_2 && (10.166)\\
&= \mathbf{I} - \left[(\mathbf{K}_2 + \mathbf{\Sigma}_2)^{-1} + \mathbf{M}_2\right]\mathbf{K}_2 && (10.167)\\
&= \mathbf{I} - (\mathbf{K}_2 + \mathbf{\Sigma}_2)^{-1}\mathbf{K}_2 && (10.168)\\
&= (\mathbf{K}_2 + \mathbf{\Sigma}_2)^{-1}\mathbf{\Sigma}_2 && (10.169)
\end{aligned}$$

where (10.167) is due to (10.105), (10.168) comes from (10.100).

10.6.6 Proof of Lemma 10.3

The first two statements of this lemma are rather straightforward to show. We consider the third statement as follows

$$\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1 = \mathbf{K}_1^* + \left[(\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} \tag{10.170}$$

$$= \mathbf{K}_1^* + \left[\mathbf{I} + (\mathbf{K}_2^* + \mathbf{\Sigma}_1)\mathbf{M}_1\right]^{-1} (\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{10.171}$$

$$= \mathbf{K}_1^* + \left[\mathbf{I} + (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)\mathbf{M}_1\right]^{-1} (\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{10.172}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{10.173}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1 - \mathbf{K}_1^*) \tag{10.174}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}\mathbf{K}_1^* \tag{10.175}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right] \mathbf{K}_1^* \tag{10.176}$$

$$= \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \mathbf{M}_1\right]^{-1} \tag{10.177}$$

where (10.170) is due to (10.118), (10.172) and (10.176) comes from (10.99). We now show the fourth statement of the lemma. To this end, we note that (10.115) and the third part of the lemma implies

$$(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{10.178}$$

which, in turn, implies

$$(\mathbf{S}-\mathbf{K}_1^*-\mathbf{K}_2^*)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1)^{-1}=(\mathbf{S}-\mathbf{K}_1^*-\mathbf{K}_2^*)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z)^{-1} \quad (10.179)$$

due to (10.101). Equation (10.179) implies the desired identity

$$(\mathbf{S}+\tilde{\mathbf{\Sigma}}_1)(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1)^{-1}=(\mathbf{S}+\mathbf{\Sigma}_Z)(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_Z)^{-1} \quad (10.180)$$

We now show the fifth statement of the lemma as follows

$$\begin{aligned}(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1)^{-1}\tilde{\mathbf{\Sigma}}_1 &= \mathbf{I}-(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1)^{-1}\mathbf{K}_2 && (10.181)\\ &= \mathbf{I}-\left[(\mathbf{K}_2^*+\mathbf{\Sigma}_Z)^{-1}+\mathbf{M}_2\right]\mathbf{K}_2 && (10.182)\\ &= \mathbf{I}-(\mathbf{K}_2^*+\mathbf{\Sigma}_Z)^{-1}\mathbf{K}_2 && (10.183)\\ &= (\mathbf{K}_2^*+\mathbf{\Sigma}_Z)^{-1}\mathbf{\Sigma}_Z && (10.184)\end{aligned}$$

where (10.182) comes from (10.116) and (10.118), and (10.183) is due to (10.100). We now show the last statement of the lemma as follows

$$\begin{aligned}(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1)^{-1}(\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1) &= \mathbf{I}-(\mathbf{K}_1^*+\mathbf{K}_2^*+\tilde{\mathbf{\Sigma}}_1)^{-1}\mathbf{K}_1^* && (10.185)\\ &= \mathbf{I}-\left[(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}+\mathbf{M}_1\right]\mathbf{K}_1^* && (10.186)\\ &= \mathbf{I}-(\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}\mathbf{K}_1^* && (10.187)\\ &= (\mathbf{K}_1^*+\mathbf{K}_2^*+\mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^*+\mathbf{\Sigma}_1) && (10.188)\end{aligned}$$

where (10.186) comes from the third part of the lemma, and (10.187) is due to (10.99).

10.6.7 Proof of Lemma 10.4

The first statement is straightforward to show. The proof of the second statement goes as follows

$$\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1 = \mathbf{K}_1^* + \left[(\mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1} \tag{10.189}$$

$$= \mathbf{K}_1^* + \left[\mathbf{I} + \frac{1}{\lambda}(\mathbf{K}_2^* + \mathbf{\Sigma}_1)\mathbf{M}_1\right]^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{10.190}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{10.191}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1 - \mathbf{K}_1^*) \tag{10.192}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1}(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}\mathbf{K}_1^* \tag{10.193}$$

$$= \mathbf{K}_1^* + \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1}\left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]\mathbf{K}_1^* \tag{10.194}$$

$$= \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]^{-1} \tag{10.195}$$

where (10.189) comes from (10.130), and (10.191) and (10.194) are due to (10.99). We now prove the third statement of the lemma. To this end, we note that using

(10.130), (10.131) and the second part of this lemma in (10.97) and (10.98) yield

$$\lambda(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = \lambda(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_S \tag{10.196}$$

$$\bar{\lambda}(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_2)^{-1} - \bar{\lambda}(\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} = \lambda(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} - \lambda(\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} \tag{10.197}$$

Equation (10.196) implies $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_Z$. Since $\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_Z$, the right hand-side of (10.197) is positive semi-definite. This implies the positive semi-definiteness of the left hand-side of (10.197), which, in turn, implies $\tilde{\mathbf{\Sigma}}_2 \preceq \mathbf{\Sigma}_Z$. We now show the fourth statement of this lemma. If $\lambda = 0.5$, i.e., $\bar{\lambda} = \lambda = 0.5$, we have $\tilde{\mathbf{\Sigma}}_1 = \tilde{\mathbf{\Sigma}}_2$ due to (10.197). If $\lambda < 0.5$, i.e., $\bar{\lambda} > 0.5 > \lambda$, (10.197) yields

$$\lambda(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_2)^{-1} - \lambda(\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} \preceq \lambda(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} - \lambda(\mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} \tag{10.198}$$

which implies $\tilde{\mathbf{\Sigma}}_1 \preceq \tilde{\mathbf{\Sigma}}_2$. The other case $\lambda > 0.5$, i.e., $\lambda > 0.5 > \bar{\lambda}$ yields $\tilde{\mathbf{\Sigma}}_2 \preceq \tilde{\mathbf{\Sigma}}_1$, and this can be shown similarly. We now show the fifth statement of the lemma. Multiplying (10.196) with $\mathbf{S} - \mathbf{K}_1^* - \mathbf{K}_2^*$ yields

$$\lambda(\mathbf{S} - \mathbf{K}_1^* - \mathbf{K}_2^*)(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = \lambda(\mathbf{S} - \mathbf{K}_1^* - \mathbf{K}_2^*)(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} \tag{10.199}$$

due to (10.101). Equation (10.199) implies the desired identity

$$(\mathbf{S} + \tilde{\mathbf{\Sigma}}_1)(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1} = (\mathbf{S} + \mathbf{\Sigma}_Z)(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_Z)^{-1} \tag{10.200}$$

We now prove the sixth statement of this lemma as follows

$$(\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1}(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1) = \mathbf{I} - (\mathbf{K}_1^* + \mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_1)^{-1}\mathbf{K}_1^* \tag{10.201}$$

$$= \mathbf{I} - \left[(\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1} + \frac{1}{\lambda}\mathbf{M}_1\right]\mathbf{K}_1^* \tag{10.202}$$

$$= \mathbf{I} - (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}\mathbf{K}_1^* \tag{10.203}$$

$$= (\mathbf{K}_1^* + \mathbf{K}_2^* + \mathbf{\Sigma}_1)^{-1}(\mathbf{K}_2^* + \mathbf{\Sigma}_1) \tag{10.204}$$

where (10.202) is due to the second part of this lemma, and (10.203) comes from (10.99). We now show the last statement of this lemma as follows

$$(\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_2)^{-1}\tilde{\mathbf{\Sigma}}_2 = \mathbf{I} - (\mathbf{K}_2^* + \tilde{\mathbf{\Sigma}}_2)^{-1}\mathbf{K}_2^* \tag{10.205}$$

$$= \mathbf{I} - \left[(\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1} + \frac{1}{\bar{\lambda}}\mathbf{M}_2\right]\mathbf{K}_2^* \tag{10.206}$$

$$= \mathbf{I} - (\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1}\mathbf{K}_2^* \tag{10.207}$$

$$= (\mathbf{K}_2^* + \mathbf{\Sigma}_2)^{-1}\mathbf{K}_2^* \tag{10.208}$$

where (10.206) is due to (10.131), and (10.207) comes from (10.100).

10.7 Proof of Theorem 10.6

We first note that since the eavesdropper is degraded with respect to the second user, the secrecy capacity of the Gaussian MIMO wiretap channel between the second user

and the eavesdropper is given by [21]

$$C_{S2}(\mathbf{S}) = \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.209}$$

We next note that we can get the following achievable secrecy rate

$$R = \min\{I(V_0;\mathbf{Y}_1) - I(V_0;\mathbf{Z}), I(\mathbf{X};\mathbf{Y}_2) - I(\mathbf{X};\mathbf{Z})\} \tag{10.210}$$

by setting $V_1 = \phi, V_2 = \mathbf{X}$ in Corollary 10.1. Let V_0 be a Gaussian random vector with covariance matrix $\mathbf{S}-\mathbf{K}$, and $\mathbf{X} = V_0+V_0'$ where V_0' is a Gaussian random vector with covariance matrix $\mathbf{K}$, is independent of V_0. Computation of the achievable secrecy rate in (10.210) for this particular choice of $(V_0, \mathbf{X})$ yields

$$R(\mathbf{K}) = \min\left\{\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_1|}{|\mathbf{K}+\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|}, C_{S2}(\mathbf{S})\right\} \tag{10.211}$$

We now consider the maximization of (10.211) over all positive semi-definite matrices $\mathbf{K}$ such that $\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}$. Since $\mathbf{K}$ is involved only in the first term of (10.211), maximizing (10.211) over $\mathbf{K}$ is equivalent to the following maximization

$$\max_{\mathbf{0}\preceq\mathbf{K}\preceq\mathbf{S}} \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_1|}{|\mathbf{K}+\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{10.212}$$

Using Theorem 2 in [8], we have

$$C_{S1}(\mathbf{S}) = \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{10.213}$$

$$= \max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_1|}{|\mathbf{K} + \mathbf{\Sigma}_1|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{K} + \mathbf{\Sigma}_Z|} \tag{10.214}$$

Thus, using (10.214), we get

$$\max_{\mathbf{0} \preceq \mathbf{K} \preceq \mathbf{S}} R(\mathbf{K}) = \min\{C_{S1}(\mathbf{S}), C_{S2}(\mathbf{S})\} \tag{10.215}$$

as an achievable secrecy rate. Since (10.215) is equal to the upper bound on the secrecy capacity of the Gaussian MIMO compound wiretap channel given in Theorem 10.1, this completes the proof.

Chapter 11

Degraded Compound Multi-receiver Wiretap Channels

11.1 Introduction

In this chapter, we generalize the compound wiretap channel we study in Chapter 10 to a multi-user setting by incorporating more than one group of legitimate users (and hence, more than one confidential message) to the channel model.

In particular, we study the degraded compound multi-receiver wiretap channel (DCMRWC) that consists of two groups of users and a group of eavesdroppers, as shown in Figure 11.1. The degradedness of these channels is defined with respect to two fictitious users (see Figure 11.1). In particular, we assume that the first fictitious user is degraded with respect to any user from the first group, and any user from the second group is degraded with respect to the first fictitious user. Similarly, we also assume that the second fictitious user is degraded with respect to any user from the second group, and any eavesdropper is degraded with respect to it. Without eavesdroppers, this channel model reduces to the degraded compound broadcast channel studied in [5].

The presence of these fictitious users brings a conditional independence structure to the channel model, which enables us to define appropriate auxiliary random variables. In turn, these auxiliary random variables involving the fictitious users enable us to obtain single-letter descriptions for the secrecy capacity regions.

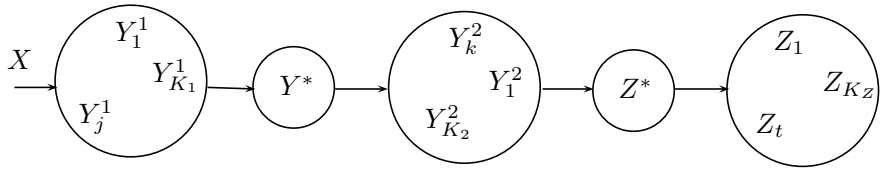

Figure 11.1: The degraded compound multi-receiver wiretap channel.

We study two communication scenarios for the DCMRWC. In the first scenario, which is illustrated in Figure 11.2, the transmitter sends a confidential message to each group of users where these messages should be kept hidden from the eavesdropper. For this scenario, we assume that there exists only one eavesdropper and obtain the secrecy capacity region in a single-letter form for the discrete memoryless setting. Next, we specialize this result to the parallel DCMRWC as well as its Gaussian instance. For the parallel Gaussian case, we use Costa's entropy power inequality [44] to evaluate the secrecy capacity region. Finally, we consider the Gaussian MIMO DCMRWC and obtain its secrecy capacity region when there is only one user in the second group. To obtain the secrecy capacity region for the Gaussian MIMO case, we use our technique that we developed in Chapter 5 to evaluate single-letter descriptions for vector Gaussian models.

In the second scenario illustrated in Figure 11.3, the transmitter sends a confidential message to the users in the first group which needs to be kept confidential from the users in the second group and the eavesdroppers. Moreover, the transmitter sends a different confidential message to the users in the second group, which needs to be kept confidential from the eavesdroppers. If there were only one user in each group and one eavesdropper, this channel model would reduce to the channel

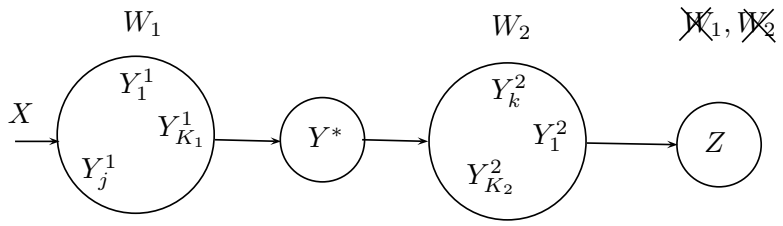

Figure 11.2: The first scenario for the degraded compound multi-receiver wiretap channel.

model that was studied in [45]. Hence, our model can be viewed as a generalization of [45] to a compound setting. Adapting their terminology, we call this channel model the *degraded compound multi-receiver wiretap channel with layered messages* (DCMRWC with layered messages). For this scenario also, we obtain the secrecy capacity region in a single-letter form for a general discrete memoryless setting. Next, we specialize this result to the parallel DCMRWC with layered messages as well as its Gaussian MIMO instance. For the parallel Gaussian case, we again use Costa's entropy power inequality [44] to obtain the secrecy capacity region. Finally, we consider the Gaussian MIMO DCMRWC with layered messages, and evaluate its secrecy capacity region when there is only one user in the second group. For the Gaussian MIMO case, we again use our technique that we developed in Chapter 5.

11.2 System Model

In this chapter, we consider DCMRWC, see Figure 11.1, which consists of two groups of users and a group of eavesdroppers. There are K_1 users in the first group, K_2 users in the second group, and K_Z eavesdroppers. The channel is assumed to be

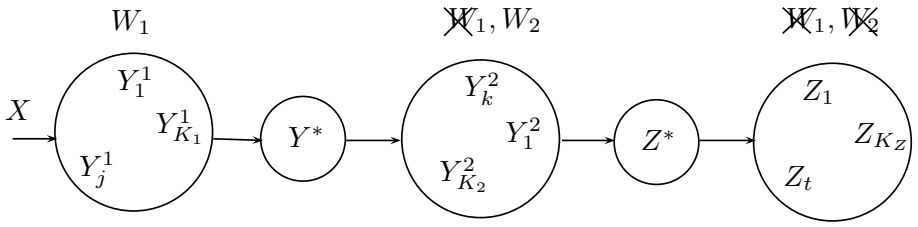

Figure 11.3: The second scenario for the degraded compound multi-receiver wiretap channel.

memoryless with a transition probability

$$p(y_1^1, \ldots, y_{K_1}^1, y_1^2, \ldots, y_{K_2}^2, z_1, \ldots, z_{K_Z}|x) \tag{11.1}$$

where $X \in \mathcal{X}$ is the channel input, $Y_j^1 \in \mathcal{Y}_j^1$ is the channel output of the jth user in the first group, $j = 1, \ldots, K_1$, $Y_k^2 \in \mathcal{Y}_k^2$ is the channel output of the kth user in the second group, $k = 1, \ldots, K_2$, and $Z_t \in \mathcal{Z}_t$ is the channel output of the tth eavesdropper, $t = 1, \ldots, K_Z$.

We assume that there exist two fictitious users with observations $Y^* \in \mathcal{Y}^*, Z^* \in \mathcal{Z}^*$ such that they satisfy the Markov chain

$$X \to Y_j^1 \to Y^* \to Y_k^2 \to Z^* \to Z_t, \quad \forall (j, k, t) \tag{11.2}$$

This Markov chain is the reason why we call the compound multi-receiver wiretap channel we study the *degraded* compound multi-receiver wiretap channel. Actually, there is a slight inexactness in the terminology here because the Markov chain in

(11.2) is more restrictive than the Markov chain

$$X \to Y_j^1 \to Y_k^2 \to Z_t, \quad \forall (j,k,t) \tag{11.3}$$

and it might be more natural to define the degradedness of the compound multi-receiver wiretap channel by the Markov chain in (11.3). However, in this work, we adapt the terminology of the previous work on compound broadcast channels [5], and call the channel satisfying (11.2) the *degraded* compound multi-receiver wiretap channel. Finally, we note that when there are no eavesdroppers, this channel reduces to the degraded compound broadcast channel that was studied in [5].

11.2.1 Parallel DCMRWC

The parallel DCMRWC, where each user's and each eavesdropper's channel consists of L independent sub-channels, i.e.,

$$Y_j^1 = (Y_{j1}^1, \ldots, Y_{jL}^1), \quad j = 1, \ldots, K_1 \tag{11.4}$$

$$Y_k^2 = (Y_{k1}^2, \ldots, Y_{kL}^2), \quad k = 1, \ldots, K_2 \tag{11.5}$$

$$Z_t = (Z_{t1}, \ldots, Z_{tL}), \quad t = 1, \ldots, K_Z \tag{11.6}$$

has the following overall transition probability

$$p(y_1^1, \ldots, y_{K_1}^1, y_1^2, \ldots, y_{K_2}^2, z_1, \ldots, z_{K_Z}|x) = \prod_{\ell=1}^{L} p(y_{1\ell}^1, \ldots, y_{K_1\ell}^1, y_{1\ell}^2, \ldots, y_{K_2\ell}^2, z_{1\ell}, \ldots, z_{K_Z\ell}|x_\ell) \tag{11.7}$$

where $X_\ell,\ \ell = 1, \ldots, L$, is the ℓth sub-channel's input. We define the degradedness of the parallel compound multi-receiver wiretap channel in a similar fashion. In particular, we call a parallel compound multi-receiver wiretap channel degraded, if there exist two sequences of random variables

$$Y^* = (Y_1^*, \ldots, Y_L^*) \tag{11.8}$$

$$Z^* = (Z_1^*, \ldots, Z_L^*) \tag{11.9}$$

which satisfy Markov chains

$$X_\ell \to Y_{j\ell}^1 \to Y_\ell^* \to Y_{k\ell}^2 \to Z_\ell^* \to Z_{t\ell}, \quad \forall (j, k, t, \ell) \tag{11.10}$$

11.2.2 Gaussian Parallel DCMRWC

The Gaussian parallel DCMRWC is defined by

$$\mathbf{Y}_j^1 = \mathbf{X} + \mathbf{N}_j^1, \quad j = 1, \ldots, K_1 \tag{11.11}$$

$$\mathbf{Y}_k^2 = \mathbf{X} + \mathbf{N}_k^2, \quad k = 1, \ldots, K_2 \tag{11.12}$$

$$\mathbf{Z}_t = \mathbf{X} + \mathbf{N}_t^Z, \quad t = 1, \ldots, K_Z \tag{11.13}$$

where all column vectors $\{\mathbf{Y}_j^1\}_{j=1}^{K_1}, \{\mathbf{Y}_k^1\}_{k=1}^{K_2}, \{\mathbf{Z}_t\}_{t=1}^{K_Z}, \mathbf{X}, \{\mathbf{N}_j^1\}_{j=1}^{K_1}, \{\mathbf{N}_k^2\}_{k=1}^{K_2}, \{\mathbf{N}_t^Z\}_{t=1}^{K_Z}$ are of dimensions $L \times 1$. $\{\mathbf{N}_j^1\}_{j=1}^{K_1}, \{\mathbf{N}_k^2\}_{k=1}^{K_2}, \{\mathbf{N}_t^Z\}_{t=1}^{K_Z}$ are Gaussian random vectors with diagonal covariance matrices $\{\mathbf{\Lambda}_j^1\}_{j=1}^{K_1}, \{\mathbf{\Lambda}_k^2\}_{j=1}^{K_2}, \{\mathbf{\Lambda}_t^Z\}_{t=1}^{K_Z}$, respectively. The channel input $\mathbf{X}$ is subject to a trace constraint as

$$E\left[\mathbf{X}^\top \mathbf{X}\right] = \mathrm{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right) \leq P \tag{11.14}$$

In this Chapter, we will be interested in Gaussian parallel *degraded* compound multi-receiver wiretap channels which means that the covariance matrices satisfy the following order

$$\mathbf{\Lambda}_j^1 \preceq \mathbf{\Lambda}_k^2 \preceq \mathbf{\Lambda}_t^Z, \quad \forall (j,k,t) \tag{11.15}$$

Since noise covariance matrices are diagonal, the order in (11.15) implies

$$\Lambda_{j,\ell\ell}^1 \leq \Lambda_{k,\ell\ell}^2 \leq \Lambda_{t,\ell\ell}^Z, \quad \forall (j,k,t,\ell) \tag{11.16}$$

where $\Lambda^1_{j,\ell\ell}, \Lambda^2_{k,\ell\ell}, \Lambda^Z_{t,\ell\ell}$ denote the ℓth diagonal element of $\mathbf{\Lambda}^1_j, \mathbf{\Lambda}^2_k, \mathbf{\Lambda}^Z_t$, respectively.

The diagonality of noise covariance matrices also ensures the existence of diagonal matrices $\mathbf{\Lambda}^*_Y$ and $\mathbf{\Lambda}^*_Z$ such that

$$\mathbf{\Lambda}^1_j \preceq \mathbf{\Lambda}^*_Y \preceq \mathbf{\Lambda}^2_k \preceq \mathbf{\Lambda}^*_Z \preceq \mathbf{\Lambda}^Z_t, \quad \forall (k, j, t) \tag{11.17}$$

For example, we can select $\mathbf{\Lambda}^*_Y$ as $\Lambda^*_{Y,\ell\ell} = \max_{j=1,\ldots,K_1} \Lambda^1_{j,\ell\ell}$ which already satisfies (11.17) because of $\max_{j=1,\ldots,K_1} \Lambda^1_{j,\ell\ell} \leq \min_{k=1,\ldots,K_2} \Lambda^2_{k,\ell\ell}$ which is due to (11.16). Similarly, we can select $\mathbf{\Lambda}^*_Z$. Thus, for Gaussian parallel compound multi-receiver channels, the two possible ways of defining degradedness, i.e., (11.2) and (11.3), are equivalent due to the equivalence of (11.15) and (11.17).

11.2.3 Gaussian MIMO DCMRWC

The Gaussian MIMO DCMRWC is defined by

$$\mathbf{Y}^1_j = \mathbf{X} + \mathbf{N}^1_j, \quad j = 1, \ldots, K_1 \tag{11.18}$$

$$\mathbf{Y}^2_k = \mathbf{X} + \mathbf{N}^2_k, \quad k = 1, \ldots, K_2 \tag{11.19}$$

$$\mathbf{Z}_t = \mathbf{X} + \mathbf{N}^Z_t, \quad t = 1, \ldots, K_Z \tag{11.20}$$

where all column vectors $\{\mathbf{Y}^1_j\}_{j=1}^{K_1}, \{\mathbf{Y}^2_k\}_{k=1}^{K_2}, \{\mathbf{Z}_t\}_{t=1}^{K_Z}, \mathbf{X}, \{\mathbf{N}^1_j\}_{j=1}^{K_1}, \{\mathbf{N}^2_k\}_{k=1}^{K_2}, \{\mathbf{N}^Z_t\}_{t=1}^{K_Z}$ are of dimensions $M \times 1$. $\{\mathbf{N}^1_j\}_{j=1}^{K_1}, \{\mathbf{N}^2_k\}_{k=1}^{K_2}, \{\mathbf{N}^Z_t\}_{t=1}^{K_Z}$ are Gaussian random vectors with covariance matrices $\{\mathbf{\Sigma}^1_j\}_{j=1}^{K_1}, \{\mathbf{\Sigma}^2_k\}_{k=1}^{K_2}, \{\mathbf{\Sigma}^Z_t\}_{t=1}^{K_Z}$, respectively. Unlike in the case of Gaussian parallel channels, these covariance matrices are not necessarily

diagonal. The channel input $\mathbf{X}$ is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S} \tag{11.21}$$

where $\mathbf{S} \succ \mathbf{0}$.

In this Chapter, we study Gaussian MIMO *degraded* compound multi-receiver wiretap channels for which there exist covariance matrices $\mathbf{\Sigma}_Y^*$ and $\mathbf{\Sigma}_Z^*$ such that

$$\mathbf{\Sigma}_j^1 \preceq \mathbf{\Sigma}_Y^* \preceq \mathbf{\Sigma}_k^2 \preceq \mathbf{\Sigma}_Z^* \preceq \mathbf{\Sigma}_t^Z, \quad \forall (j,k,t) \tag{11.22}$$

We note that the order in (11.22), by which we define the degradedness, is more restrictive than the other possible order that can be used to define the degradedness, i.e.,

$$\mathbf{\Sigma}_j^1 \preceq \mathbf{\Sigma}_k^2 \preceq \mathbf{\Sigma}_t^Z, \quad \forall (j,k,t) \tag{11.23}$$

In [5], a specific numerical example is provided to show that the order in (11.23) strictly subsumes the one in (11.22).

11.2.4 Comments on Gaussian MIMO DCMRWC

We provide some comments about the way we define the Gaussian MIMO DCM-RWC. The first one is about the covariance constraint in (11.21). Though it is more common to define capacity regions under a total power constraint, i.e.,

$\text{tr}\left(E\left[\mathbf{X}\mathbf{X}^{\top}\right]\right) \leq P$, the covariance constraint in (11.21) is more general and it subsumes the total power constraint as a special case [4]. In particular, if we denote the secrecy capacity region under the constraint in (11.21) by $C(\mathbf{S})$, then the secrecy capacity region under the trace constraint, $\text{tr}\left(E\left[\mathbf{X}\mathbf{X}^{\top}\right]\right) \leq P$, can be written as [4]

$$C^{\text{trace}}(P) = \bigcup_{\mathbf{S}:\text{tr}(\mathbf{S})\leq P} C(\mathbf{S}) \tag{11.24}$$

The second comment is about our assumption that $\mathbf{S}$ is strictly positive definite. This assumption does not lead to any loss of generality because for any Gaussian MIMO compound multi-receiver wiretap channel with a positive semi-definite covariance constraint, i.e., $\mathbf{S} \succeq \mathbf{0}$ and $|\mathbf{S}| = 0$, we can always construct an equivalent channel with the constraint $E\left[\mathbf{X}\mathbf{X}^{\top}\right] \preceq \mathbf{S}'$ where $\mathbf{S}' \succ \mathbf{0}$ (see Lemma 2 of [4]), which has the same secrecy capacity region.

The last comment is about the assumption that the transmitter and all receivers have the same number of antennas. This assumption is implicit in the channel definition, see (11.18)-(11.20), and also in the definition of degradedness, see (11.22). However, we can extend the definition of the Gaussian MIMO DCMRWC to include the cases where the number of transmit antennas and the number of receive antennas at each receiver are not necessarily the same. To this end, we first

introduce the following channel model

$$\mathbf{Y}_j^1 = \mathbf{H}_j^1\mathbf{X} + \mathbf{N}_j^1, \quad j = 1, \ldots, K_1 \tag{11.25}$$

$$\mathbf{Y}_k^2 = \mathbf{H}_k^2\mathbf{X} + \mathbf{N}_k^2, \quad k = 1, \ldots, K_2 \tag{11.26}$$

$$\mathbf{Z}_t = \mathbf{H}_t^Z\mathbf{X} + \mathbf{N}_t^Z, \quad t = 1, \ldots, K_Z \tag{11.27}$$

where $\mathbf{H}_j^1, \mathbf{H}_k^2, \mathbf{H}_t^Z$ are the channel matrices of sizes $r_j^1 \times t, r_k^2 \times t, r_t^Z \times t$, respectively, and $\mathbf{X}$ is of size $t \times 1$. The channel outputs $\mathbf{Y}_j^1, \mathbf{Y}_k^2, \mathbf{Z}_t$ are of sizes $r_j^1 \times 1, r_k^2 \times 1, r_t^Z \times 1$, respectively. The Gaussian noise vectors $\mathbf{N}_j^1, \mathbf{N}_k^2, \mathbf{N}_t^Z$ are assumed to have identity covariance matrices.

To define degradedness for the channel model given in (11.25)-(11.27), we need the following definition from [5]: A receive vector $\mathbf{Y}_a = \mathbf{H}_a\mathbf{X} + \mathbf{N}_a$ of size $r_a \times 1$ is said to be degraded with respect to $\mathbf{Y}_b = \mathbf{H}_b\mathbf{X} + \mathbf{N}_b$ of size $r_b \times 1$, if there exists a matrix $\mathbf{D}$ of size $r_a \times r_b$ such that $\mathbf{D}\mathbf{H}_b = \mathbf{H}_a$ and $\mathbf{D}\mathbf{D}^\top \preceq \mathbf{I}$. Using this equivalent definition of degradedness, we now give the equivalent definition of degradedness for the channel model in (11.25)-(11.27). To this end, we first introduce two fictitious users with observations $\mathbf{Y}^*$ and $\mathbf{Z}^*$, which are given by

$$\mathbf{Y}^* = \mathbf{H}_Y^*\mathbf{X} + \mathbf{N}_Y^* \tag{11.28}$$

$$\mathbf{Z}^* = \mathbf{H}_Z^*\mathbf{X} + \mathbf{N}_Z^* \tag{11.29}$$

The Gaussian MIMO compound multi-receiver wiretap channel in (11.25)-(11.27) is said to be degraded if the following two conditions hold: i) $\mathbf{Y}^*$ is degraded with

respect to any user from the first group, and any user from the second group is degraded with respect to $\mathbf{Y}^*$, and ii) $\mathbf{Z}^*$ is degraded with respect to any user from the second group, and any eavesdropper is degraded with respect to $\mathbf{Z}^*$, where degradedness here is with respect to the definition given above.

In the rest of this chapter, we consider the channel model given in (11.18)-(11.20) instead of the channel model given in (11.25)-(11.27), which is more general. However, if we establish the secrecy capacity region for the Gaussian MIMO DCMRWC defined by (11.18)-(11.20), we can also obtain the secrecy capacity region for the general Gaussian MIMO DCMRWC defined by (11.25)-(11.27) using the analysis carried out in Section V of [5] and in Chapter 5.7. Since this analysis is quite standard and can be found in other works cited above, whenever we have a capacity result for the Gaussian MIMO DCMRWC defined by (11.18)-(11.20), we provide the extension of this capacity result to the general Gaussian MIMO DCMRWC defined by (11.25)-(11.27) without a proof.

11.3 Problem Statement and Main Results

In this chapter, we consider two different communication scenarios for the DCMRWC.

11.3.1 The First Scenario: External Eavesdroppers

In the first scenario, the transmitter wants to send a confidential message to users in the first group and a different confidential message to users in the second group,

where both messages need to be kept confidential from the eavesdroppers. In this case, we assume that there is only one eavesdropper, i.e., $K_Z = 1$. The graphical illustration of the first scenario is given in Figure 11.2.

An $(n, 2^{nR_1}, 2^{nR_2})$ code for the first scenario consists of two message sets $\mathcal{W}_1 = \{1, \ldots, 2^{nR_1}\}, \mathcal{W}_2 = \{1, \ldots, 2^{nR_2}\}$, an encoder $f : \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, one decoder for each legitimate user in the first group $g_j^1 : \mathcal{Y}_j^{1,n} \to \mathcal{W}_1,\ j = 1, \ldots, K_1$, and one decoder for each legitimate user in the second group $g_k^2 : \mathcal{Y}_k^{2,n} \to \mathcal{W}_2,\ k = 1, \ldots, K_2$. The probability of error is defined as $P_e^n = \max\{P_e^{1,n}, P_e^{2,n}\}$ where $P_e^{1,n}$ and $P_e^{2,n}$ are given by

$$P_e^{1,n} = \max_{j \in \{1,\ldots,K_1\}} \Pr\left[g_j^1\left(Y_j^{1,n}\right) \neq W_1\right] \tag{11.30}$$

$$P_e^{2,n} = \max_{k \in \{1,\ldots,K_2\}} \Pr\left[g_k^2\left(Y_k^{2,n}\right) \neq W_2\right] \tag{11.31}$$

A secrecy rate pair (R_1, R_2) is said to be achievable if there exists an $(n, 2^{nR_1}, 2^{nR_2})$ code which has $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} I(W_1, W_2; Z^n) = 0 \tag{11.32}$$

where we dropped the subscript of Z_t since $K_Z = 1$. We note that (11.32) implies

$$\lim_{n\to\infty} \frac{1}{n} I(W_1; Z^n) = 0 \qquad \text{and} \qquad \lim_{n\to\infty} \frac{1}{n} I(W_2; Z^n) = 0 \tag{11.33}$$

From these definitions, it is clear that we are only interested in perfect secrecy rates

of the channel. The secrecy capacity region is defined as the closure of all achievable secrecy rate pairs. A single-letter characterization of the secrecy capacity region is given as follows.

Theorem 11.1 *The secrecy capacity region of the DCMRWC is given by the union of rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \min_{j=1,\ldots,K_1} I(X; Y_j^1 | U, Z) \tag{11.34}$$

$$R_2 \leq \min_{k=1,\ldots,K_2} I(U; Y_k^2 | Z) \tag{11.35}$$

where the union is over all (U, X) *such that*

$$U \to X \to Y_j^1 \to Y^* \to Y_k^2 \to Z \tag{11.36}$$

for any (j, k) *pair.*

Showing the achievability of this region is rather standard, thus is omitted here. We provide the converse proof in Appendix 11.5.1. The presence of the fictitious user with observation Y^* proves to be crucial in the converse proof. Essentially, it brings a conditional independence structure to the channel, which enables us to define the auxiliary random variable U, which, in turn, provides the converse proof.

As a side note, if we disable the eavesdropper by setting $Z = \phi$, the region in Theorem 11.1 reduces to the capacity region of the underlying degraded compound broadcast channel which was established in [5].

11.3.1.1 Parallel DCMRWC

In the upcoming section, we will consider the Gaussian parallel DCMRWC. For that purpose, here, we provide the secrecy capacity region of the parallel DCMRWC in a single-letter form.

Theorem 11.2 *The secrecy capacity region of the parallel DCMRWC is given by the union of rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1 | U_\ell, Z_\ell) \tag{11.37}$$

$$R_2 \leq \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U_\ell; Y_{k\ell}^2 | Z_\ell) \tag{11.38}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$ *such that*

$$U_\ell \to X_\ell \to Y_{j\ell}^1 \to Y_\ell^* \to Y_{k\ell}^2 \to Z_\ell \tag{11.39}$$

for any (j, k, ℓ) *triple.*

Though Theorem 11.1 provides the secrecy capacity region for a rather general channel model including the parallel DCMRWC as a special case, we still need a converse proof to show that the region in Theorem 11.1 reduces to the region in Theorem 11.2 for parallel channels. In other words, we still need to show the optimality of independent signalling on each sub-channel. This proof is provided in Appendix 11.5.2.

11.3.1.2 Gaussian Parallel DCMRWC

We now obtain the secrecy capacity region of the Gaussian parallel DCMRWC. To that end, we need to evaluate the region given in Theorem 11.2, i.e., we need to find the optimal joint distribution $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. We first introduce the following theorem which will be instrumental in evaluating the region in Theorem 11.2 for Gaussian parallel channels.

Theorem 11.3 *Let N_1, N^*, N_2, N_Z be zero-mean Gaussian random variables with variances $\sigma_1^2, \sigma_*^2, \sigma_2^2, \sigma_Z^2$, respectively, where*

$$\sigma_1^2 \leq \sigma_*^2 \leq \sigma_2^2 \leq \sigma_Z^2 \tag{11.40}$$

Let (U, X) be an arbitrarily dependent random variable pair, which is independent of (N_1, N^*, N_2, N_Z), and the second-moment of X be constrained as $E[X^2] \leq P$. Then, for any feasible (U, X), we can find a $P^* \leq P$ such that

$$h(X + N_Z|U) - h(X + N^*|U) = \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_*^2} \tag{11.41}$$

and

$$h(X + N_Z|U) - h(X + N_1|U) \geq \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_1^2} \tag{11.42}$$

$$h(X + N_Z|U) - h(X + N_2|U) \leq \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_2^2} \tag{11.43}$$

for any (σ_1^2, σ_2^2) satisfying the order in (11.40).

The proof of this theorem is provided in Appendix 11.5.3. In this proof, Costa's entropy power inequality [44] plays a key role.

We now establish the secrecy capacity region of the Gaussian parallel DCMRWC.

Theorem 11.4 *The secrecy capacity region of the Gaussian parallel DCMRWC is given by the union of rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} \frac{1}{2} \log\left(1 + \frac{\beta_\ell P_\ell}{\Lambda^1_{j,\ell\ell}}\right) - \frac{1}{2}\log\left(1 + \frac{\beta_\ell P_\ell}{\Lambda_{Z,\ell\ell}}\right) \tag{11.44}$$

$$R_2 \leq \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} \frac{1}{2} \log\left(1 + \frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda^2_{k,\ell\ell}}\right) - \frac{1}{2}\log\left(1 + \frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda_{Z,\ell\ell}}\right) \tag{11.45}$$

where the union is over all $\{P_\ell\}_{\ell=1}^{L}$ *such that* $\sum_{\ell=1}^{L} P_\ell = P$ *and* $\bar{\beta}_\ell = 1 - \beta_\ell \in [0,1],\ \ell = 1, \ldots, L$.

The proof of this theorem is provided in Appendix 11.5.4. Here, P_ℓ denotes the part of the total available power P which is devoted to the transmission in the ℓth sub-channel. Furthermore, β_ℓ denotes the fraction of the power P_ℓ of the ℓth sub-channel spent for the transmission to users in the first group.

11.3.1.3 Gaussian MIMO DCMRWC

In this section, we first obtain the secrecy capacity region of the Gaussian MIMO DCMRWC when $K_2 = 1$. To that end, we need to evaluate the region given in Theorem 11.1. In other words, we need to find the optimal random variable pair $(U, \mathbf{X})$. We are able to do this when there is only one user in the second group, i.e.,

$K_2 = 1$. For this, we need the following theorem.

Theorem 11.5 ([Chapter 5, Theorem 5.7]) *Let* $(\mathbf{N}_1, \mathbf{N}^*, \mathbf{N}_Z)$ *be zero-mean Gaussian random vectors with covariance matrices* $\mathbf{\Sigma}_1, \mathbf{\Sigma}^*, \mathbf{\Sigma}_Z$*, respectively, where*

$$\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}^* \preceq \mathbf{\Sigma}_Z \tag{11.46}$$

Let $(U, \mathbf{X})$ *be arbitrarily dependent random vector, which is independent of* $(\mathbf{N}_1, \mathbf{N}^*, \mathbf{N}_Z)$*, and let the second moment of* $\mathbf{X}$ *be constrained as* $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$*. Then, for any feasible* $(U, \mathbf{X})$*, we can find a positive semi-definite matrix* $\mathbf{K}^*$ *such that* $\mathbf{K}^* \preceq \mathbf{S}$*, and it satisfies*

$$h(\mathbf{X} + \mathbf{N}_Z|U) - h(\mathbf{X} + \mathbf{N}^*|U) = \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}^*|} \tag{11.47}$$

and

$$h(\mathbf{X} + \mathbf{N}_Z|U) - h(\mathbf{X} + \mathbf{N}_1|U) \geq \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_1|} \tag{11.48}$$

for any $\mathbf{\Sigma}_1$ *satisfying the order in (11.46).*

Using this theorem, we can establish the secrecy capacity region of the Gaussian MIMO DCMRWC when $K_2 = 1$ as follows.

Theorem 11.6 *The secrecy capacity region of the Gaussian MIMO DCMRWC*

when $K_2 = 1$ is given by the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j=1,\ldots,K_1} \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{11.49}$$

$$R_2 \leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}^2|}{|\mathbf{K} + \mathbf{\Sigma}^2|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{K} + \mathbf{\Sigma}_Z|} \tag{11.50}$$

where we dropped the subscript of $\mathbf{\Sigma}_k^2$ since $K_2 = 1$, and the union is over all positive semi-definite matrices $\mathbf{K}$ such that $\mathbf{K} \preceq \mathbf{S}$.

The proof of this theorem is given in Appendix 11.5.5. Now, we would like to comment about why we can obtain the secrecy capacity region of the Gaussian MIMO DCMRWC only when $K_2 = 1$. The reason is that we can extend Theorem 11.3, which was used to obtain the secrecy capacity region of the Gaussian parallel DCMRWC, to vector case in Theorem 11.5 partially, i.e., not completely. In particular, we could not show that the matrix $\mathbf{K}^*$ in Theorem 11.5 also satisfies

$$h(\mathbf{X} + \mathbf{N}_Z|U) - h(\mathbf{X} + \mathbf{N}_2|U) \leq \frac{1}{2} \log \frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} \tag{11.51}$$

for any Gaussian random vector $\mathbf{N}_2$ with covariance matrix satisfying $\mathbf{\Sigma}^* \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z$. If (11.51) can be shown, the secrecy capacity region of the Gaussian MIMO DCMRWC can be obtained as the union of rate pairs (R_1, R_2) satisfying

$$R_1 \leq \min_{j=1,\ldots,K_1} \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2} \log \frac{|\mathbf{K} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{11.52}$$

$$R_2 \leq \min_{k=1,\ldots,K_2} \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_k^2|}{|\mathbf{K} + \mathbf{\Sigma}_k^2|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{K} + \mathbf{\Sigma}_Z|} \tag{11.53}$$

where the union is over all positive semi-definite matrices $\mathbf{K}$ such that $\mathbf{K} \preceq \mathbf{S}$.

Finally we note that using the analysis carried out in Section V of [5] and Chapter 5.7, the capacity result given in Theorem 11.6 can be extended to the general Gaussian MIMO DCMRWC defined by (11.25)-(11.27) as follows.

Corollary 11.1 *The secrecy capacity region of the general Gaussian MIMO DCM-RWC, which is defined by (11.25)-(11.27), when $K_2 = 1$, is given by the union of rate pairs (R_1, R_2) satisfying*

$$R_1 \leq \min_{j=1,\ldots,K_1} \frac{1}{2} \log \frac{|\mathbf{H}_j^1 \mathbf{K} (\mathbf{H}_j^1)^\top + \mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2} \log \frac{|\mathbf{H}_Z \mathbf{K} \mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{11.54}$$

$$R_2 \leq \frac{1}{2} \log \frac{|\mathbf{H}^2 \mathbf{S} (\mathbf{H}^2)^\top + \mathbf{\Sigma}^2|}{|\mathbf{H}^2 \mathbf{K} (\mathbf{H}^2)^\top + \mathbf{\Sigma}^2|} - \frac{1}{2} \log \frac{|\mathbf{H}_Z \mathbf{S} \mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|}{|\mathbf{H}_Z \mathbf{K} \mathbf{H}_Z^\top + \mathbf{\Sigma}_Z|} \tag{11.55}$$

where we dropped the subscripts of $\mathbf{\Sigma}_k^2, \mathbf{H}_k^2$ since $K_2 = 1$, and the union is over all positive semi-definite matrices $\mathbf{K}$ such that $\mathbf{K} \preceq \mathbf{S}$.

11.3.2 The Second Scenario: Layered Confidential Messages

In the second scenario, the transmitter wants to send a confidential message to users in the first group which needs to be kept confidential from the second group of users and eavesdroppers. The transmitter also wants to send a different confidential message to users in the second group, which needs to be kept confidential from the eavesdroppers. As opposed to the first scenario, in this case, we do not put any restriction on the number of eavesdroppers. The graphical illustration of the second scenario is given in Figure 11.3. The situation where there is only one user in each

group and one eavesdropper was investigated in [45]. Hence, this second scenario can be seen as a generalization of the model in [45] to a compound channel setting. Following the terminology of [45], we call this channel model DCMRWC with *layered messages*.

An $(n, 2^{nR_1}, 2^{nR_2})$ code for DCMRWC with *layered messages* consists of two message sets $\mathcal{W}_1 = \{1, \ldots, 2^{nR_1}\}, \mathcal{W}_2 = \{1, \ldots, 2^{nR_2}\}$ and an encoder $f : \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, one decoder for each legitimate user in the first group $g_j^1 : \mathcal{Y}_j^{1,n} \to \mathcal{W}_1,\ j = 1, \ldots, K_1$, and one decoder for each legitimate user in the second group $g_k^2 : \mathcal{Y}_k^{2,n} \to \mathcal{W}_2,\ k = 1, \ldots, K_2$. The probability of error is defined as $P_e^n = \max\{P_e^{1,n}, P_e^{2,n}\}$ where $P_e^{1,n}$ and $P_e^{2,n}$ are given by

$$P_e^{1,n} = \max_{j \in \{1,\ldots,K_1\}} \Pr\left[g_j^1(Y_j^{1,n}) \neq W_1\right] \tag{11.56}$$

$$P_e^{2,n} = \max_{k \in \{1,\ldots,K_2\}} \Pr\left[g_k^2(Y_k^{2,n}) \neq W_2\right] \tag{11.57}$$

A secrecy rate pair is said to be achievable if there exists an $(n, 2^{nR_1}, 2^{nR_2})$ code which has $\lim_{n\to\infty} P_e^n = 0$,

$$\lim_{n\to\infty} \frac{1}{n} I(W_2; Z_t^n) = 0, \quad t = 1, \ldots, K_Z \tag{11.58}$$

and

$$\lim_{n\to\infty} \frac{1}{n} I(W_1; Y_k^{2,n} | W_2) = 0, \quad k = 1, \ldots, K_2 \tag{11.59}$$

We note that these two secrecy conditions imply

$$\lim_{n\to\infty} \frac{1}{n} I(W_1, W_2; Z_t^n) = 0, \quad t = 1, \ldots, K_Z \tag{11.60}$$

Furthermore, it is clear that we are only interested in perfect secrecy rates of the channel. The secrecy capacity region is defined as the closure of all achievable secrecy rate pairs. A single-letter characterization of the secrecy capacity region is given as follows.

Theorem 11.7 *The secrecy capacity region of the DCMRWC with layered messages is given by the union of rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} I(X; Y_j^1 | U, Y_k^2) \tag{11.61}$$

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} I(U; Y_k^2 | Z_t) \tag{11.62}$$

where the union is over all random variable pairs (U, X) *such that*

$$U \to X \to Y_j^1 \to Y^* \to Y_k^2 \to Z^* \to Z_t \tag{11.63}$$

for any triple (j, k, t).

The proof of this theorem is given in Appendix 11.5.6. Similar to the converse proof of Theorem 11.1, the presence of the fictitious users Y^* and Z^* plays an important role here as well. In particular, these two random variables introduce a conditional independence structure to the channel which enables us to define

the auxiliary random variable U that yields a tight outer bound. Despite this similarity in the role of fictitious users in converse proofs, there is a significant difference between Theorems 11.1 and 11.7; in particular, it does not seem to be possible to extend Theorem 11.1 to an arbitrary number of eavesdroppers, while Theorem 11.7 holds for any number of eavesdroppers. This is due to the difference of two communication scenarios. In the second scenario, since we assume that users in the second group as well as the eavesdroppers wiretap users in the first group, we are able to provide a converse proof for the general situation of arbitrary number of eavesdroppers.

As an aside, if we set $K_1 = K_2 = K_Z = 1$, then DCMRWC with layered messages reduces to the degraded multi-receiver wiretap channel with layered messages of [45], the secrecy capacity region in Theorem 11.7 reduces to the secrecy capacity region of the channel model in [45].

11.3.2.1 Parallel DCMRWC with Layered Messages

In the next section, we investigate the Gaussian parallel DCMRWC with layered messages. To that end, here we obtain the secrecy capacity region of the parallel DCMRWC with layered messages in a single-letter form as follows.

Theorem 11.8 *The secrecy capacity region of the parallel DCMRWC with layered*

messages is given by the union of rate pairs (R_1, R_2) *satisfying*

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1 | U_\ell, Y_{k\ell}^2) \tag{11.64}$$

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} I(U_\ell; Y_{k\ell}^2 | Z_{t\ell}) \tag{11.65}$$

where the union is over all $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$ *such that*

$$U_\ell \to X_\ell \to Y_{j\ell}^1 \to Y_\ell^* \to Y_{k\ell}^2 \to Z_\ell^* \to Z_{t\ell} \tag{11.66}$$

for any (ℓ, j, k, t).

Since the parallel DCMRWC with layered messages is a special case of the DCMRWC with layered messages, Theorem 11.7 implicitly gives the secrecy capacity region of the parallel DCMRWC with layered messages. However, we still need to show that the region in Theorem 11.7 is equivalent to the region in Theorem 11.8. That is, we need to prove the optimality of independent signalling in each sub-channel. The proof of Theorem 11.8 is provided in Appendix 11.5.7.

11.3.2.2 Gaussian Parallel DCMRWC with Layered Messages

We now obtain the secrecy capacity region of the Gaussian parallel DCMRWC with layered messages. To that end, we need to evaluate the region given in Theorem 11.8, i.e., we need to find the optimal distribution $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. We first introduce the following theorem, which is an extension of Theorem 11.3.

Theorem 11.9 *Let $N_1, N^*, N_2, \tilde{N}, N_Z$ be zero-mean Gaussian random variables with variances $\sigma_1^2, \sigma_*^2, \sigma_2^2, \tilde{\sigma}^2, \sigma_Z^2$, respectively, where*

$$\sigma_1^2 \leq \sigma_*^2 \leq \sigma_2^2 \leq \tilde{\sigma}^2 \leq \sigma_Z^2 \tag{11.67}$$

Let (U, X) be an arbitrarily dependent random variable pair, which is independent of $(N_1, N^*, N_2, \tilde{N}, N_Z)$, and the second moment of X be constrained as $E[X^2] \leq P$. Then, for any feasible (U, X), we can find a $P^* \leq P$ such that

$$h(X + \tilde{N}|U) - h(X + N^*|U) = \frac{1}{2} \log \frac{P^* + \tilde{\sigma}^2}{P^* + \sigma_*^2} \tag{11.68}$$

and

$$h(X + N_Z|U) - h(X + N_2|U) \leq \frac{1}{2} \log \frac{P^* + \sigma_Z^2}{P^* + \sigma_2^2} \tag{11.69}$$

$$h(X + N_2|U) - h(X + N_1|U) \geq \frac{1}{2} \log \frac{P^* + \sigma_2^2}{P^* + \sigma_1^2} \tag{11.70}$$

for any $(\sigma_1^2, \sigma_2^2, \sigma_Z^2)$ satisfying the order in (11.67).

The proof of this theorem is given in Appendix 11.5.8. The proof of this theorem basically relies on Theorem 11.3 and Costa's entropy power inequality [44].

Using this theorem, we can establish the secrecy capacity region of the Gaussian parallel DCMRWC with layered messages as follows.

Theorem 11.10 *The secrecy capacity region of the Gaussian parallel DCMRWC*

with layered messages is given by the union of rate pairs (R_1, R_2) *satisfying*

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} \frac{1}{2}\log\left(1+\frac{\beta_\ell P_\ell}{\Lambda^1_{j,\ell\ell}}\right) - \frac{1}{2}\log\left(1+\frac{\beta_\ell P_\ell}{\Lambda^2_{k,\ell\ell}}\right) \tag{11.71}$$

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} \frac{1}{2}\log\left(1+\frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda^2_{k,\ell\ell}}\right) - \frac{1}{2}\log\left(1+\frac{\bar{\beta}_\ell P_\ell}{\beta_\ell P_\ell + \Lambda^Z_{t,\ell\ell}}\right) \tag{11.72}$$

where $\bar{\beta}_\ell = 1 - \beta_\ell \in [0,1],\ \ell = 1, \ldots, L$, *and the union is over all* $\{P_\ell\}_{\ell=1}^L$ *such that* $\sum_{\ell=1}^L P_\ell = P$.

The proof of this theorem is given in Appendix 11.5.9. Similar to Theorem 11.4, here also, P_ℓ denotes the amount of power P devoted to the transmission in the ℓth sub-channel. Similarly, β_ℓ is the fraction of the power P_ℓ of the ℓth sub-channel spent for the transmission to users in the first group.

11.3.2.3 Gaussian MIMO DCMRWC with Layered Messages

We now obtain the secrecy capacity region of the Gaussian MIMO DCMRWC with layered messages. To that end, we need to evaluate the region given in Theorem 11.7, i.e., find the optimal random vector pair $(U, \mathbf{X})$. We are able to find the optimal random vector pair $(U, \mathbf{X})$ when there is only one user in the second group, i.e., $K_2 = 1$. To obtain that result, we first need the following generalization of Theorem 11.5.

Theorem 11.11 *Let* $(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}^*, \mathbf{N}_Z)$ *be Gaussian random vectors with covariance matrices* $\mathbf{\Sigma}_1, \mathbf{\Sigma}_2, \mathbf{\Sigma}^*, \mathbf{\Sigma}_Z$, *respectively, where*

$$\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}^* \preceq \mathbf{\Sigma}_Z \tag{11.73}$$

Let $(U, \mathbf{X})$ *be an arbitrarily dependent random vector pair, which is independent of* $(\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}^*, \mathbf{N}_Z)$*, and the second moment of* $\mathbf{X}$ *be constrained as* $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$*. Then, for any feasible* $(U, \mathbf{X})$*, there exists a positive semi-definite matrix* $\mathbf{K}^*$ *such that* $\mathbf{K}^* \preceq \mathbf{S}$*, and it satisfies*

$$h(\mathbf{X} + \mathbf{N}^*|U) - h(\mathbf{X} + \mathbf{N}_2|U) = \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}^*|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} \tag{11.74}$$

and

$$h(\mathbf{X} + \mathbf{N}_Z|U) - h(\mathbf{X} + \mathbf{N}_2|U) \leq \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} \tag{11.75}$$

$$h(\mathbf{X} + \mathbf{N}_2|U) - h(\mathbf{X} + \mathbf{N}_1|U) \geq \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_2|}{|\mathbf{K}^* + \mathbf{\Sigma}_1|} \tag{11.76}$$

for any $(\mathbf{\Sigma}_1, \mathbf{\Sigma}_Z)$ *satisfying the order in (11.73).*

The proof of this theorem is given in Appendix 11.5.10. Using this theorem, we can find the secrecy capacity region of the Gaussian MIMO DCMRWC with layered messages when $K_2 = 1$ as follows.

Theorem 11.12 *The secrecy capacity region of the Gaussian MIMO DCMRWC with layered messages when* $K_2 = 1$ *is given by the union of rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \min_{j=1,\ldots,K_1} \frac{1}{2}\log\frac{|\mathbf{K} + \mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2}\log\frac{|\mathbf{K} + \mathbf{\Sigma}^2|}{|\mathbf{\Sigma}^2|} \tag{11.77}$$

$$R_2 \leq \min_{t=1,\ldots,K_Z} \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}^2|}{|\mathbf{K} + \mathbf{\Sigma}^2|} - \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_t^Z|}{|\mathbf{K} + \mathbf{\Sigma}_t^Z|} \tag{11.78}$$

where the union is over all positive semi-definite matrices $\mathbf{K}$ *such that* $\mathbf{K} \preceq \mathbf{S}$.

The proof of this theorem is given in Appendix 11.5.11. As an aside, if we set $K_1 = K_Z = 1$ in this theorem, we can recover the secrecy capacity region of the degraded multi-receiver wiretap channel with layered messages that was established in [45].

Finally we note that using the analysis carried out in Section V of [5] and Chapter 5.7, the capacity result given in Theorem 11.12 can be extended to the general Gaussian MIMO DCMRWC defined by (11.25)-(11.27) as follows.

Corollary 11.2 *The secrecy capacity region of the general Gaussian MIMO DCMRWC, defined by (11.25)-(11.27), with layered messages when* $K_2 = 1$ *is given by the union of rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \min_{j=1,\ldots,K_1} \frac{1}{2} \log \frac{|\mathbf{H}_j^1 \mathbf{K} (\mathbf{H}_j^1)^\top + \mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2} \log \frac{|\mathbf{H}^2 \mathbf{K} (\mathbf{H}^2)^\top + \mathbf{\Sigma}^2|}{|\mathbf{\Sigma}^2|} \tag{11.79}$$

$$R_2 \leq \min_{t=1,\ldots,K_Z} \frac{1}{2} \log \frac{|\mathbf{H}^2 \mathbf{S} (\mathbf{H}^2)^\top + \mathbf{\Sigma}^2|}{|\mathbf{H}^2 \mathbf{K} (\mathbf{H}^2)^\top + \mathbf{\Sigma}^2|} - \frac{1}{2} \log \frac{|\mathbf{H}_t^Z \mathbf{S} (\mathbf{H}_t^Z)^\top + \mathbf{\Sigma}_t^Z|}{|\mathbf{H}_t^Z \mathbf{K} (\mathbf{H}_t^Z)^\top + \mathbf{\Sigma}_t^Z|} \tag{11.80}$$

where the union is over all positive semi-definite matrices $\mathbf{K}$ *such that* $\mathbf{K} \preceq \mathbf{S}$.

11.4 Conclusions

In this chapter, we consider the DCMRWC for different communication scenarios, and obtain the corresponding secrecy capacity regions for the discrete memoryless case as well as its parallel and Gaussian parallel instances. We also consider MIMO channels, and obtain the secrecy capacity region under certain conditions.

11.5 Appendix

11.5.1 Proof of Theorem 11.1

Achievability is clear. We provide the converse proof. For an arbitrary code achieving the secrecy rates (R_1, R_2), there exist $(\epsilon_{1,n}, \epsilon_{2,n})$ and γ_n which vanish as $n \to \infty$ such that

$$H(W_1|Y_j^{1,n}) \leq n\epsilon_{1,n}, \quad j = 1, \ldots, K_1 \tag{11.81}$$

$$H(W_2|Y_k^{2,n}) \leq n\epsilon_{2,n}, \quad k = 1, \ldots, K_2 \tag{11.82}$$

$$I(W_1, W_2; Z^n) \leq n\gamma_n \tag{11.83}$$

where (11.81) and (11.82) are due to Fano's lemma, and (11.83) is due to the perfect secrecy requirement stated in (11.32).

We define the following auxiliary random variables

$$U_i = W_2 Y^{*,i-1} Z_{i+1}^n, \quad i = 1, \ldots, n \tag{11.84}$$

which satisfy the following Markov chain

$$U_i \to X_i \to Y_{j,i}^1 \to Y_i^* \to Y_{k,i}^2 \to Z_i, \quad i = 1, \ldots, n \tag{11.85}$$

for any (j, k) pair. The Markov chain in (11.85) is a consequence of the fact that the channel is memoryless and degraded.

We first bound the rate of the second message:

$$
\begin{aligned}
nR_2 &= H(W_2) && (11.86)\\
&\le I(W_2; Y_k^{2,n}) + n\epsilon_{2,n} && (11.87)\\
&\le I(W_2; Y_k^{2,n}) - I(W_2; Z^n) + n(\epsilon_{2,n} + \gamma_n) && (11.88)\\
&= I(W_2; Y_k^{2,n} | Z^n) + n(\epsilon_{2,n} + \gamma_n) && (11.89)\\
&= \sum_{i=1}^{n} I(W_2; Y_{k,i}^2 | Y_k^{2,i-1}, Z^n) + n(\epsilon_{2,n} + \gamma_n) && (11.90)\\
&= \sum_{i=1}^{n} I(W_2; Y_{k,i}^2 | Y_k^{2,i-1}, Z_{i+1}^n, Z_i) + n(\epsilon_{2,n} + \gamma_n) && (11.91)\\
&\le \sum_{i=1}^{n} I(Y_k^{2,i-1}, Z_{i+1}^n, W_2; Y_{k,i}^2 | Z_i) + n(\epsilon_{2,n} + \gamma_n) && (11.92)\\
&\le \sum_{i=1}^{n} I(Y^{*,i-1}, Y_k^{2,i-1}, Z_{i+1}^n, W_2; Y_{k,i}^2 | Z_i) + n(\epsilon_{2,n} + \gamma_n) && (11.93)\\
&= \sum_{i=1}^{n} I(Y^{*,i-1}, Z_{i+1}^n, W_2; Y_{k,i}^2 | Z_i) + n(\epsilon_{2,n} + \gamma_n) && (11.94)\\
&= \sum_{i=1}^{n} I(U_i; Y_{k,i}^2 | Z_i) + n(\epsilon_{2,n} + \gamma_n) && (11.95)
\end{aligned}
$$

where (11.87) is due to (11.82), (11.88) is a consequence of (11.83), (11.89) comes from the Markov chain

$$W_2 \to Y_k^{2,n} \to Z^n, \quad k = 1, \ldots, K_2 \tag{11.96}$$

which is a consequence of the fact that the channel is degraded, (11.91) comes from

the Markov chain

$$Z^{i-1} \to Y_k^{2,i-1} \to (Y_{k,i}^2, Z_i^n, W_2), \quad k = 1, \ldots, K_2 \tag{11.97}$$

which is due to the fact that the channel is degraded and memoryless, and (11.94) is a consequence of the Markov chain

$$Y_k^{2,i-1} \to Y^{*,i-1} \to (W_2, Z_i^n, Y_{k,i}^2), \quad k = 1, \ldots, K_2 \tag{11.98}$$

which is due to the Markov chain in (11.2) and the fact that the channel is memoryless.

Next we bound the rate of the first message:

$$\begin{aligned}
nR_1 &= H(W_1) && (11.99)\\
&= H(W_1|W_2) && (11.100)\\
&\le I(W_1; Y_j^{1,n}|W_2) + n\epsilon_{1,n} && (11.101)\\
&\le I(W_1; Y_j^{1,n}|W_2) - I(W_1; Z^n|W_2) + n(\epsilon_{1,n} + \gamma_n) && (11.102)\\
&= I(W_1; Y_j^{1,n}|W_2, Z^n) + n(\epsilon_{1,n} + \gamma_n) && (11.103)\\
&= \sum_{i=1}^{n} I(W_1; Y_{j,i}^1|W_2, Z^n, Y_j^{1,i-1}) + n(\epsilon_{1,n} + \gamma_n) && (11.104)\\
&= \sum_{i=1}^{n} I(W_1; Y_{j,i}^1|W_2, Z_{i+1}^n, Y_j^{1,i-1}, Z_i) + n(\epsilon_{1,n} + \gamma_n) && (11.105)\\
&= \sum_{i=1}^{n} I(W_1; Y_{j,i}^1|W_2, Z_{i+1}^n, Y_j^{1,i-1}, Y^{*,i-1}, Z_i) + n(\epsilon_{1,n} + \gamma_n) && (11.106)
\end{aligned}$$

$$\leq \sum_{i=1}^{n} I(X_i, W_1; Y_{j,i}^1 | W_2, Z_{i+1}^n, Y_j^{1,i-1}, Y^{*,i-1}, Z_i) + n(\epsilon_{1,n} + \gamma_n) \tag{11.107}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{j,i}^1 | W_2, Z_{i+1}^n, Y_j^{1,i-1}, Y^{*,i-1}, Z_i) + n(\epsilon_{1,n} + \gamma_n) \tag{11.108}$$

$$= \sum_{i=1}^{n} H(Y_{j,i}^1 | W_2, Z_{i+1}^n, Y_j^{1,i-1}, Y^{*,i-1}, Z_i) - H(Y_{j,i}^1 | W_2, Z_{i+1}^n, Y_j^{1,i-1}, Y^{*,i-1}, Z_i, X_i)$$

$$+ n(\epsilon_{1,n} + \gamma_n) \tag{11.109}$$

$$\leq \sum_{i=1}^{n} H(Y_{j,i}^1 | W_2, Z_{i+1}^n, Y^{*,i-1}, Z_i) - H(Y_{j,i}^1 | W_2, Z_{i+1}^n, Y_j^{1,i-1}, Y^{*,i-1}, Z_i, X_i)$$

$$+ n(\epsilon_{1,n} + \gamma_n) \tag{11.110}$$

$$= \sum_{i=1}^{n} H(Y_{j,i}^1 | W_2, Z_{i+1}^n, Y^{*,i-1}, Z_i) - H(Y_{j,i}^1 | W_2, Z_{i+1}^n, Y^{*,i-1}, Z_i, X_i)$$

$$+ n(\epsilon_{1,n} + \gamma_n) \tag{11.111}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{j,i}^1 | W_2, Z_{i+1}^n, Y^{*,i-1}, Z_i) + n(\epsilon_{1,n} + \gamma_n) \tag{11.112}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{j,i}^1 | U_i, Z_i) + n(\epsilon_{1,n} + \gamma_n) \tag{11.113}$$

where (11.101) is due to (11.81), (11.102) is a consequence of (11.83), (11.103) comes from the Markov chain

$$(W_2, W_1) \to Y_j^{1,n} \to Z^n, \quad j = 1, \ldots, K_1 \tag{11.114}$$

which is due to the fact that the channel is degraded, (11.105) comes from the Markov chain

$$Z^{i-1} \to Y_j^{1,i-1} \to (W_1, W_2, Y_{j,i}^1, Z_i^n), \quad j = 1, \ldots, K_1 \tag{11.115}$$

which is a consequence of the fact that the channel is degraded and memoryless, (11.106) follows from the Markov chain

$$Y^{*,i-1} \to Y_j^{1,i-1} \to (W_1, W_2, Y_{j,i}^1, Z_i^n), \quad j = 1, \ldots, K_1 \tag{11.116}$$

which results from the Markov chain in (11.2) and the fact that the channel is memoryless, (11.108) is a consequence of the Markov chain

$$(Y_{j,i}^1, Z_i) \to X_i \to (Y^{*,i-1}, Y_j^{1,i-1}, Z_{i+1}^n, W_1, W_2), \quad j = 1, \ldots, K_1 \tag{11.117}$$

which is due to the fact that the channel is memoryless, (11.110) comes from the fact that conditioning cannot increase entropy, and (11.111) is again due to the Markov chain in (11.117).

Next, we define a uniformly distributed random variable $Q \in \{1, \ldots, n\}$, and $U = (Q, U_Q), X = X_Q, Y_j^1 = Y_{j,Q}^1, Y_k^2 = Y_{k,Q}^2$, and $Z = Z_Q$. Using these definitions in (11.95) and (11.113), we obtain the single-letter expressions in Theorem 11.1.

11.5.2 Proof of Theorem 11.2

The achievability of this region follows from Theorem 11.1 by selecting $(U, X) = (U_1, X_1, \ldots, U_L, X_L)$ with a joint distribution of the product form $p(u, x) = \prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. We next provide the converse proof. To that end, we define the

following auxiliary random variables

$$U_\ell = UY^*_{[1:\ell-1]}Z_{[\ell+1:L]}, \quad \ell = 1, \ldots, L \tag{11.118}$$

which satisfy the Markov chain

$$U_\ell \to X_\ell \to (Y^1_{j\ell}, Y^2_{k\ell}, Z_\ell) \tag{11.119}$$

for any (j, k, ℓ) triple because of the facts that the channel is memoryless and sub-channels are independent.

We bound the rate of the second message as follows

$$\begin{aligned}
R_2 &\le \min_{k=1,\ldots,K_2} I(U; Y^2_{k[1:L]}|Z_{[1:L]}) && (11.120)\\
&= \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U; Y^2_{k\ell}|Y^2_{k[1:\ell-1]}, Z_{[1:L]}) && (11.121)\\
&= \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U; Y^2_{k\ell}|Y^2_{k[1:\ell-1]}, Z_{[\ell:L]}) && (11.122)\\
&\le \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U, Y^2_{k[1:\ell-1]}, Z_{[\ell+1:L]}; Y^2_{k\ell}|Z_\ell) && (11.123)\\
&\le \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U, Y^*_{[1:\ell-1]}, Y^2_{k[1:\ell-1]}, Z_{[\ell+1:L]}; Y^2_{k\ell}|Z_\ell) && (11.124)\\
&= \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U, Y^*_{[1:\ell-1]}, Z_{[\ell+1:L]}; Y^2_{k\ell}|Z_\ell) && (11.125)\\
&= \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U_\ell; Y^2_{k\ell}|Z_\ell) && (11.126)
\end{aligned}$$

where (11.122) follows from the Markov chain

$$Z_{[1:\ell-1]} \to Y^2_{k[1:\ell-1]} \to (U, Y^2_{k\ell}, Z_{[\ell:L]}) \tag{11.127}$$

which is a consequence of the facts that the channel is degraded and memoryless, and sub-channels are independent, and (11.125) is due to the Markov chain

$$Y^2_{k[1:\ell-1]} \to Y^*_{[1:\ell-1]} \to U, Y^2_{k\ell}, Z_{[\ell:L]} \tag{11.128}$$

which is a consequence of the Markov chain in (11.10) and the facts that the channel is memoryless and sub-channels are independent.

We next bound the rate of the first message as follows

$$\begin{aligned}
R_1 &\leq \min_{j=1,\ldots,K_1} I(X_{[1:L]}; Y^1_{j[1:L]}|U, Z_{[1:L]}) && (11.129)\\
&= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_{[1:L]}; Y^1_{j\ell}|U, Y^1_{j[1:\ell-1]}, Z_{[1:L]}) && (11.130)\\
&= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_{[1:L]}; Y^1_{j\ell}|U, Y^1_{j[1:\ell-1]}, Z_{[\ell:L]}) && (11.131)\\
&= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_{[1:L]}; Y^1_{j\ell}|U, Y^1_{j[1:\ell-1]}, Y^*_{[1:\ell-1]}, Z_{[\ell:L]}) && (11.132)\\
&= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_{[1:L]}; Y^1_{j\ell}|U_\ell, Y^1_{j[1:\ell-1]}, Z_\ell) && (11.133)\\
&= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} H(Y^1_{j\ell}|U_\ell, Y^1_{j[1:\ell-1]}, Z_\ell) - H(Y^1_{j\ell}|U_\ell, Y^1_{j[1:\ell-1]}, Z_\ell, X_{[1:L]}) && (11.134)\\
&\leq \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} H(Y^1_{j\ell}|U_\ell, Z_\ell) - H(Y^1_{j\ell}|U_\ell, Y^1_{j[1:\ell-1]}, Z_\ell, X_{[1:L]}) && (11.135)
\end{aligned}$$

$$= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} H(Y_{j\ell}^1|U_\ell, Z_\ell) - H(Y_{j\ell}^1|U_\ell, Z_\ell, X_\ell) \tag{11.136}$$

$$= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1|U_\ell, Z_\ell) \tag{11.137}$$

where (11.131) and (11.132) follow from the Markov chain

$$Z_{[1:\ell-1]} \to Y_{[1:\ell-1]}^* \to Y_{j[1:\ell-1]}^1 \to (U, Y_{j\ell}^1, Z_{[\ell:L]}, X_{[1:L]}) \tag{11.138}$$

which is due to the facts that the channel is degraded and memoryless, sub-channels are independent, and the Markov chain in (11.10), (11.135) results from the fact that conditioning cannot increase entropy, (11.136) comes from the Markov chain

$$(Y_{j\ell}^1, Z_\ell) \to X_\ell \to (U_\ell, Y_{j[1:\ell-1]}^1, X_{[1:\ell-1]}, X_{[\ell+1:L]}) \tag{11.139}$$

which is a consequence of the facts that the channel is memoryless, and sub-channels are independent.

In view of (11.126) and (11.137), we obtain the single-letter expressions in Theorem 11.2. Finally, we note that each expression in the bounds given by (11.126) and (11.137) depend on the the joint distribution $p(u_{[1:L]}, x_{[1:L]})$ through its marginals $p(u_\ell, x_\ell)$. Thus, there is no loss of optimality to choose $p(u_{[1:L]}, x_{[1:L]}) = \prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. This completes the converse proof.

11.5.3 Proof of Theorem 11.3

We first note that

$$\frac{1}{2}\log\frac{\sigma_*^2}{\sigma_Z^2} \leq h(X+N^*|U) - h(X+N_Z|U) \leq \frac{1}{2}\log\frac{P+\sigma_*^2}{P+\sigma_Z^2} \tag{11.140}$$

where the right-hand side can be shown via the entropy power inequality [42, 43]. To show the left-hand side, let us define a Gaussian random variable $\tilde{N}$ with variance $\sigma_Z^2 - \sigma_*^2$, and independent of (U, X, N^*). Thus, we can write down the difference of differential entropy terms in (11.140) as

$$\begin{aligned}
h(X+N^*|U) - h(X+N_Z|U) &= h(X+N^*|U) - h(X+N^*+\tilde{N}|U) && (11.141)\\
&= -I(\tilde{N}; X+N^*+\tilde{N}|U) && (11.142)\\
&= -h(\tilde{N}|U) + h(\tilde{N}|U, X+N^*+\tilde{N}) && (11.143)\\
&\geq -h(\tilde{N}|U) + h(\tilde{N}|U, X+N^*+\tilde{N}, X) && (11.144)\\
&= -h(\tilde{N}) + h(\tilde{N}|N^*+\tilde{N}) && (11.145)\\
&= \frac{1}{2}\log\frac{\sigma_*^2}{\sigma_Z^2} && (11.146)
\end{aligned}$$

where (11.144) is due to the fact that conditioning cannot increase entropy and (11.145) is a consequence of the fact that (U, X) and $(N^*, \tilde{N})$ are independent.

Equation (11.140) implies that there exists P^* such that $P^* \leq P$ and

$$h(X+N^*|U) - h(X+N_Z|U) = \frac{1}{2}\log\frac{P^*+\sigma_*^2}{P^*+\sigma_Z^2} \tag{11.147}$$

which will be used frequently hereafter.

We now state Costa's entropy power inequality [44] which will be used in the upcoming proof[1].

Lemma 11.1 ([44, Theorem 1]) *Let (U, X) be an arbitrarily dependent random variable pair, which is independent of N, where N is a Gaussian random variable. Then, we have*

$$e^{2h(X+\sqrt{t}N|U)} \geq (1-t)e^{2h(X|U)} + te^{2h(X+N|U)}, \quad 0 \leq t \leq 1 \tag{11.148}$$

We now consider (11.42). We first note that we can write N^* as

$$N^* = N_1 + \sqrt{t_1}\tilde{N}_1 \tag{11.149}$$

where $\tilde{N}_1$ is a Gaussian random variable with variance $\sigma_Z^2 - \sigma_1^2$, which is independent of (U, X, N_1). t_1 in (11.149) is given by

$$t_1 = \frac{\sigma_*^2 - \sigma_1^2}{\sigma_Z^2 - \sigma_1^2} \tag{11.150}$$

where it is clear that $t_1 \in [0, 1]$. Using (11.149) and Costa's entropy power inequal-

[1]Although, Theorem 1 of [44] states the inequality for a constant U, using Jensen's inequality, the current form of the inequality for an arbitrary U can be shown.

ity [44], we get

$$e^{2h(X+N^*|U)} = e^{2h(X+N_1+\sqrt{t_1}\tilde{N}_1|U)} \tag{11.151}$$

$$\geq (1-t_1)e^{2h(X+N_1|U)} + t_1 e^{2h(X+N_Z|U)} \tag{11.152}$$

which is equivalent to

$$(1-t_1)e^{2[h(X+N_1|U)-h(X+N_Z|U)]} + t_1 \leq e^{2[h(X+N^*|U)-h(X+N_Z|U)]} \tag{11.153}$$

$$= \frac{P^*+\sigma_*^2}{P^*+\sigma_Z^2} \tag{11.154}$$

where (11.154) is obtained by using (11.147). Equation (11.154) is equivalent to

$$h(X+N_1|U) - h(X+N_Z|U) \leq \frac{1}{2}\log\frac{1}{1-t_1}\left(\frac{P^*+\sigma_*^2}{P^*+\sigma_Z^2} - t_1\right) \tag{11.155}$$

$$= \frac{1}{2}\log\left(\frac{P^*}{P^*+\sigma_Z^2} + \frac{1}{1-t_1}\frac{\sigma_*^2 - t_1\sigma_Z^2}{P^*+\sigma_Z^2}\right) \tag{11.156}$$

$$= \frac{1}{2}\log\frac{P^*+\sigma_1^2}{P^*+\sigma_Z^2} \tag{11.157}$$

where we used the definition of t_1 given in (11.150) to obtain (11.157). Equation (11.157) proves (11.42).

We now consider (11.43). First, we note that we can write N_2

$$N_2 = N^* + \sqrt{t_2}\tilde{N}_Z \tag{11.158}$$

where $\tilde{N}_Z$ is a Gaussian random variable with variance $\sigma_Z^2 - \sigma_*^2$, which is independent

of (U, X, N^*). t_2 in (11.158) is given by

$$t_2 = \frac{\sigma_2^2 - \sigma_*^2}{\sigma_Z^2 - \sigma_*^2} \tag{11.159}$$

where it is clear that $t_2 \in [0, 1]$. Using (11.158) and Costa's entropy power inequality [44], we get

$$e^{2h(X+N_2|U)} = e^{2h(X+N^*+\sqrt{t_2}\tilde{N}_Z|U)} \tag{11.160}$$

$$\geq (1-t_2)e^{2h(X+N^*|U)} + t_2 e^{2h(X+N_Z|U)} \tag{11.161}$$

which is equivalent to

$$e^{2[h(X+N_2|U)-h(X+N_Z|U)]} \geq (1-t_2)e^{2[h(X+N^*|U)-h(X+N_Z|U)]} + t_2 \tag{11.162}$$

$$= (1-t_2)\frac{P^* + \sigma_*^2}{P^* + \sigma_Z^2} + t_2 \tag{11.163}$$

$$= \frac{P^* + \sigma_2^2}{P^* + \sigma_Z^2} \tag{11.164}$$

where (11.164) is obtained by using the definition of t_2 given in (11.159). Equation (11.164) is equivalent to

$$h(X + N_Z|U) - h(X + N_2|U) \leq \frac{1}{2}\log\frac{P^* + \sigma_Z^2}{P^* + \sigma_2^2} \tag{11.165}$$

which is (11.43). This completes the proof of Theorem 11.3.

11.5.4 Proof of Theorem 11.4

Achievability is clear. We provide the converse proof. To this end, let us fix the distribution $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$ such that

$$E\left[X_\ell^2\right] = P_\ell, \quad \ell = 1, \ldots, L \tag{11.166}$$

and $\sum_{\ell=1}^{L} P_\ell \leq P$. We first establish the bound on R_2 given in (11.45). To this end, we start with (11.38). Using the Markov chain $U_\ell \to Y_{k\ell}^2 \to Z_\ell$, we have

$$R_2 \leq \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} I(U_\ell; Y_{k\ell}^2) - I(U_\ell; Z_\ell) \tag{11.167}$$

$$= \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} \left[h(Y_{k\ell}^2) - h(Z_\ell)\right] + \left[h(Z_\ell|U) - h(Y_{k\ell}^2|U)\right] \tag{11.168}$$

$$\leq \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} \frac{1}{2} \log \frac{P_\ell + \Lambda_{k,\ell\ell}^2}{P_\ell + \Lambda_{Z,\ell\ell}} + \left[h(Z_\ell|U) - h(Y_{k\ell}^2|U)\right] \tag{11.169}$$

where (11.169) comes from the fact that Gaussian X_ℓ maximizes

$$h(Y_{k\ell}^2) - h(Z_\ell) \tag{11.170}$$

which can be shown via the entropy power inequality [42, 43]. We now use Theorem 11.3. For that purpose, we introduce the diagonal covariance matrix $\mathbf{\Lambda}^*$ which satisfies

$$\mathbf{\Lambda}_j^1 \preceq \mathbf{\Lambda}^* \preceq \mathbf{\Lambda}_k^2 \tag{11.171}$$

for any (j,k) pair, and in particular, for the diagonal elements of these matrices, we have

$$\Lambda^1_{j,\ell\ell} \leq \Lambda^*_{\ell\ell} \leq \Lambda^2_{k,\ell\ell} \tag{11.172}$$

for any triple (j,k,ℓ). Thus, due to Theorem 11.3, for any selection of $\{(U_\ell, X_\ell)\}_{\ell=1}^L$, there exists a P^*_ℓ such that

$$P^*_\ell \leq P_\ell \tag{11.173}$$

$$h(Z_\ell|U_\ell) - h(Y^1_{j\ell}|U_\ell) \geq \frac{1}{2}\log\frac{P^*_\ell + \Lambda_{Z,\ell\ell}}{P^*_\ell + \Lambda^1_{j,\ell\ell}} \tag{11.174}$$

$$h(Z_\ell|U_\ell) - h(Y^2_{k\ell}|U_\ell) \leq \frac{1}{2}\log\frac{P^*_\ell + \Lambda_{Z,\ell\ell}}{P^*_\ell + \Lambda^2_{k,\ell\ell}} \tag{11.175}$$

for any triple (j,k,ℓ). Using (11.175) in (11.169), we get

$$R_2 \leq \min_{k=1,\ldots,K_2} \sum_{\ell=1}^{L} \frac{1}{2}\log\frac{P_\ell + \Lambda^2_{k,\ell\ell}}{P^*_\ell + \Lambda^2_{k,\ell\ell}} - \frac{1}{2}\log\frac{P_\ell + \Lambda_{Z,\ell\ell}}{P^*_\ell + \Lambda_{Z,\ell\ell}} \tag{11.176}$$

We define $P^*_\ell = \beta_\ell P_\ell$ and $\bar{\beta}_\ell = 1 - \beta_\ell,\ \ell = 1,\ldots,L$, where $\beta_\ell \in [0,1]$ due to (11.173). Thus, we have established the desired bound on R_2 given in (11.45). We now bound

R_1. We start with (11.37). Using the Markov chain $(U_\ell, X_\ell) \to Y_{j\ell}^1 \to Z_\ell$, we have

$$R_1 \leq \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1|U_\ell) - I(X_\ell; Z_\ell|U_\ell) \tag{11.177}$$

$$= \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} h(Y_{j\ell}^1|U_\ell) - h(Z_\ell|U_\ell) - \frac{1}{2}\log\frac{\Lambda_{j,\ell\ell}^1}{\Lambda_{Z,\ell\ell}} \tag{11.178}$$

$$\leq \min_{j=1,\ldots,K_1} \sum_{\ell=1}^{L} \frac{1}{2}\log\frac{P_\ell^* + \Lambda_{j,\ell\ell}^1}{P_\ell^* + \Lambda_{Z,\ell\ell}} - \frac{1}{2}\log\frac{\Lambda_{j,\ell\ell}^1}{\Lambda_{Z,\ell\ell}} \tag{11.179}$$

where (11.179) comes from (11.174). Since we defined $P_\ell^* = \beta_\ell P_\ell$, (11.179) is the desired bound on R_1 given in (11.44), completing the proof.

11.5.5 Proof of Theorem 11.6

The main tools for the proof of Theorem 11.6 are Theorem 11.5, and the following so-called worst additive noise lemma [36, 37].

Lemma 11.2 ([36, 37]) *Let* $\mathbf{N}$ *be a Gaussian random vector with covariance matrix* $\mathbf{\Sigma}$*, and* $\mathbf{K}_X$ *be a positive semi-definite matrix. Consider the following optimization problem,*

$$\min_{p(\mathbf{x})} \quad I(\mathbf{N}; \mathbf{N}+\mathbf{X}) \qquad \text{s.t.} \;\; \text{Cov}(\mathbf{X}) = \mathbf{K}_X \tag{11.180}$$

where $\mathbf{X}$ *and* $\mathbf{N}$ *are independent. A Gaussian* $\mathbf{X}$ *is the minimizer of this optimization problem.*

We first bound R_2. Assume we fixed the distribution of $(U, \mathbf{X})$ such that $\mathrm{Cov}(\mathbf{X}) = \mathbf{K}_X$. Then, we have

$$R_2 \leq I(U; \mathbf{Y}^2) - I(U; \mathbf{Z}) \tag{11.181}$$

$$= h(\mathbf{Y}^2) - h(\mathbf{Z}) + [h(\mathbf{Z}|U) - h(\mathbf{Y}^2|U)] \tag{11.182}$$

$$\leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}^2|}{|\mathbf{S} + \mathbf{\Sigma}_Z|} + [h(\mathbf{Z}|U) - h(\mathbf{Y}^2|U)] \tag{11.183}$$

To show (11.183), consider $\tilde{\mathbf{N}}$ which is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_Z - \mathbf{\Sigma}^2$, and is independent of $(U, \mathbf{X}, \mathbf{N}^2)$. Thus, we can write

$$h(\mathbf{Y}^2) - h(\mathbf{Z}) = h(\mathbf{Z}|\tilde{\mathbf{N}}) - h(\mathbf{Z}) \tag{11.184}$$

$$= -I(\tilde{\mathbf{N}}; \mathbf{X} + \mathbf{N}^2 + \tilde{\mathbf{N}}) \tag{11.185}$$

$$\leq \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{\Sigma}^2|}{|\mathbf{K}_X + \mathbf{\Sigma}_Z|} \tag{11.186}$$

$$\leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}^2|}{|\mathbf{S} + \mathbf{\Sigma}_Z|} \tag{11.187}$$

where (11.186) is due to Lemma 11.2, and (11.187) follows from the fact that

$$\frac{|\mathbf{A}|}{|\mathbf{A} + \mathbf{B}|} \leq \frac{|\mathbf{A} + \mathbf{\Delta}|}{|\mathbf{A} + \mathbf{B} + \mathbf{\Delta}|} \tag{11.188}$$

for $\mathbf{A} \succeq \mathbf{0}, \mathbf{B} \succ \mathbf{0}, \mathbf{\Delta} \succeq \mathbf{0}$ [4, 19].

For the rest of the proof, we need Theorem 11.5. According to Theorem 11.5, for any $(U, \mathbf{X})$, there exists a $\mathbf{0} \preceq \mathbf{K} \preceq \mathrm{Cov}(\mathbf{X}|U)$ such that

$$h(\mathbf{Z}|U) - h(\mathbf{Y}^2|U) = \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}^2|} \tag{11.189}$$

$$h(\mathbf{Z}|U) - h(\mathbf{Y}_j^1|U) \geq \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_j^1|}, \quad j = 1, \ldots, K_1 \tag{11.190}$$

because $\mathbf{\Sigma}_j^1 \preceq \mathbf{\Sigma}^2,\ j = 1, \ldots, K_1$. Using (11.189) in (11.183) yields

$$R_2 \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}^2|}{|\mathbf{K}+\mathbf{\Sigma}^2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} \tag{11.191}$$

which is the desired bound on R_2.

The desired bound on R_1 can be obtained as follows

$$R_1 \leq \min_{j=1,\ldots,K_1} I(\mathbf{X};\mathbf{Y}_j^1|U) - I(\mathbf{X};\mathbf{Z}|U) \tag{11.192}$$

$$= \min_{j=1,\ldots,K_1} h(\mathbf{Y}_j^1|U) - h(\mathbf{Z}|U) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_Z|} \tag{11.193}$$

$$\leq \min_{j=1,\ldots,K_1} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_j^1|}{|\mathbf{K}+\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_Z|} \tag{11.194}$$

$$= \min_{j=1,\ldots,K_1} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{11.195}$$

where (11.194) is due to (11.190). This completes the proof of Theorem 11.6.

11.5.6 Proof of Theorem 11.7

We first show the achievability of the region given in Theorem 11.7, then provide the converse proof.

11.5.6.1 Achievability

First, we present the following lemma which simplifies the achievability proof.

Lemma 11.3 ([38, Lemma A.1]) *Let $U, X, Z_1, Z_2, Y_1^2, Y_2^2$ be random variables such that they satisfy the following Markov chains*

$$U \to X \to Z_1, Z_2 \tag{11.196}$$

$$U \to X \to Y_1^2, Y_2^2 \tag{11.197}$$

If $I(U;Z_1) < I(U;Z_2)$, there exists a random variable $\tilde{Z}$ such that $I(U;Z_1,\tilde{Z}) = I(U;Z_2)$ and $\tilde{Z}$ satisfies the following Markov chain

$$U \to X \to (Z_1, Z_2) \to \tilde{Z} \tag{11.198}$$

Similarly, if $I(X;Y_1^2|U) < I(X;Y_2^2|U)$, there exists a random variable $\tilde{Y}^2$ such that $I(X;Y_1^2,\tilde{Y}^2|U) = I(X;Y_2^2|U)$ and $\tilde{Y}^2$ satisfies the following Markov chain

$$U \to X \to (Y_1^2, Y_2^2) \to \tilde{Y}^2 \tag{11.199}$$

We now show the achievability of the region given in Theorem 11.7. First, we fix the distribution $p(u,x)$.

Codebook generation:

- Generate $2^{n(R_2+\tilde{R}_2)}$ length-n $\mathbf{u}$ sequences through $p(\mathbf{u}) = \prod_{i=1}^{n} p(u_i)$ where

$\tilde{R}_2 = \max_{t=1,\ldots,K_Z} I(U;Z_t)$. We index $\mathbf{u}$ sequences as $\mathbf{u}(w_2,\tilde{w}_2)$ where $w_2 \in \{1,\ldots,2^{nR_2}\}$, and $\tilde{w}_2 \in \{1,\ldots,2^{n\tilde{R}_2}\}$.

- For each $\mathbf{u}$, generate $2^{n(R_1+\tilde{R}_1)}$ length-n $\mathbf{x}$ sequences through $p(\mathbf{x}|\mathbf{u}) = \prod_{i=1}^{n} p(x_i|u_i)$ where $\tilde{R}_1 = \max_{k=1,\ldots,K_2} I(X;Y_k^2|U)$. We index $\mathbf{x}$ sequences as $\mathbf{x}(w_1,\tilde{w}_1|\mathbf{w}_2)$ where $\mathbf{w}_2 = (w_2,\tilde{w}_2)$, $w_1 \in \{1,\ldots,2^{nR_1}\}$, and $\tilde{w}_1 \in \{1,\ldots,2^{n\tilde{R}_1}\}$.

Encoding:

If (w_1,w_2) is the message to be transmitted, we pick $\tilde{w}_1,\tilde{w}_2$ independently and uniformly, and send the corresponding $\mathbf{x}$.

Decoding:

The legitimate users can decode the messages with vanishingly small probability of error, if the rates satisfy

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} I(X;Y_j^1|U) - I(X;Y_k^2|U) \tag{11.200}$$

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} I(U;Y_k^2) - I(U;Z_t) \tag{11.201}$$

which is the same as the region given in Theorem 11.7 because of the degradedness of the channel.

Equivocation computation:

We now show that this coding scheme satisfies the secrecy requirements given in (11.58) and (11.59). To this end, we will take a shortcut by using Lemma 11.3, as

it is done in [38]. To show (11.58), we consider the enhanced eavesdroppers with observations $(Z_t, \tilde{Z}_t)$ such that $I(U; Z_t, \tilde{Z}_t) = \max_{t=1,\ldots,K_Z} I(U; Z_t)$, where the existence of the random variable $\tilde{Z}_t$ is ensured by Lemma 11.3. Following the equivocation computation in Appendix A of [45], one can get

$$\lim_{n\to\infty} \frac{1}{n} I(W_2; Z_t^n, \tilde{Z}_t^n) = 0 \tag{11.202}$$

which implies that the secrecy requirement in (11.58) is satisfied.

Next we show that the proposed encoding scheme satisfies the secrecy requirement in (11.59) as well. Similar to what we did to show (11.58), we take a shortcut by using Lemma 11.3. In particular, we consider the enhanced second group of users with observations $(Y_k^2, \tilde{Y}_k^2)$ such that $I(X; Y_k^2, \tilde{Y}_k^2|U) = \max_{k=1,\ldots,K_2} I(X; Y_k^2, \tilde{Y}_k^2|U)$ where the existence of the random variable $\tilde{Y}_k^2$ is ensured by Lemma 11.3. Following the equivocation computation in Appendix A of [45], one can get

$$\lim_{n\to\infty} \frac{1}{n} I(W_1; Y_k^{2,n}, \tilde{Y}_k^{2,n}|W_2) = 0 \tag{11.203}$$

which implies that the secrecy requirement in (11.59) is satisfied. This completes the achievability proof of Theorem 11.7.

11.5.6.2 Converse

First, we note that for an arbitrary code achieving the secrecy rate pairs (R_1, R_2), there exist $(\epsilon_{1,n}, \epsilon_{2,n})$ and $(\gamma_{1,n}, \gamma_{2,n})$ which vanish as $n \to \infty$ such that

$$H(W_1|Y_j^{1,n}) \leq n\epsilon_{1,n}, \quad j = 1, \ldots, K_1 \tag{11.204}$$

$$H(W_2|Y_k^{2,n}) \leq n\epsilon_{2,n}, \quad k = 1, \ldots, K_2 \tag{11.205}$$

$$I(W_2; Z_t^n) \leq n\gamma_{2,n}, \quad t = 1, \ldots, K_Z \tag{11.206}$$

$$I(W_1; Y_k^{2,n}|W_2) \leq n\gamma_{1,n}, \quad k = 1, \ldots, K_2 \tag{11.207}$$

where (11.204) and (11.205) are due to Fano's lemma, and (11.206) and (11.207) come from perfect secrecy requirements in (11.58) and (11.59).

We now define the following auxiliary random variables

$$U_i = W_2 Y^{*,i-1} Z_{i+1}^{*,n}, \quad i = 1, \ldots, n \tag{11.208}$$

which satisfy the Markov chains

$$U_i \to X_i \to Y_{j,i}^1 \to Y_i^* \to Y_{k,i}^2 \to Z_i^* \to Z_{t,i}, \quad i = 1, \ldots, n \tag{11.209}$$

for any (j, k, t) triple. The Markov chain in (11.209) is a consequence of the fact that the channel is memoryless and degraded.

We first establish the desired bound on R_2 as follows

$$nR_2 \leq I(W_2; Y_{k,i}^2 | Z_{t,i+1}^n, Y_k^{2,i-1}, Z_{t,i}) + n(\epsilon_{2,n} + \gamma_{2,n}) \tag{11.210}$$

$$\leq \sum_{i=1}^{n} I(Z_{t,i+1}^n, Y_k^{2,i-1}, W_2; Y_{k,i}^2 | Z_{t,i}) + n(\epsilon_{2,n} + \gamma_{2,n}) \tag{11.211}$$

$$\leq \sum_{i=1}^{n} I(Z_{i+1}^{*,n}, Y^{*,i-1}, Z_{t,i+1}^n, Y_k^{2,i-1}, W_2; Y_{k,i}^2 | Z_{t,i}) + n(\epsilon_{2,n} + \gamma_{2,n}) \tag{11.212}$$

$$\leq \sum_{i=1}^{n} I(Z_{i+1}^{*,n}, Y^{*,i-1}, W_2; Y_{k,i}^2 | Z_{t,i}) + n(\epsilon_{2,n} + \gamma_{2,n}) \tag{11.213}$$

$$= \sum_{i=1}^{n} I(U_i; Y_{k,i}^2 | Z_{t,i}) + n(\epsilon_{2,n} + \gamma_{2,n}) \tag{11.214}$$

where (11.210) can be obtained by following the steps similar to (11.86)-(11.91) in Appendix 11.5.1 and (11.213) is due to the Markov chain

$$(Z_{t,i+1}^n, Y_k^{2,i-1}) \to (Z_{i+1}^{*,n}, Y^{*,i-1}) \to (W_2, Y_{k,i}^2, Z_{t,i}) \tag{11.215}$$

which is a consequence of the Markov chain in (11.2).

We now establish the bound on R_1 as follows

$$nR_1 \leq \sum_{i=1}^{n} I(W_1; Y_{j,i}^1 | W_2, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Y_{k,i}^2) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.216}$$

$$= \sum_{i=1}^{n} I(W_1; Y_{j,i}^1 | W_2, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Z_{i+1}^{*,n}, Y^{*,i-1}, Y_{k,i}^2) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.217}$$

$$= \sum_{i=1}^{n} I(W_1; Y_{j,i}^1 | U_i, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Y_{k,i}^2) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.218}$$

$$\leq \sum_{i=1}^{n} I(X_i, W_1; Y_{j,i}^1 | U_i, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Y_{k,i}^2) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.219}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{j,i}^1 | U_i, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Y_{k,i}^2) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.220}$$

$$= \sum_{i=1}^{n} H(Y_{j,i}^1 | U_i, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Y_{k,i}^2) - H(Y_{j,i}^1 | U_i, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Y_{k,i}^2, X_i)$$

$$+ n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.221}$$

$$= \sum_{i=1}^{n} H(Y_{j,i}^1 | U_i, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}, Y_{k,i}^2) - H(Y_{j,i}^1 | U_i, Y_{k,i}^2, X_i) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.222}$$

$$\leq \sum_{i=1}^{n} H(Y_{j,i}^1 | U_i, Y_{k,i}^2) - H(Y_{j,i}^1 | U_i, Y_{k,i}^2, X_i) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.223}$$

$$= \sum_{i=1}^{n} I(X_i; Y_{j,i}^1 | U_i, Y_{k,i}^2) + n(\epsilon_{1,n} + \gamma_{1,n}) \tag{11.224}$$

where (11.216) can be obtained by following the steps similar to (11.99)-(11.105) in Appendix 11.5.1, (11.217) is a consequence of the Markov chain

$$(Z_{i+1}^{*,n}, Y^{*,i-1}) \to (Y_{k,i+1}^{2,n}, Y_j^{1,i-1}) \to (W_2, W_1, Y_{j,i}^1, Y_{k,i}^2) \tag{11.225}$$

which results from the Markov chain in (11.2), (11.220) comes from the Markov chain

$$(Y_{k,i}^2, Y_{j,i}^1) \to X_i \to (W_1, W_2, U_i, Y_{k,i+1}^{2,n}, Y_j^{1,i-1}) \tag{11.226}$$

which is due to the fact that the channel is memoryless, (11.222) is also due to the Markov chain in (11.226), and (11.223) comes from the fact that conditioning cannot increase entropy.

Single-letterization can be accomplished as outlined in the proof of Theorem 11.1, completing the converse proof.

11.5.7 Proof of Theorem 11.8

The achievability of the region given in Theorem 11.8 can be shown by selecting $(U, X) = (U_1, X_1, \ldots, U_L, X_L)$ with a joint distribution of the form $p(u, x) = \prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. We next provide an outline of the converse proof. To that end, we define the following auxiliary random variables

$$U_\ell = UY^*_{[1:\ell-1]}Z^*_{[\ell+1:L],}, \quad \ell = 1, \ldots, L \tag{11.227}$$

which satisfy the Markov chains

$$U_\ell \to X_\ell \to Y^1_{j\ell} \to Y^*_\ell \to Y^2_{k\ell} \to Z^*_\ell \to Z_{t\ell}, \quad \ell = 1, \ldots, L \tag{11.228}$$

for any (j, k, t) triple. These Markov chains are a consequence of the facts that the channel is memoryless and degraded, and sub-channels are independent. Once the auxiliary random variables $\{U_\ell\}_{\ell=1}^{L}$ in (11.227) are identified, the rest of the converse proof is similar to the converse proof of Theorem 11.2 given in Appendix 11.5.2. In particular, to obtain the desired bound on R_2, we start with

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} I(U; Y^2_{k[1:L]} | Z_{t[1:L]}) \tag{11.229}$$

which is a direct consequence of Theorem 11.7. Next, following the steps similar to (11.121)-(11.126) in Appendix 11.5.2, one can reach the desired bound:

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} I(U_\ell; Y_{k\ell}^2 | Z_{t\ell}) \tag{11.230}$$

Similarly, to obtain the desired bound on R_1, we start with

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} I(X_{[1:L]}; Y_{j[1:L]}^1 | U, Y_{k[1:L]}^2) \tag{11.231}$$

which is also a direct consequence of Theorem 11.7. Next, following the steps similar to (11.130)-(11.137) in Appendix 11.5.2, one can each the desired bound:

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1 | U_\ell, Y_{k\ell}^2) \tag{11.232}$$

To complete the converse proof, we note that each expression in the bounds given by (11.230) and (11.232) depend on the the joint distribution $p(u_{[1:L]}, x_{[1:L]})$ through its marginals $p(u_\ell, x_\ell)$. Thus, there is no loss of optimality to choose $p(u_{[1:L]}, x_{[1:L]}) = \prod_{\ell=1}^{L} p(u_\ell, x_\ell)$. This completes the converse proof.

11.5.8 Proof of Theorem 11.9

According to Theorem 11.3, there exists a $P^* \leq P$ such that

$$h(X + \tilde{N}|U) - h(X + N^*|U) = \frac{1}{2} \log \frac{P^* + \tilde{\sigma}^2}{P^* + \sigma_*^2} \tag{11.233}$$

$$h(X + \tilde{N}|U) - h(X + N_2|U) \leq \frac{1}{2} \log \frac{P^* + \tilde{\sigma}^2}{P^* + \sigma_2^2} \tag{11.234}$$

$$h(X + \tilde{N}|U) - h(X + N_1|U) \geq \frac{1}{2} \log \frac{P^* + \tilde{\sigma}^2}{P^* + \sigma_1^2} \tag{11.235}$$

for any (σ_1^2, σ_2^2) as long as they satisfy

$$\sigma_1^2 \leq \sigma_*^2 \leq \sigma_2^2 \leq \tilde{\sigma}^2 \tag{11.236}$$

We first show (11.70). To this end, we note that (11.233) and (11.234) imply

$$h(X + N_2|U) - h(X + N^*|U) \geq \frac{1}{2} \log \frac{P^* + \sigma_2^2}{P^* + \sigma_*^2} \tag{11.237}$$

Furthermore, (11.233) and (11.235) imply

$$h(X + N^*|U) - h(X + N_1|U) \geq \frac{1}{2} \log \frac{P^* + \sigma_*^2}{P^* + \sigma_1^2} \tag{11.238}$$

Combining (11.237) and (11.238) yields

$$h(X + N_2|U) - h(X + N_1|U) \geq \frac{1}{2} \log \frac{P^* + \sigma_2^2}{P^* + \sigma_1^2} \tag{11.239}$$

which is the desired result in (11.70).

We now show (11.69). We first note that we can write $\tilde{N}$ as

$$\tilde{N} = N_2 + \sqrt{t}\tilde{N}_Z \tag{11.240}$$

where $\tilde{N}_Z$ is a zero-mean Gaussian random variable with variance $\sigma_Z^2 - \sigma_2^2$, and independent of (U, X, N_2). $t \in [0, 1]$ in (11.240) is given by

$$t = \frac{\tilde{\sigma}^2 - \sigma_2^2}{\sigma_Z^2 - \sigma_2^2} \tag{11.241}$$

We now use Costa's entropy power inequality [44] to arrive at (11.69)

$$e^{2h(X+\tilde{N}|U)} = e^{2h(X+N_2+\sqrt{t}\tilde{N}_Z|U)} \geq (1-t)e^{2h(X+N_2|U)} + te^{2h(X+N_Z|U)} \tag{11.242}$$

which is equivalent to

$$e^{2\left[h(X+\tilde{N}|U)-h(X+N_2|U)\right]} \geq (1-t) + te^{2[h(X+N_Z|U)-h(X+N_2|U)]} \tag{11.243}$$

which can be written as

$$h(X+N_Z|U) - h(X+N_2|U) \leq \frac{1}{2}\log\left[\frac{1}{t}e^{2\left[h(X+\tilde{N}|U)-h(X+N_2|U)\right]} - \frac{1-t}{t}\right] \tag{11.244}$$

$$\leq \frac{1}{2}\log\left[\frac{1}{t}\frac{P^* + \tilde{\sigma}^2}{P^* + \sigma_2^2} - \frac{1-t}{t}\right] \tag{11.245}$$

$$= \frac{1}{2}\log\left[\frac{P^*}{P^* + \sigma_2^2} - \frac{1}{t}\frac{\tilde{\sigma}^2 - (1-t)\sigma_2^2}{P^* + \sigma_2^2}\right] \tag{11.246}$$

$$= \frac{1}{2}\log\frac{P^* + \sigma_Z^2}{P^* + \sigma_2^2} \tag{11.247}$$

where (11.245) is due to (11.234) and (11.247) comes from (11.241). Since (11.247) is the desired result in (11.69), this completes the proof.

11.5.9 Proof of Theorem 11.10

Achievability is clear. We provide the converse proof. We fix the distribution $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$ such that

$$E\left[X_\ell^2\right] = P_\ell, \quad \ell = 1, \ldots, L \tag{11.248}$$

and $\sum_{\ell=1}^{L} P_\ell = P$. We first establish the bound on R_2 given in (11.72). To this end, we start with (11.65). Using the Markov chain $U_\ell \to Y_{k\ell}^2 \to Z_{t\ell}$, we have

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} I(U_\ell; Y_{k\ell}^2) - I(U_\ell; Z_{t\ell}) \tag{11.249}$$

$$= \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} h(Y_{k\ell}^2) - h(Z_{t\ell}) + \left[h(Z_{t\ell}|U_\ell) - h(Y_{k\ell}^2|U_\ell)\right] \tag{11.250}$$

$$\leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} \frac{1}{2} \log \frac{P_\ell + \Lambda_{k,\ell\ell}^2}{P_\ell + \Lambda_{t,\ell\ell}^Z} + \left[h(Z_{t\ell}|U_\ell) - h(Y_{k\ell}^2|U_\ell)\right] \tag{11.251}$$

where (11.251) comes from the fact that

$$h(Y_{k\ell}^2) - h(Z_{t\ell}) \tag{11.252}$$

is maximized by Gaussian distribution which can be shown by using the entropy power inequality [42, 43]. We now use Theorem 11.9. For that purpose, we introduce

$\mathbf{\Lambda}_Y^*$ and $\mathbf{\Lambda}_Z^*$ which satisfy

$$\mathbf{\Lambda}_j^1 \preceq \mathbf{\Lambda}_Y^* \preceq \mathbf{\Lambda}_k^2 \preceq \mathbf{\Lambda}_Z^* \preceq \mathbf{\Lambda}_t^Z \tag{11.253}$$

for any (j,k,t) triple, and in particular, for the diagonal, elements of these matrices, we have

$$\Lambda_{j,\ell\ell}^1 \leq \Lambda_{Y,\ell\ell}^* \leq \Lambda_{k,\ell\ell}^2 \leq \Lambda_{Z,\ell\ell}^* \leq \Lambda_{t,\ell\ell}^Z \tag{11.254}$$

for any (j,k,t,ℓ). Thus, due to Theorem 11.9, for any selection of $\{(U_\ell, X_\ell)\}_{\ell=1}^L$, we have

$$P_\ell^* \leq P_\ell \tag{11.255}$$

$$h(Z_{t\ell}|U_\ell) - h(Y_{k\ell}^2|U_\ell) \leq \frac{1}{2}\log\frac{P_\ell^* + \Lambda_{t,\ell\ell}^Z}{P_\ell^* + \Lambda_{k,\ell\ell}^2} \tag{11.256}$$

$$h(Y_{k\ell}^2|U_\ell) - h(Y_{j\ell}^1|U_\ell) \geq \frac{1}{2}\log\frac{P_\ell^* + \Lambda_{k,\ell\ell}^2}{P_\ell^* + \Lambda_{j,\ell\ell}^1} \tag{11.257}$$

for any (k,j,t,ℓ). Using (11.256) in (11.251) yields

$$R_2 \leq \min_{\substack{k=1,\ldots,K_2 \\ t=1,\ldots,K_Z}} \sum_{\ell=1}^{L} \frac{1}{2}\log\frac{P_\ell + \Lambda_{k,\ell\ell}^2}{P_\ell^* + \Lambda_{k,\ell\ell}^2} - \frac{1}{2}\log\frac{P_\ell + \Lambda_{t,\ell\ell}^Z}{P_\ell^* + \Lambda_{t,\ell\ell}^Z} \tag{11.258}$$

By defining $P_\ell^* = \beta_\ell P_\ell$ and $\bar{\beta}_\ell = 1 - \beta_\ell,\ \ell = 1,\ldots,L$, where $\beta_\ell \in [0,1]$ due to (11.255), we get the desired bound on R_2 given in (11.72).

We now bound R_1. We start with (11.64). Using the Markov chain $U_\ell \rightarrow$

$X_\ell \to Y_{j\ell}^1 \to Y_{k\ell}^2$, we have

$$R_1 \leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} I(X_\ell; Y_{j\ell}^1|U_\ell) - I(X_\ell; Y_{k\ell}^2|U_\ell) \tag{11.259}$$

$$= \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} h(Y_{j\ell}^1|U_\ell) - h(Y_{k\ell}^2|U_\ell) - \frac{1}{2}\log\frac{\Lambda_{j,\ell\ell}^1}{\Lambda_{k,\ell\ell}^2} \tag{11.260}$$

$$\leq \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} \frac{1}{2}\log\frac{P_\ell^* + \Lambda_{j,\ell\ell}^1}{P_\ell^* + \Lambda_{k,\ell\ell}^2} - \frac{1}{2}\log\frac{\Lambda_{j,\ell\ell}^1}{\Lambda_{k,\ell\ell}^2} \tag{11.261}$$

$$= \min_{\substack{j=1,\ldots,K_1 \\ k=1,\ldots,K_2}} \sum_{\ell=1}^{L} \frac{1}{2}\log\left(1 + \frac{\beta_\ell P_\ell}{\Lambda_{j,\ell\ell}^1}\right) - \frac{1}{2}\log\left(1 + \frac{\beta_\ell P_\ell}{\Lambda_{k,\ell\ell}^2}\right) \tag{11.262}$$

where (11.261) is due to (11.257). Since (11.262) is the desired bound on R_1 given in (11.71), this completes the proof.

11.5.10 Proof of Theorem 11.11

According to Theorem 11.5, for any selection of $(U, \mathbf{X})$, there exists a $\mathbf{K}^* \preceq \mathbf{S}$ such that

$$h(\mathbf{X} + \mathbf{N}^*|U) - h(\mathbf{X} + \mathbf{N}_2|U) = \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}^*|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} \tag{11.263}$$

$$h(\mathbf{X} + \mathbf{N}^*|U) - h(\mathbf{X} + \mathbf{N}_1|U) \geq \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}^*|}{|\mathbf{K}^* + \mathbf{\Sigma}_1|} \tag{11.264}$$

for any $\mathbf{\Sigma}_1$ such that $\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2$. Furthermore, $\mathbf{K}^*$ satisfies [19]

$$\mathbf{K}^* \preceq \mathbf{J}^{-1}(\mathbf{X} + \mathbf{N}^*|U) - \mathbf{\Sigma}^* \tag{11.265}$$

Equations (11.263) and (11.264) already imply

$$h(\mathbf{X}+\mathbf{N}_2|U) - h(\mathbf{X}+\mathbf{N}_1|U) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_2|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{11.266}$$

for any $\mathbf{\Sigma}_1$ such that $\mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2$, which is the desired inequality in (11.76).

We now prove (11.75). For that purpose, we note that (11.265) implies

$$\mathbf{K}^* \preceq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}|U) - \mathbf{\Sigma}_N \tag{11.267}$$

for any Gaussian random vector $\mathbf{N}$, independent of $(U, \mathbf{X})$, with covariance matrix $\mathbf{\Sigma}_N$ such that $\mathbf{\Sigma}_N \succeq \mathbf{\Sigma}^*$ because of Lemma 5.16. The order in (11.267) is equivalent to

$$\mathbf{J}(\mathbf{X}+\mathbf{N}|U) \preceq (\mathbf{K}^*+\mathbf{\Sigma}_N)^{-1}, \quad \mathbf{\Sigma}^* \preceq \mathbf{\Sigma}_N \tag{11.268}$$

Now, we can obtain (11.75) as follows

$$\begin{aligned}
&h(\mathbf{X}+\mathbf{N}_Z|U) - h(\mathbf{X}+\mathbf{N}_2|U) \\
&\quad = h(\mathbf{X}+\mathbf{N}_Z|U) - h(\mathbf{X}+\mathbf{N}^*|U) + h(\mathbf{X}+\mathbf{N}^*|U) - h(\mathbf{X}+\mathbf{N}_2|U) && (11.269)\\
&\quad = h(\mathbf{X}+\mathbf{N}_Z|U) - h(\mathbf{X}+\mathbf{N}^*|U) + \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}^*|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} && (11.270)\\
&\quad = \frac{1}{2}\int_{\mathbf{\Sigma}^*}^{\mathbf{\Sigma}_Z} \mathbf{J}(\mathbf{X}+\mathbf{N}|U)\; d\mathbf{\Sigma}_N + \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}^*|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} && (11.271)\\
&\quad \leq \frac{1}{2}\int_{\mathbf{\Sigma}^*}^{\mathbf{\Sigma}_Z} (\mathbf{K}^*+\mathbf{\Sigma}_N)^{-1} d\mathbf{\Sigma}_N + \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}^*|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} && (11.272)
\end{aligned}$$

$$\leq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{11.273}$$

where (11.270) is due to (11.263), (11.271) is obtained by using Lemma 5.17, and (11.272) comes from Lemma 5.8 by noting (11.268). Since (11.273) is the desired inequality in (11.75), this completes the proof.

11.5.11 Proof of Theorem 11.12

We first establish the desired bound on R_2 given in (11.78) as follows

$$R_2 \leq \min_{t=1,\ldots,K_Z} I(U;\mathbf{Y}^2) - I(U;\mathbf{Z}_t) \tag{11.274}$$

$$= \min_{t=1,\ldots,K_Z} h(\mathbf{Y}^2) - h(\mathbf{Z}_t) + \big[h(\mathbf{Z}_t|U) - h(\mathbf{Y}^2|U)\big] \tag{11.275}$$

$$\leq \min_{t=1,\ldots,K_Z} \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}^2|}{|\mathbf{S}+\mathbf{\Sigma}_t^Z|} + \big[h(\mathbf{Z}_t|U) - h(\mathbf{Y}^2|U)\big] \tag{11.276}$$

where (11.274) comes from Theorem 11.7 by noting the Markov chain $U \to \mathbf{Y}^2 \to \mathbf{Z}_t$, and (11.276) can be obtained by using the worst additive noise lemma, i.e., Lemma 11.2, as it is done in the proof of Theorem 11.6. We now use Theorem 11.11. According to Theorem 11.11, for any selection of $(U,\mathbf{X})$, there exists a positive semi-definite matrix $\mathbf{K}$ such that $\mathbf{K} \preceq \mathbf{S}$ and

$$h(\mathbf{Z}_t|U) - h(\mathbf{Y}^2|U) \leq \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_t^Z|}{|\mathbf{K}+\mathbf{\Sigma}^2|} \tag{11.277}$$

$$h(\mathbf{Y}^2|U) - h(\mathbf{Y}_j^1|U) \geq \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}^2|}{|\mathbf{K}+\mathbf{\Sigma}_j^1|} \tag{11.278}$$

for any (j,t) pair. Using (11.277) in (11.276) yields

$$R_2 \leq \min_{t=1,\ldots,K_Z} \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}^2|}{|\mathbf{K}+\mathbf{\Sigma}^2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_t^Z|}{|\mathbf{K}+\mathbf{\Sigma}_t^Z|} \tag{11.279}$$

which is the desired bound on R_2 given in (11.78).

We now obtain the desired bound on R_1 given in (11.77) as follows

$$R_1 \leq \min_{j=1,\ldots,K_1} I(\mathbf{X};\mathbf{Y}_j^1|U) - I(\mathbf{X};\mathbf{Y}^2|U) \tag{11.280}$$

$$= \min_{j=1,\ldots,K_1} h(\mathbf{Y}_j^1|U) - h(\mathbf{Y}^2|U) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}^2|} \tag{11.281}$$

$$\leq \min_{j=1,\ldots,K_1} \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}_j^1|}{|\mathbf{\Sigma}_j^1|} - \frac{1}{2}\log\frac{|\mathbf{K}+\mathbf{\Sigma}^2|}{|\mathbf{\Sigma}^2|} \tag{11.282}$$

where (11.280) comes from Theorem 11.7 by noting the Markov chain $U \to \mathbf{X} \to \mathbf{Y}_j^1 \to \mathbf{Y}^2$ and (11.282) is obtained by using (11.278). Since (11.282) is the desired bound on R_1 given in (11.77), this completes the proof.

Chapter 12

Ergodic Secrecy Capacity Region of the Fading Broadcast Channel

12.1 Introduction

In this chapter, we study the two-user fading broadcast channel from a secrecy point of view. Previous works on this subject are reported in [24, 26, 27, 95–98]. References [26, 27, 95] obtain the ergodic secrecy capacity for the fading wiretap channel when the channel state information (CSI) of both the legitimate receiver and the eavesdropper are available at all terminals. The ergodic secrecy capacity gives the amount of confidential information that the transmitter can send to the receiver, when the receiver can afford arbitrarily long delays, hence can average its secrecy rate over all channel realizations. The case where the transmitter has the CSI of only the legitimate receiver (but not the eavesdropper) is studied in [24, 95, 96] from the ergodic secrecy perspective. Reference [95] obtains the ergodic secrecy capacity for a slow-fading channel, and [24, 96] provide achievable rates for a fast fading channel.

When the receiver is delay-intolerant, the related information theoretic measure for fading channels is the outage capacity (delay-limited capacity), which is the amount of information that can be transmitted within a certain time [99]. The outage probability, and hence, the outage capacity, of the fading wiretap channel is derived in [26, 97, 98]. The outage probability denotes the fraction of time that the

legitimate receiver cannot get a pre-specified target secrecy rate.

In this chapter, we study the two-user fading broadcast channel with confidential messages, where the transmitter sends a confidential message to each user that needs to be kept hidden from the other user. Hence, our work generalizes [26, 27, 95], where only one of the receivers requires confidential communication, to a symmetric setting, where both receivers want to have confidential communication with the transmitter. Similar to [26, 27], we assume that the CSI is available to all parties perfectly and instantaneously.

We first consider the parallel less noisy broadcast channel with confidential messages, where, in each sub-channel, one user's channel is less noisy than the other user's channel. We note that, in each sub-channel, the less noisiness order might be different, hence, the overall channel is not less noisy. The parallel Gaussian broadcast channel is inherently a parallel less noisy channel, and hence, using the secrecy capacity region we find, we explicitly evaluate the secrecy capacity region of the parallel Gaussian broadcast channel by finding the optimal input distribution.

We then consider the ergodic secrecy capacity region of the fading broadcast channel by assuming that there are no delay constraints, i.e., each receiver can wait arbitrarily long to decode its message enabling the codeword to experience all possible channel realizations. Consequently, the achievable rate becomes an average of the rates achievable at all channel states. Moreover, under this scenario, the entire fading broadcast channel can be viewed as a parallel Gaussian broadcast channel; each sub-channel corresponding to a particular realization of the channel state. This observation enables us to obtain the secrecy capacity region of the fading broadcast

channel by using the capacity results we obtain for parallel Gaussian broadcast channels. We finally present some numerical results which demonstrate that fading enables both users to have positive secrecy rates which is impossible for scalar non-fading Gaussian broadcast channels.

12.2 Parallel Less Noisy Broadcast Channels with Confidential Messages

We consider the parallel less noisy broadcast channel, where in each sub-channel, one user's channel is less noisy with respect to the other user. However, the overall channel is not less noisy for any one of the users, as discussed earlier. The transmitter sends an individual confidential message to each user that needs to be kept hidden from the other user, in addition to a common message that needs to be delivered to both users.

This channel consists of one input alphabet $x = (x_1, \ldots, x_L) \in \mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_L$ and two output alphabets $y_j = (y_{j1}, \ldots, y_{jL}) \in \mathcal{Y}_j = \mathcal{Y}_{j1} \times \ldots \times \mathcal{Y}_{jL}, j = 1, 2$, where $x_\ell, \ell = 1, \ldots, L$, is the input to the ℓth sub-channel and $y_{j\ell}, j = 1, 2, \ell \in \{1, \ldots, L\}$, is the output of the jth user's ℓth sub-channel. The channel transition probability is given by

$$p(y_{11}^n, y_{21}^n, \ldots, y_{1L}^n, y_{2L}^n | x_1^n, \ldots, x_L^n) = \prod_{\ell=1}^{L} \prod_{i=1}^{n} p(y_{1\ell,i}, y_{2\ell,i} | x_{\ell,i}) \tag{12.1}$$

which implies that the sub-channels are all independent and each sub-channel is

memoryless. Furthermore, in each sub-channel, one user's channel is less noisy with respect to the other user, i.e., for any random variable U satisfying the Markov chain $U \to X_\ell \to (Y_{1\ell}, Y_{2\ell})$, we have [3]

$$I(U;Y_{1\ell}) > I(U;Y_{2\ell}), \quad \ell \in \mathcal{S}_1 \tag{12.2}$$

$$I(U;Y_{2\ell}) > I(U;Y_{1\ell}), \quad \ell \in \mathcal{S}_2 \tag{12.3}$$

where $\mathcal{S}_j$, $j = 1, 2$, is the set of the sub-channel indices in which user j's channel is less noisy. We remark that as long as $\mathcal{S}_j \neq \{1, \ldots, L\}$, $j = 1, 2$, the overall channel is not less noisy for any one of the users.

An $(n, 2^{nR_0}, 2^{nR_1}, 2^{nR_2})$ code for this channel consists of three message sets $\mathcal{W}_0 = \left\{1, \ldots, 2^{nR_0}\right\}$, $\mathcal{W}_j = \left\{1, \ldots, 2^{nR_j}\right\}, j = 1, 2$, one encoder $f : \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}_1^n \times \ldots \times \mathcal{X}_L^n$ and two decoders, one at each receiver, $g_j : \mathcal{Y}_{j1}^n \times \ldots \mathcal{Y}_{jL}^n \to \mathcal{W}_0 \times \mathcal{W}_j, j = 1, 2$. The probability of error for the jth user is defined as $P_{e,j}^n = \Pr\left[(\hat{W}_0, \hat{W}_j) \neq (W_0, W_j)\right], j = 1, 2$, where $(\hat{W}_0, \hat{W}_j)$ is the output of the jth user's decoder. The secrecy of the code is measured through equivocation rates which are $\frac{1}{n}H(W_1|Y_2^n), \frac{1}{n}H(W_2|Y_1^n)$.

A rate tuple (R_0, R_1, R_2) is said to be achievable if there exist codes such that $\lim_{n\to\infty} P_{e,j}^n = 0, j = 1, 2$, and

$$\lim_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n) \geq R_1, \quad \lim_{n\to\infty} \frac{1}{n} H(W_2|Y_1^n) \geq R_2 \tag{12.4}$$

Thus, our focus will be on the perfect secrecy rates.

The secrecy capacity region of this channel is given by the following theorem.

Theorem 12.1 *The secrecy capacity region of the parallel less noisy broadcast channel is given by the union of the rate tuples* (R_0, R_1, R_2) *satisfying*

$$R_0 \leq \min\left[\sum_{\ell=1}^{L} I(U_\ell; Y_{1\ell}), \sum_{\ell=1}^{L} I(U_\ell; Y_{2\ell})\right] \tag{12.5}$$

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} \Big[I(X_\ell; Y_{1\ell}|U_\ell) - I(X_\ell; Y_{2\ell}|U_\ell)\Big] \tag{12.6}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} \Big[I(X_\ell; Y_{2\ell}|U_\ell) - I(X_\ell; Y_{1\ell}|U_\ell)\Big] \tag{12.7}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$.

The proof of this theorem is given in Appendix 12.7.1.

Remark 12.1 *The capacity achieving scheme uses all of the sub-channels to transmit the common message on which, of course, no secrecy constraint is imposed. The confidential messages of user* j *are sent over the sub-channels where user* j *has a less noisy observation with respect to the other user, i.e., over sub-channels in* $\mathcal{S}_j$.

Remark 12.2 *The region given in Theorem 12.1 remains unchanged if we let arbitrary correlation among* $\{u_\ell, x_\ell\}_{\ell=1}^{L}$ *because all of the expressions in Theorem 12.1 depend on one of the distributions* $\{p(u_\ell, x_\ell, y_{1\ell}, y_{2\ell})\}_{\ell=1}^{L}$, *but not on any joint distributions across sub-channels. Thus, the use of independent inputs for each sub-channel is capacity achieving.*

We now consider a special instance of this channel, where in each sub-channel, one of the users' channel is degraded with respect to the other user. For this so-called

parallel degraded broadcast channel, we have,

$$X_\ell \to Y_{1\ell} \to Y_{2\ell}, \quad \ell \in \mathcal{S}_1 \tag{12.8}$$

$$X_\ell \to Y_{2\ell} \to Y_{1\ell}, \quad \ell \in \mathcal{S}_2 \tag{12.9}$$

We note that the channels satisfying (12.8)-(12.9) satisfy (12.2)-(12.3). We also note that since the user which has degraded channel can be different in each sub-channel, the overall channel is not degraded for any one of the users. In other words, as long as $\mathcal{S}_j \neq \{1, \ldots, L\}, j = 1, 2$, the overall channel is not degraded. The secrecy capacity region of the parallel degraded broadcast channel is given as follows.

Corollary 12.1 *The secrecy capacity region of the parallel degraded broadcast channel is given by the union of the rate tuples* (R_0, R_1, R_2) *satisfying*

$$R_0 \leq \min \left[\sum_{\ell=1}^{L} I(U_\ell; Y_{1\ell}), \sum_{\ell=1}^{L} I(U_\ell; Y_{2\ell}) \right] \tag{12.10}$$

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{1\ell} | U_\ell, Y_{2\ell}) \tag{12.11}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} I(X_\ell; Y_{2\ell} | U_\ell, Y_{1\ell}) \tag{12.12}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(u_\ell, x_\ell)$.

We now specialize the result in Corollary 12.1 to the case where there is no common message to be transmitted.

Corollary 12.2 *The secrecy capacity region of the parallel degraded broadcast channel without a common message is given by the union of the rate pairs* (R_1, R_2) *sat-*

isfying

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{1\ell}|Y_{2\ell}) \tag{12.13}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} I(X_\ell; Y_{2\ell}|Y_{1\ell}) \tag{12.14}$$

where the union is over all distributions of the form $\prod_{\ell=1}^{L} p(x_\ell)$.

12.3 Parallel Gaussian Broadcast Channels

We now consider the two-user parallel Gaussian broadcast channel with L independent sub-channels. The ℓth, $\ell \in \{1, \ldots, L\}$, sub-channel is described by

$$Y_{1\ell,i} = h_{1\ell} X_{\ell,i} + N_{1\ell,i} \tag{12.15}$$

$$Y_{2\ell,i} = h_{2\ell} X_{\ell,i} + N_{2\ell,i} \tag{12.16}$$

where for any given $\ell \in \{1, \ldots, L\}$ and $j = 1, 2$, the noise process $\{N_{j\ell,i}\}_{i=1}^{n}$ has components which are i.i.d. Gaussian with zero-mean and unit-variance. Moreover, the noise processes of different sub-channels are independent implying the independence of the sub-channels. We have an average power constraint on the input signal as

$$\frac{1}{n} \sum_{i=1}^{n} \sum_{\ell=1}^{L} x_{\ell,i}^2 \leq P \tag{12.17}$$

We want to obtain the secrecy capacity region of this channel. To this end, we

first show that the parallel Gaussian broadcast channel is an instance of the parallel degraded broadcast channel described in the previous section in Corollaries 12.1 and 12.2. To see this point, we argue that the secrecy capacity region of the parallel Gaussian broadcast channel is invariant with respect to the correlation between $N_{1\ell,i}$ and $N_{2\ell,i}$. Since each user decodes its own message and gets information about the other user's message only through its own observation, the only probability distribution that matters is the marginal distribution of the channel, i.e., $p(y_{1\ell,i}|x_{\ell,i})$ and $p(y_{2\ell,i}|x_{\ell,i})$, but not the joint distribution $p(y_{1\ell,i}, y_{2\ell,i}|x_{\ell,i})$. Hence, the correlation between $N_{1\ell,i}$ and $N_{2\ell,i}$ for any given ℓ has no effect on the secrecy capacity region of the parallel Gaussian broadcast channel [26]. Therefore, we can introduce an equivalent Gaussian channel which is defined for $\ell \in \mathcal{S}_1$ by

$$Y_{1\ell,i} = h_{1\ell}X_{\ell,i} + N_{1\ell,i}, \quad \tilde{Y}_{2\ell,i} = \frac{h_{2\ell}}{h_{1\ell}}Y_{1\ell,i} + \tilde{N}_{2\ell,i} \tag{12.18}$$

and for $\ell \in \mathcal{S}_2$ by

$$Y_{2\ell,i} = h_{2\ell}X_{\ell,i} + N_{2\ell,i} \quad \tilde{Y}_{1\ell,i} = \frac{h_{1\ell}}{h_{2\ell}}Y_{2\ell,i} + \tilde{N}_{1\ell,i} \tag{12.19}$$

where the sets $\mathcal{S}_1$ and $\mathcal{S}_2$ are given by

$$\mathcal{S}_1 = \{\ell : h_{1\ell} > h_{2\ell}\}, \quad \mathcal{S}_2 = \{\ell : h_{2\ell} > h_{1\ell}\} \tag{12.20}$$

and $\tilde{N}_{1\ell,i}$, $\tilde{N}_{2\ell,i}$ are Gaussian with zero-mean and variances $1 - (h_{1\ell}/h_{2\ell})^2$, $1 - (h_{2\ell}/h_{1\ell})^2$, respectively, and they are independent of each other and the rest of

the random variables. Since the channel described by (12.18)-(12.19) satisfies the degradedness conditions in (12.8)-(12.9), it is a parallel degraded broadcast channel. Thus, the secrecy capacity region of the parallel Gaussian broadcast channel is given by Corollaries 12.1 and 12.2. Moreover, since the channels described by (12.15)-(12.16) and (12.18)-(12.19) have the same marginal distributions, they have the same secrecy capacity region.

Theorem 12.2 *The secrecy capacity region of the parallel Gaussian broadcast channel is given by the union of the rate pairs* (R_1, R_2) *satisfying*

$$R_1 \leq \frac{1}{2} \sum_{\ell \in \mathcal{S}_1} \Big[\log(1 + \alpha_{1\ell} h_{1\ell}^2) - \log(1 + \alpha_{1\ell} h_{2\ell}^2) \Big] \tag{12.21}$$

$$R_2 \leq \frac{1}{2} \sum_{\ell \in \mathcal{S}_2} \Big[\log(1 + \alpha_{2\ell} h_{2\ell}^2) - \log(1 + \alpha_{2\ell} h_{1\ell}^2) \Big] \tag{12.22}$$

where the union is over all $\beta \in [0, 1]$*, and* $\{\alpha_{j\ell}\}_{\ell \in \mathcal{S}_j}, j = 1, 2$*, are defined by*

$$\alpha_{1\ell} = \left[-\frac{1}{2} \left(\frac{1}{h_{1\ell}^2} + \frac{1}{h_{2\ell}^2} \right) + \frac{1}{2} \sqrt{\left(\frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2} \right)^2 + \frac{2P}{\lambda_1} \left(\frac{1}{h_{2\ell}^2} - \frac{1}{h_{1\ell}^2} \right)} \right]^+ \tag{12.23}$$

$$\alpha_{2\ell} = \left[-\frac{1}{2} \left(\frac{1}{h_{1\ell}^2} + \frac{1}{h_{2\ell}^2} \right) + \frac{1}{2} \sqrt{\left(\frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2} \right)^2 + \frac{2P}{\lambda_2} \left(\frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2} \right)} \right]^+ \tag{12.24}$$

where $(x)^+ = \max(0, x)$*, and* λ_1, λ_2 *are selected to satisfy*

$$\sum_{\ell \in \mathcal{S}_1} \alpha_{1\ell} = \beta P, \qquad \sum_{\ell \in \mathcal{S}_2} \alpha_{2\ell} = (1 - \beta) P \tag{12.25}$$

Remark 12.3 *If we set one of the users' secrecy rate to zero, we can recover the*

secrecy capacity of the parallel Gaussian wiretap channel found in [26, 27].

The proof of this theorem is given in Appendix 12.7.2. The proof consists of two steps. In the first step, we identify the input distribution maximizing the terms in Corollary 12.2, which is Gaussian [49]. Secondly, we compute the optimal power allocation to obtain the boundary of the capacity region. The resulting optimal power allocation scheme is reminiscent of the water-filling solution, however, here we use the difference of the noise levels in each sub-channel, as the "base of the tank" on which we water-fill. More precisely, the water-filling solution here considers the difference

$$\left| \frac{1}{h_{1\ell}^2} - \frac{1}{h_{2\ell}^2} \right| \tag{12.26}$$

which can be viewed as the difference between the effective noise levels of the two users in sub-channel ℓ, because $h_{j\ell}^2$ is the signal-to-noise ratio of the jth user in the ℓth sub-channel. Consequently, if this difference is sufficiently large, then the corresponding sub-channel is used, otherwise it is not used.

12.4 Ergodic Secrecy Capacity Region of the Fading Broadcast Channel

We now consider the fading broadcast channel which is given by

$$Y_{1,i} = h_{1,i}X_i + N_{1,i} \tag{12.27}$$

$$Y_{2,i} = h_{2,i}X_i + N_{2,i} \tag{12.28}$$

where $\{N_{j,i}\}_{i=1}^{n},\ j = 1, 2$, is an i.i.d. Gaussian random sequence with zero-mean and unit-variance. We assume that the fading processes $\{h_{j,i}\}_{i=1}^{n},\ j = 1, 2$, are ergodic and stationary. We have the power constraint on the channel input as $(1/n)\sum_{i=1}^{n} x_i^2 \leq P$. The joint cumulative probability distribution of $(h_{1,i}, h_{2,i})$ is denoted by $F(\mathbf{h})$.

We want to obtain the secrecy capacity region of this fading broadcast channel. We assume that CSI of both users $\mathbf{h}_i = (h_{1,i}, h_{2,i})$ is instantaneously known by all parties. We further assume that none of the users has a delay constraint on the transmission, thus the notion of ergodic capacity can be used. To find the corresponding secrecy capacity region, we invoke the equivalence of the fading broadcast channel channel with the parallel Gaussian broadcast channel which was studied in Section 12.3. Thus, we use the secrecy capacity region of the parallel Gaussian broadcast channel given in Theorem 12.2 to obtain the ergodic secrecy capacity of the fading broadcast channel.

Corollary 12.3 *The ergodic secrecy capacity region of the fading broadcast channel*

is given by the union of the rate pairs (R_1, R_2) *satisfying*

$$R_1 \leq \frac{1}{2}\int_{\mathcal{H}_1}\Big[\log\left(1+\alpha_1(\mathbf{h})h_1^2\right)-\log\left(1+\alpha_1(\mathbf{h})h_2^2\right)\Big]dF(\mathbf{h}) \tag{12.29}$$

$$R_2 \leq \frac{1}{2}\int_{\mathcal{H}_2}\Big[\log\left(1+\alpha_2(\mathbf{h})h_2^2\right)-\log\left(1+\alpha_2(\mathbf{h})h_1^2\right)\Big]dF(\mathbf{h}) \tag{12.30}$$

where the union is over all $\beta \in [0,1]$*, and the regions* $\mathcal{H}_1, \mathcal{H}_2$ *are defined by*

$$\mathcal{H}_1 = \{\mathbf{h} : h_1 > h_2\}, \quad \mathcal{H}_2 = \{\mathbf{h} : h_2 > h_1\} \tag{12.31}$$

Here, $\{\alpha_j(\mathbf{h})\}_{j=1}^2$ *are also given by (12.23)-(12.24) and* λ_1, λ_2 *are selected to satisfy*

$$\int_{\mathcal{H}_1}\alpha_1(\mathbf{h})dF(\mathbf{h}) = \beta P, \ \int_{\mathcal{H}_2}\alpha_2(\mathbf{h})dF(\mathbf{h}) = (1-\beta)P \tag{12.32}$$

Remark 12.4 *If we set one of the users' secrecy rate to zero, we can recover the ergodic secrecy capacity of the fading wiretap channel found in [26, 27].*

Remark 12.5 *We only assumed that the fading processes* $\{h_{j,i}\}_{i=1}^n$*,* $j = 1, 2$*, are ergodic and stationary, and did not impose any restrictions on the correlation structure. Consequently, Corollary 12.3 gives the secrecy capacity region for any ergodic and stationary fading process.*

This corollary is a direct consequence of Theorem 12.2. To adopt the corresponding result, we need to identify the channel states which are equivalent to the sub-channels of a parallel Gaussian broadcast channel. Thus, we define the sets $\mathcal{H}_j, j = 1, 2$, which are similar to $\mathcal{S}_j, j = 1, 2$. Consequently, when the first (resp.

second) user has a stronger channel in the sense that $h_1 > h_2$ (resp. $h_2 > h_1$), first (resp. second) user's confidential message is transmitted. Moreover, using Theorem 12.2, we also obtain the optimal power allocations $\alpha_1(\mathbf{h})$ and $\alpha_2(\mathbf{h})$ that give the boundary of the secrecy capacity region.

12.5 Numerical Results

We now present some numerical illustrations for the ergodic secrecy capacity region. We select h_1, h_2 to be independent Rayleigh random variables. Consequently, the powers of the channel gains, i.e., h_1^2 and h_2^2, are exponential random variables with mean values σ_1 and σ_2, respectively. The difference between these mean values can be viewed as a measure of the relative strengths of the users' channels on average. Thus, we expect that the user that has a larger mean value would have larger secrecy rates. In Figure 12.1, ergodic secrecy capacity region is given for two different sets of $\{\sigma_1, \sigma_2\}$. For the first set, we have $\sigma_1 = \sigma_2 = 1$ which results in a symmetric ergodic secrecy capacity region. For the second set, we select $\sigma_1 = 1, \sigma_2 = 0.5$. Since user 2's average signal-to-noise ratio is lower in this case, the maximum secrecy rate of user 1 is larger while the maximum secrecy rate of user 2 is lower.

To observe the effect of optimal power allocation, we compute the achievable secrecy region obtained by using a uniform power allocation, i.e., $\alpha_1(\mathbf{h})$ (resp. $\alpha_2(\mathbf{h})$) is selected to be constant over $\mathcal{H}_1$ (resp. $\mathcal{H}_2$). The corresponding plot is given in Figure 12.2. We note that the optimal power allocation offers a significant advantage over the suboptimal uniform power allocation. This also implies that the availability

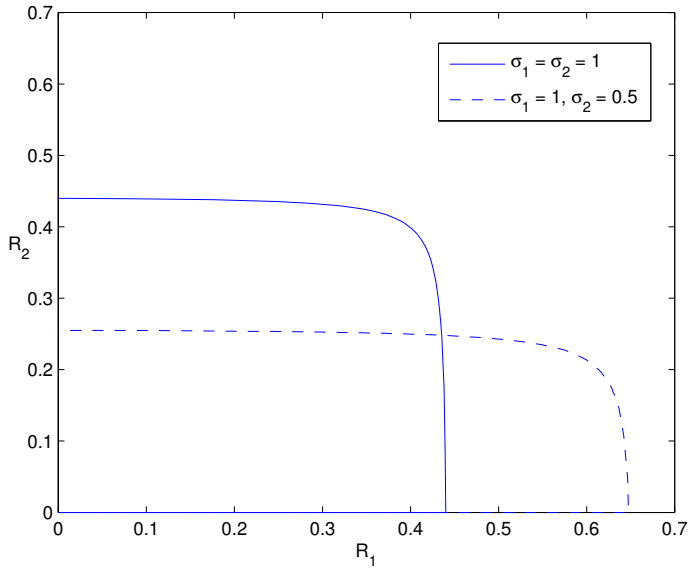

Figure 12.1: Ergodic secrecy capacity region for different mean values of the fading distribution. The average power, P, is 5 dB.

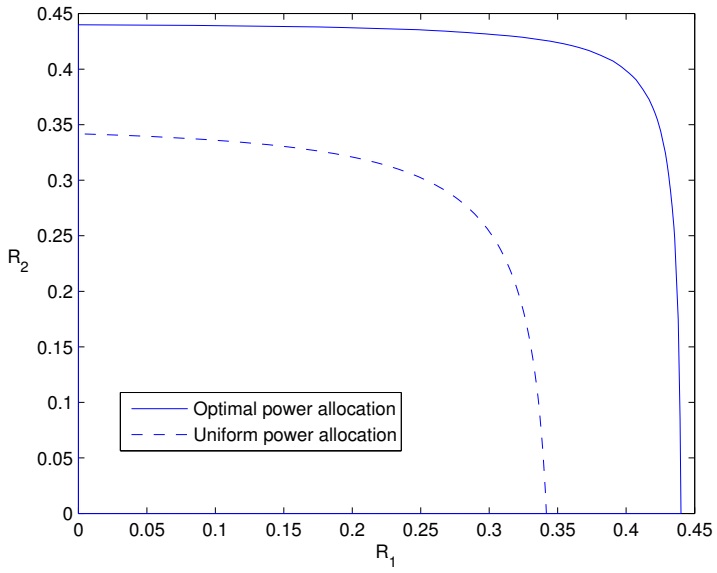

Figure 12.2: Comparison of the ergodic secrecy capacity region and an achievable secrecy region obtained by using a uniform power allocation. The average power, P, is 5 dB.

of the CSI at the transmitter results in a noticeable secrecy rate gain.

12.6 Conclusions

In this chapter, we study the two-user fading broadcast channel with confidential messages. We first obtain the secrecy capacity region of the parallel less noisy broadcast channel, where, in each sub-channel, one of the users is less noisy with respect to the other user. This model subsumes the parallel Gaussian broadcast channel, enabling us to obtain the secrecy capacity region of the parallel Gaussian channel. Finally, using the equivalence between the parallel Gaussian broadcast channel and the fading broadcast channel, we establish the ergodic secrecy capacity region of the fading broadcast channel.

12.7 Appendix

12.7.1 Proof of Theorem 12.1

12.7.1.1 Achievability

We prove the achievability of the region given Theorem 12.1. We use an encoding scheme where the common message is sent through all subchannels and the jth user's confidential messages is sent through the subchannels in $\mathcal{S}_j,\ j = 1, 2$. Our achievable scheme uses a stochastic encoder for each user's confidential message. This stochastic encoder associates each confidential message with many codewords

in order to confuse the other user. Fix the probability distribution

$$\prod_{\ell=1}^{L} p(u_\ell, x_\ell) p(y_{1\ell}, y_{2\ell}|x_\ell) \tag{12.33}$$

Codebook generation:

- Generate 2^{nR_0} length-n sequences $\mathbf{u}_\ell$ through $p(\mathbf{u}_\ell) = \prod_{i=1}^{n} p(u_{\ell,i})$ and index them as $\mathbf{u}_\ell(w_0)$ where $w_0 \in \left\{1, \ldots, 2^{nR_0}\right\}$ for $\ell = 1, \ldots, L$.

- For each $\ell \in \mathcal{S}_1$ and corresponding $\mathbf{u}_\ell$, generate $2^{n(R_1+\tilde{R}_{1\ell})}$ length-n sequences $\mathbf{x}_\ell$ through $p(\mathbf{x}_\ell|\mathbf{u}_\ell) = \prod_{i=1}^{n} p(x_{\ell,i}|u_{\ell,i})$ and index them as $\mathbf{x}_\ell(w_1, \tilde{w}_{1\ell})$ where $w_1 \in \left\{1, \ldots, 2^{nR_1}\right\}$, $\tilde{w}_{1\ell} \in \left\{1, \ldots, 2^{n\tilde{R}_{1\ell}}\right\}$.

- For each $\ell \in \mathcal{S}_2$ and corresponding $\mathbf{u}_\ell$, generate $2^{n(R_2+\tilde{R}_{2\ell})}$ length-n sequences $\mathbf{x}_\ell$ through $p(\mathbf{x}_\ell|\mathbf{u}_\ell) = \prod_{i=1}^{n} p(x_{\ell,i}|u_{\ell,i})$ and index them as $\mathbf{x}_\ell(w_2, \tilde{w}_{2\ell})$ where $w_2 \in \left\{1, \ldots, 2^{nR_2}\right\}$, $\tilde{w}_{2\ell} \in \left\{1, \ldots, 2^{n\tilde{R}_{2\ell}}\right\}$.

- Furthermore, we set the rates of dummy codewords as

$$\tilde{R}_{1\ell} = I(X_\ell; Y_{2\ell}|U_\ell), \quad \ell \in \mathcal{S}_1 \tag{12.34}$$

$$\tilde{R}_{2\ell} = I(X_\ell; Y_{1\ell}|U_\ell), \quad \ell \in \mathcal{S}_2 \tag{12.35}$$

Encoding:

If (w_0, w_1, w_2) is the message tuple to be sent, then randomly pick the dummy message indices $\{\tilde{w}_{1\ell}\}_{\ell\in\mathcal{S}_1}$, $\{\tilde{w}_{2\ell}\}_{\ell\in\mathcal{S}_2}$ and transmit $\mathbf{x}_\ell(w_0, w_1, \tilde{w}_{1\ell})$, $\mathbf{x}_\ell(w_0, w_2, \tilde{w}_{2\ell})$ through the subchannels in $\mathcal{S}_1$ and $\mathcal{S}_2$, respectively.

Decoding:

- Each user decodes the common message using all its channel outputs and employs joint typical decoding. Consider user 1. If w_0 is the unique message for which we have $(\mathbf{u}_\ell(w_0), \mathbf{y}_{1\ell}) \in A_\epsilon^n$ for all $\ell \in \{1, \ldots, L\}$,where A_ϵ^n is the set of typical sequences, then it is decoded as w_0. For the error analysis, we define the events

$$\mathcal{E}_{w_0,\ell}^1 = \left\{(\mathbf{u}_\ell(w_0), \mathbf{y}_{1\ell}) \in A_\epsilon^n\right\}, \quad \forall \ell \in 1, \ldots, L \tag{12.36}$$

$$\mathcal{E}_{w_0}^1 = \bigcap_{\ell \in \{1,\ldots,L\}} \mathcal{E}_{w_0,\ell}^1 \tag{12.37}$$

Assuming $w_0 = 1$ is transmitted, error probability is given by

$$P_e^n = \Pr\left[\mathcal{E}_1^{1,c} \cup \mathcal{E}_2^1 \cup \ldots \cup \mathcal{E}_{2^{nR_0}}^1\right] \tag{12.38}$$

$$\leq \Pr\left[\mathcal{E}_1^{1,c}\right] + \sum_{\substack{j=1 \\ j\neq 1}}^{2^{nR_0}} \Pr\left[\mathcal{E}_j^1\right] \tag{12.39}$$

$$= \Pr\left[\mathcal{E}_1^{1,c}\right] + \sum_{\substack{j=1 \\ j\neq 1}}^{2^{nR_0}} \prod_{\ell=1}^{L} \Pr\left[\mathcal{E}_{j,\ell}^1\right] \tag{12.40}$$

where (12.39) comes from the union bound and (12.40) is a consequence of the independence of subchannels and the codebooks. Since $w_0 = 1$, we have $\Pr\left[(\mathbf{u}_\ell(1), \mathbf{y}_{1\ell}) \notin A_\epsilon^n\right] \leq \frac{\epsilon_n}{L}$ for all $\ell \in \{1, \ldots, L\}$ which implies

$$\Pr\left[\mathcal{E}_1^{1,c}\right] = \Pr\left[\left(\cap_{\ell=1}^L \mathcal{E}_{1,\ell}^1\right)^c\right] \leq \sum_{\ell=1}^{L} \Pr\left[\mathcal{E}_{1,\ell}^{1,c}\right] \leq \epsilon_n \tag{12.41}$$

Furthermore, using (12.41) and the following bound

$$\Pr\left[\mathcal{E}_{j,\ell}^{1}\right] \leq 2^{-n[I(U_\ell;Y_{1\ell})-\epsilon_n']} \tag{12.42}$$

in (12.40), we conclude that the rates satisfying

$$R_0 \leq \sum_{\ell=1}^{L} I(U_\ell; Y_{1\ell}) \tag{12.43}$$

can be decoded by user 1 with vanishingly small error probability. Similarly, we can show that the common message rate needs to satisfy

$$R_0 \leq \sum_{\ell=1}^{L} I(U_\ell; Y_{2\ell}) \tag{12.44}$$

- User 1 decodes w_1 using the subchannels in $\mathcal{S}_1$. Assume that it has decoded w_0 correctly. Then, if w_1 is the unique message for which we have

$$\{\exists \tilde{w}_1 : (\mathbf{x}_{1\ell}(w_0, w_1, \tilde{w}_1), \mathbf{y}_{1\ell}) \in A_\epsilon^n\} \tag{12.45}$$

for all $\ell \in \mathcal{S}_1$, then it is decoded as w_1. We define the events

$$\mathcal{E}_{w_1,\ell} = \{\exists \tilde{w}_1 : (\mathbf{x}_{1\ell}(w_0, w_1, \tilde{w}_1), \mathbf{y}_{1\ell}) \in A_\epsilon^n\}, \quad \ell \in \mathcal{S}_1 \tag{12.46}$$

and $\mathcal{E}_{w_1} = \bigcap_{\ell\in\mathcal{S}_1} \mathcal{E}_{w_1,\ell}$. Assume $w_1 = 1$ is transmitted. The error probability

is given by

$$P_e^n = \Pr\left[\mathcal{E}_1^c \cup \mathcal{E}_2 \cup \ldots \cup \mathcal{E}_{2^{nR_1}}\right] \tag{12.47}$$

$$\leq \Pr\left[\mathcal{E}_1^c\right] + \sum_{w_1=2}^{2^{nR_1}} \Pr\left[\mathcal{E}_{w_1}\right] \tag{12.48}$$

$$= \Pr\left[\mathcal{E}_1^c\right] + \sum_{w_1=2}^{2^{nR_1}} \prod_{\ell \in \mathcal{S}_1} \Pr\left[\mathcal{E}_{w_1,\ell}\right] \tag{12.49}$$

where (12.48) is obtained by using the union bound, (12.49) is due to the independence of subchannels and the codebooks. Since $w_1 = 1$, we have

$$\Pr\left[\exists \tilde{w}_1 : (\mathbf{x}_{1\ell}(w_0, 1, \tilde{w}_1), \mathbf{y}_{1\ell}) \in A_\epsilon^n\right] \leq \frac{\epsilon_n}{|\mathcal{S}_1|} \tag{12.50}$$

where $|\mathcal{S}_1|$ denotes the cardinality of the set $\mathcal{S}_1$, and consequently, we have

$$\Pr\left[\mathcal{E}_1^c\right] \leq \epsilon_n \tag{12.51}$$

We now consider an arbitrary term in (12.49):

$$\Pr\left[\mathcal{E}_{w_1,\ell}\right] = \Pr\left[\exists \tilde{w}_1 : (\mathbf{x}_{1\ell}(w_0, w_1, \tilde{w}_1), \mathbf{y}_{1\ell}) \in A_\epsilon^n\right] \tag{12.52}$$

$$\leq \sum_{\tilde{w}_1=1}^{2^{n\tilde{R}_{1\ell}}} \Pr\left[(\mathbf{x}_{1\ell}(w_0, w_1, \tilde{w}_1), \mathbf{y}_{1\ell}) \in A_\epsilon^n\right] \tag{12.53}$$

$$\leq \sum_{\tilde{w}_1=1}^{2^{n\tilde{R}_{1\ell}}} 2^{-n[I(X_\ell;Y_{1\ell}|U_\ell)-\epsilon_n]} \tag{12.54}$$

$$= 2^{n[\tilde{R}_{1\ell}-I(X_\ell;Y_{1\ell}|U_\ell)+\epsilon_n]} \tag{12.55}$$

Therefore, using (12.51) and (12.55) in (12.49), we get

$$P_e^n \leq \epsilon_n + 2^{nR_1} 2^{n \sum_{\ell \in \mathcal{S}_1} [\tilde{R}_{1\ell} - I(X_\ell; Y_{1\ell}|U_\ell) + \epsilon_n]} \tag{12.56}$$

from which we need the following condition for reliable communication,

$$R_1 + \sum_{\ell \in \mathcal{S}_1} \tilde{R}_{1\ell} \leq \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{1\ell}|U_\ell) \tag{12.57}$$

which, after using $\tilde{R}_{1\ell}$ s given in (12.34), is equivalent to

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{1\ell}|U_\ell) - \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{2\ell}|U_\ell) \tag{12.58}$$

Similarly, we can show that

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} I(X_\ell; Y_{2\ell}|U_\ell) - \sum_{\ell \in \mathcal{S}_2} I(X_\ell; Y_{1\ell}|U_\ell) \tag{12.59}$$

is required for reliable communication of user 2.

Equivocation computation:

We now show that the coding scheme described above ensures that the messages are transmitted in perfect secrecy. We compute the equivocation rate for user

1:

$$H(W_1|Y_2^n) \geq H(W_1|Y_2^n, U^n) \tag{12.60}$$

$$= H\left(W_1 | \{Y_{2\ell}^n, U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) \tag{12.61}$$

$$= H\left(W_1, \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) - H\left(\{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) \tag{12.62}$$

$$= H\left(W_1, \{X_\ell^n\}_{\ell\in\mathcal{S}_1}, \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) - H\left(\{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right)$$
$$- H\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1} | W_1, \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1}, \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) \tag{12.63}$$

$$= H\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) + H\left(W_1, \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}, \{X_\ell^n\}_{\ell\in\mathcal{S}_1}\right)$$
$$- H\left(\{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) - H\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1} | W_1, \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1}, \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) \tag{12.64}$$

$$\geq H\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) - I\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1}; \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right)$$
$$- H\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1} | W_1, \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1}, \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) \tag{12.65}$$

where (12.61) follows from the fact that W_1 is transmitted through the subchannels in $\mathcal{S}_1$, i.e., it is independent of $\{Y_{2\ell}^n, U_\ell^n\}_{\ell\in\mathcal{S}_2}$. We treat each term of (12.65) separately. For the first term, we have

$$H\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1} | \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) = nR_1 + n\sum_{\ell\in\mathcal{S}_1}\tilde{R}_{1\ell} \tag{12.66}$$

because given $\{U_\ell^n\}_{\ell\in\mathcal{S}_1}$, $\{X_\ell^n\}_{\ell\in\mathcal{S}_1}$ can take $2^{nR_1+n\sum_{\ell\in\mathcal{S}_1}\tilde{R}_{1\ell}}$ values with equal prob-

ability. The second term of (12.65) can be bounded as

$$
\begin{aligned}
&I\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1}; \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} \,|\, \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) \\
&\quad \le \sum_{\ell\in\mathcal{S}_1} H\left(Y_{2\ell}^n|U_\ell^n\right) - H\left(\{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} \,|\, \{U_\ell^n\}_{\ell\in\mathcal{S}_1}, \{X_\ell^n\}_{\ell\in\mathcal{S}_1}\right) && (12.67)\\
&\quad = \sum_{\ell\in\mathcal{S}_1} H\left(Y_{2\ell}^n|U_\ell^n\right) - H\left(Y_{2\ell}^n|U_\ell^n, X_\ell^n\right) && (12.68)\\
&\quad = \sum_{\ell\in\mathcal{S}_1} I\left(X_\ell^n; Y_{2\ell}^n|U_\ell^n\right) && (12.69)
\end{aligned}
$$

where (12.67) is due to the fact that conditioning cannot increase entropy and (12.68) is due to the independence of the subchannels. More precisely, the latter follows from the Markov chain

$$
\left(\{Y_{2\ell}^n\}_{\substack{\ell\in\{1,\ldots,L\}\\ \ell\neq j}}, \{U_\ell^n\}_{\ell\in\{1,\ldots,L\}}, \{X_\ell^n\}_{\substack{\ell\in\{1,\ldots,L\}\\ \ell\neq j}}\right) \to X_j^n \to Y_{2j}^n \tag{12.70}
$$

We can further bound each summand in (12.69) as

$$
I\left(X_\ell^n; Y_{2\ell}^n|U_\ell^n\right) \le nI(X_\ell; Y_{2\ell}|U_\ell) + \epsilon_n \tag{12.71}
$$

using the approach in [2]. Consequently, (12.69) is bounded as

$$
I\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1}; \{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1} \,|\, \{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right) \le n\sum_{\ell\in\mathcal{S}_1} I\left(X_\ell; Y_{2\ell}|U_\ell\right) + \epsilon_n \tag{12.72}
$$

We now bound the last term in (12.65). To this end, assume user 2 wants to decode $\{X_\ell^n\}_{\ell\in\mathcal{S}_1}$ using its observation over all subchannels in $\mathcal{S}_1$ and its side information

W_1. Since given $W_1 = w_1$, X_ℓ can take at most $2^{nI(X_\ell;Y_\ell|U_\ell)}$ values, user 2 can decode them with vanishingly small error probability. Thus, using Fano's lemma, we get

$$H\left(\{X_\ell^n\}_{\ell\in\mathcal{S}_1}|W_1,\{Y_{2\ell}^n\}_{\ell\in\mathcal{S}_1},\{U_\ell^n\}_{\ell\in\mathcal{S}_1}\right)\leq\epsilon_n \tag{12.73}$$

Plugging (12.66), (12.72) and (12.73) into (12.65), we get

$$H(W_1|Y_2^n)\geq nR_1+n\sum_{\ell\in\mathcal{S}_1}\tilde{R}_{1,\ell}-n\sum_{\ell\in\mathcal{S}_1}I\left(X_\ell;Y_{2\ell}|U_\ell\right)-\epsilon_n \tag{12.74}$$

$$=nR_1-\epsilon_n \tag{12.75}$$

where in the last step we use (12.34). Hence, the proposed encoding scheme can achieve perfect secrecy for user 1. Following similar lines, we can prove that the same holds for user 2 as well, completing the proof.

12.7.1.2 Converse

We now provide the converse part of the proof. We first introduce some notation:

$$Y_1^{i-1}=\left(Y_{11}^{i-1},\ldots,Y_{1L}^{i-1}\right) \tag{12.76}$$

$$Y_{2,i+1}^{n}=\left(Y_{21,i+1}^{n},\ldots,Y_{2L,i+1}^{n}\right) \tag{12.77}$$

$$Y_{1[1:\ell-1],i}=\left(Y_{11,i},\ldots,Y_{1(\ell-1),i}\right) \tag{12.78}$$

$$Y_{2[\ell+1:L],i}=\left(Y_{2(\ell+1),i},\ldots,Y_{2L,i}\right) \tag{12.79}$$

$$\tag{12.80}$$

We define the following auxiliary random variables

$$U_{\ell,i} = W_0 Y_{1[1:\ell-1],i} Y_{2[\ell+1:L],i} Y_1^{i-1} Y_{2,i+1}^n, \quad \ell = 1, \ldots, L \quad i = 1, \ldots, n \tag{12.81}$$

which satisfy the Markov chain

$$U_{\ell,i} \to X_{\ell,i} \to (Y_{1\ell,i}, Y_{2\ell,i}) \tag{12.82}$$

We start with the common message rate

$$\begin{aligned}
nR_0 &= H(W_0) && (12.83)\\
&\leq I(W_0; Y_1^n) + \epsilon_n && (12.84)\\
&= \sum_{i=1}^{n} I(W_0; Y_{1,i} | Y_1^{i-1}) + \epsilon_n && (12.85)\\
&= \sum_{i=1}^{n} \sum_{\ell=1}^{L} I(W_0; Y_{1\ell,i} | Y_1^{i-1}, Y_{1[1:\ell-1],i}) + \epsilon_n && (12.86)\\
&\leq \sum_{i=1}^{n} \sum_{\ell=1}^{L} I(W_0, Y_1^{i-1}, Y_{1[1:\ell-1],i}; Y_{1\ell,i}) + \epsilon_n && (12.87)\\
&\leq \sum_{i=1}^{n} \sum_{\ell=1}^{L} I(W_0, Y_1^{i-1}, Y_{1[1:\ell-1],i}, Y_{2,i+1}^n, Y_{2[\ell+1:L],i}; Y_{1\ell,i}) + \epsilon_n && (12.88)\\
&= \sum_{i=1}^{n} \sum_{\ell=1}^{L} I(U_{\ell,i}; Y_{1\ell,i}) + \epsilon_n && (12.89)
\end{aligned}$$

where (12.84) follows from Fano's lemma, (12.85) and (12.86) are due to the chain rule, (12.87) comes from the inequality $I(A; B|C) \leq I(A, C; B)$, (12.88) follows from the inequality $I(A; B) \leq I(A, C; B)$ and (12.89) comes from the definition of $U_{\ell,i}$ in

(12.82). Similarly, we can obtain

$$nR_0 \leq \sum_{i=1}^{n}\sum_{\ell=1}^{L} I(U_{\ell,i}; Y_{2\ell,i}) + \epsilon_n \tag{12.90}$$

We now consider the secrecy rate of the first user as follows

$$\begin{aligned}
nR_1 &\leq H(W_1|Y_2^n) && (12.91)\\
&\leq H(W_1, W_0|Y_2^n) && (12.92)\\
&= H(W_1|Y_2^n, W_0) + H(W_0|Y_2^n) && (12.93)\\
&\leq H(W_1|Y_2^n, W_0) + \epsilon_n' && (12.94)\\
&= H(W_1|W_0) - I(W_1; Y_2^n|W_0) + \epsilon_n' && (12.95)\\
&\leq I(W_1; Y_1^n|W_0) - I(W_1; Y_2^n|W_0) + \epsilon_n && (12.96)\\
&= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_0, Y_1^{i-1}) - \sum_{i=1}^{n} I(W_1; Y_{2,i}|W_0, Y_{2,i+1}^n) + \epsilon_n && (12.97)\\
&= \sum_{i=1}^{n} I(W_1, Y_{2,i+1}^n; Y_{1,i}|W_0, Y_1^{i-1}) - \sum_{i=1}^{n} I(W_1, Y_1^{i-1}; Y_{2,i}|W_0, Y_{2,i+1}^n) + \epsilon_n && (12.98)\\
&= \sum_{i=1}^{n} I(W_1; Y_{1,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n) - \sum_{i=1}^{n} I(W_1; Y_{2,i}|W_0, Y_{2,i+1}^n, Y_1^{i-1}) + \epsilon_n && (12.99)
\end{aligned}$$

where (12.94) and (12.96) follow from Fano's lemma, (12.97) is due to the chain rule and (12.98) and (12.99) come from the following inequalities:

$$\begin{aligned}
\sum_{i=1}^{n} I(Y_{2,i+1}^n; Y_{1,i}|W_0, W_1, Y_1^{i-1}) &= \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|W_0, W_1, Y_{2,i+1}^n) && (12.100)\\
\sum_{i=1}^{n} I(Y_{2,i+1}^n; Y_{1,i}|W_0, Y_1^{i-1}) &= \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2,i}|W_0, Y_{2,i+1}^n) && (12.101)
\end{aligned}$$

respectively [3]. We now consider an arbitrary summand in (12.99)

$$
\begin{aligned}
&I(W_1; Y_{1,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n) - I(W_1; Y_{2,i}|W_0, Y_{2,i+1}^n, Y_1^{i-1}) \\
&\quad = \sum_{\ell=1}^{L} I(W_1; Y_{1\ell,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n, Y_{1[1:\ell-1],i}) \\
&\qquad - \sum_{\ell=1}^{L} I(W_1; Y_{2\ell,i}|W_0, Y_{2,i+1}^n, Y_1^{i-1}, Y_{2[\ell+1:L],i}) && (12.102) \\
&\quad = \sum_{\ell=1}^{L} I(W_1, Y_{2[\ell+1:L],i}; Y_{1\ell,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n, Y_{1[1:\ell-1],i}) \\
&\qquad - \sum_{\ell=1}^{L} I(W_1, Y_{1[1:\ell-1],i}; Y_{2\ell,i}|W_0, Y_{2,i+1}^n, Y_1^{i-1}, Y_{2[\ell+1:L],i}) && (12.103) \\
&\quad = \sum_{\ell=1}^{L} I(W_1; Y_{1\ell,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n, Y_{1[1:\ell-1],i}, Y_{2[\ell+1:L],i}) \\
&\qquad - \sum_{\ell=1}^{L} I(W_1; Y_{2\ell,i}|W_0, Y_{2,i+1}^n, Y_1^{i-1}, Y_{2[\ell+1:L],i}, Y_{1[1:\ell-1],i}) && (12.104) \\
&\quad = \sum_{\ell=1}^{L} I(W_1; Y_{1\ell,i}|U_{\ell,i}) - \sum_{\ell=1}^{L} I(W_1; Y_{2\ell,i}|U_{\ell,i}) && (12.105) \\
&\quad \leq \sum_{\ell\in\mathcal{S}_1} I(W_1; Y_{1\ell,i}|U_{\ell,i}) - \sum_{\ell\in\mathcal{S}_1} I(W_1; Y_{2\ell,i}|U_{\ell,i}) && (12.106) \\
&\quad \leq \sum_{\ell\in\mathcal{S}_1} I(W_1; Y_{1\ell,i}|U_{\ell,i}) - \sum_{\ell\in\mathcal{S}_1} I(W_1; Y_{2\ell,i}|U_{\ell,i}) \\
&\qquad + \sum_{\ell\in\mathcal{S}_1} \Big[I(X_{\ell,i}; Y_{1\ell,i}|U_{\ell,i}, W_1) - I(X_{\ell,i}; Y_{2\ell,i}|U_{\ell,i}, W_1) \Big] && (12.107) \\
&\quad = \sum_{\ell\in\mathcal{S}_1} \Big[I(X_{\ell,i}; Y_{1\ell,i}|U_{\ell,i}) - I(X_{\ell,i}; Y_{2\ell,i}|U_{\ell,i}) \Big] && (12.108)
\end{aligned}
$$

where (12.102) is due to the chain rule, (12.103) and (12.104) come from the identities

$$\sum_{\ell=1}^{L} I(Y_{2[\ell+1:L],i}; Y_{1\ell,i}|W_0, W_1, Y_1^{i-1}, Y_{2,i+1}^n, Y_{1[1:\ell-1],i}) = \sum_{\ell=1}^{L} I(Y_{1[1:\ell-1],i}; Y_{2\ell,i}|W_0, W_1, Y_{2,i+1}^n, Y_1^{i-1}, Y_{2[\ell+1:L],i}) \tag{12.109}$$

$$\sum_{\ell=1}^{L} I(Y_{2[\ell+1:L],i}; Y_{1\ell,i}|W_0, Y_1^{i-1}, Y_{2,i+1}^n, Y_{1[1:\ell-1],i}) = \sum_{\ell=1}^{L} I(Y_{1[1:\ell-1],i}; Y_{2\ell,i}|W_0, Y_{2,i+1}^n, Y_1^{i-1}, Y_{2[\ell+1:L],i}) \tag{12.110}$$

respectively [3], and in (12.105), we use the definition of $U_{\ell,i}$ which is given in (12.82). Since we have

$$I(W_1; Y_{1\ell,i}|U_{\ell,i}) - I(W_1; Y_{2\ell,i}|U_{\ell,i}) < 0, \quad \forall \ell \in \mathcal{S}_2 \tag{12.111}$$

due to the Markov chain $W_1 \to X_{\ell,i} \to (Y_{1\ell,i}, Y_{2\ell,i})$ and the fact that subchannels of user 2 in $\mathcal{S}_2$ are less noisy than those of user 1 (see (12.3)), dropping these negative terms from the summation in (12.105) results in the loosened bound in (12.106). Similarly, we have

$$I(X_{1\ell,i}; Y_{1\ell,i}|W_1, U_{\ell,i}) - I(X_{1\ell,i}; Y_{2\ell,i}|W_1, U_{\ell,i}) > 0, \quad \forall \ell \in \mathcal{S}_1 \tag{12.112}$$

due to the less noisiness condition given in (12.2). Thus, adding positive terms to (12.106) results in the loosened bound in (12.107). Finally, in (12.108), we use the

Markov chain $W_1 \to X_{\ell,i} \to (Y_{1\ell,i}, Y_{2\ell,i})$. Plugging (12.108) into (12.99), we get

$$nR_1 \leq \sum_{i=1}^{n} \sum_{\ell \in \mathcal{S}_1} \Big[I(X_{\ell,i}; Y_{1\ell,i}|U_{\ell,i}) - I(X_{\ell,i}; Y_{2\ell,i}|U_{\ell,i}) \Big] \tag{12.113}$$

Similarly, we can show

$$nR_2 \leq \sum_{i=1}^{n} \sum_{\ell \in \mathcal{S}_2} \Big[I(X_{\ell,i}; Y_{2\ell,i}|U_{\ell,i}) - I(X_{\ell,i}; Y_{2\ell,i}|U_{\ell,i}) \Big] \tag{12.114}$$

We define a uniformly distributed random variable J over $\{1, \ldots, n\}$ and $U_\ell = JU_{\ell,J}$, $X_\ell = X_{\ell,J}$, $Y_{1\ell} = Y_{1\ell,J}$, $Y_{2\ell} = Y_{2\ell,J}$ for which we have the Markov chain

$$U_\ell \to X_\ell \to (Y_{1\ell}, Y_{2\ell}) \tag{12.115}$$

Using these new definitions, the bounds in (12.89), (12.90), (12.113), (12.114) can be expressed as

$$R_0 \leq \sum_{\ell=1}^{L} I(U_{\ell,J}; Y_{1\ell,J}|J) + \epsilon_n \leq \sum_{\ell=1}^{L} I(U_\ell; Y_{1\ell}) + \epsilon_n \tag{12.116}$$

$$R_0 \leq \sum_{\ell=1}^{L} I(U_{\ell,J}; Y_{2\ell,J}|J) + \epsilon_n \leq \sum_{\ell=1}^{L} I(U_\ell; Y_{2\ell}) + \epsilon_n \tag{12.117}$$

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} \Big[I(X_\ell; Y_{1\ell}|U_\ell) - I(X_\ell; Y_{2\ell}|U_\ell) \Big] + \epsilon_n \tag{12.118}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} \Big[I(X_\ell; Y_{2\ell}|U_\ell) - I(X_\ell; Y_{2\ell}|U_\ell) \Big] \tag{12.119}$$

taking the union of which over all $p(u_{[1:L]}, x_{[1:L]}, y_{1[1:L]}, y_{2[1:L]})$ gives the outer bound on the capacity region. However, since each mutual information in these terms

depends only on $p(u_\ell, x_\ell, y_{1\ell}, y_{2\ell})$ but not on the entire distribution

$$p(u_{[1:L]}, x_{[1:L]}, y_{1[1:L]}, y_{2[1:L]}) \tag{12.120}$$

there is no loss in considering the distributions of the form

$$p(u_{[1:L]}, x_{[1:L]}, y_{1[1:L]}, y_{2[1:L]}) = \prod_{\ell=1}^{L} p(u_\ell, x_\ell, y_{1\ell}, y_{2\ell}) \tag{12.121}$$

This concludes the converse part of the proof.

12.7.2 Proof of Theorem 12.2

We now prove Theorem 12.2. Since the Gaussian channel is an instance of degraded channels, its capacity region is given by

$$R_1 \leq \sum_{\ell \in \mathcal{S}_1} I(X_\ell; Y_{1\ell}|Y_{2\ell}) \tag{12.122}$$

$$R_2 \leq \sum_{\ell \in \mathcal{S}_2} I(X_\ell; Y_{2\ell}|Y_{1\ell}) \tag{12.123}$$

which is due to Corollary 12.2. Maximizing these mutual information terms is equivalent to maximizing $H(Y_{1\ell}|Y_{2\ell})$ or $H(Y_{2\ell}|Y_{1\ell})$ which happens when $(Y_{1\ell}, Y_{2\ell})$ are jointly Gaussian. Consequently, the optimum input distribution is Gaussian. Hence, we select $X_\ell \sim \mathcal{N}(0, \alpha_{j\ell}P)$ for $\ell \in \mathcal{S}_j$ $(j = 1, 2)$ where $\sum_{j=1}^{2} \sum_{\ell \in \mathcal{S}_j} \alpha_{j\ell} \leq 1$. Using the equivalent description of the Gaussian channel in (12.18)-(12.19) in conjunction

with this choice ofinput distributions for the rates (12.122)-(12.123), we get

$$R_1 \leq \frac{1}{2}\sum_{\ell\in\mathcal{S}_1}\Big[\log(1+\alpha_{1\ell}h_{1\ell}^2P)-\log(1+\alpha_{1\ell}h_{2\ell}^2P)\Big] \tag{12.124}$$

$$R_2 \leq \frac{1}{2}\sum_{\ell\in\mathcal{S}_2}\Big[\log(1+\alpha_{2\ell}h_{2\ell}^2P)-\log(1+\alpha_{2\ell}h_{1\ell}^2P)\Big] \tag{12.125}$$

Finally, we need to find the optimal values of $\{\alpha_{j\ell}\}_{\ell\in\mathcal{S}_j}$ $(j=1,2)$to characterize the boundary of the region. To this end, assume β ($\beta\in[0,1]$) of the total power is dedicated to user 1 and the rest of the power is dedicated to user 2. To find the optimal power allocation, we can use the Lagrangian technique. Since the rate expressions are concave and we have affine constraints, KKT conditions provide necessary and sufficient conditions for the optimal power allocation. Moreover, we note that since rate functions are monotonically increasing in $\{\alpha_{j\ell}\}$, power constraints should be met with equality, i.e.,

$$\sum_{\ell\in\mathcal{S}_1}\alpha_{1\ell}=\beta \quad \text{and} \quad \sum_{\ell\in\mathcal{S}_2}\alpha_{2\ell}=\bar{\beta} \tag{12.126}$$

The corresponding Lagrangian function for user 1 is given by

$$\frac{1}{2}\sum_{\ell\in\mathcal{S}_1}\Big[\log\left(1+\alpha_{1\ell}h_{1\ell}^2P\right)-\log\left(1+\alpha_{1\ell}h_{2\ell}^2P\right)\Big]-\lambda_1\sum_{\ell\in\mathcal{S}_1}\alpha_{1\ell}+\sum_{\ell\in\mathcal{S}_1}\nu_\ell\alpha_{1\ell} \tag{12.127}$$

where $\nu_\ell\geq 0$. Inspection of KKT conditions reveals that for any non-zero $\alpha_{1\ell}$, we have $\nu_\ell=0$ and the derivative of the Lagrangian with respect to α_ℓ is zero. Otherwise, we have $\nu_l>0$ and the derivative of the Lagrangian is negative. Thus,

any non-zero $\alpha_{1\ell}$ satisfies

$$\frac{1}{2}\left[\frac{h_{1\ell}P}{1+\alpha_{1\ell}h_{1\ell}P}-\frac{h_{2\ell}P}{1+\alpha_{1\ell}h_{2\ell}P}\right]-\lambda_1=0 \tag{12.128}$$

which implies

$$\alpha_{1\ell}=\left[-\frac{1}{2P}\left(\frac{1}{h_{1\ell}^2}+\frac{1}{h_{2\ell}^2}\right)+\frac{1}{2P}\sqrt{\left(\frac{1}{h_{1\ell}^2}-\frac{1}{h_{2\ell}^2}\right)^2+\frac{2P}{\lambda_1}\left(\frac{1}{h_{2\ell}^2}-\frac{1}{h_{1\ell}^2}\right)}\right]^+ \tag{12.129}$$

Moreover, λ_1 can be found through

$$\sum_{\ell\in\mathcal{S}_1}\alpha_{1\ell}=\beta \tag{12.130}$$

The optimum power allocation for user 2 can be found by symmetry.

Chapter 13

Secure Lossy Transmission of Vector Gaussian Sources

13.1 Introduction

In this chapter, we study the secure lossy source coding problem for a vector Gaussian model, see Figure 13.1. Secure source coding problem has been studied for both lossless and lossy reconstruction cases in [14, 100–112]. Secure *lossless* source coding problem is studied in [100–106], where the common theme is that the legitimate receiver wants to reconstruct the source in a lossless fashion by using the information it gets from the transmitter in conjunction with its side information, while keeping the eavesdropper ignorant of the source as much as possible. Secure *lossy* source coding problem is studied in [14, 107–112], which differ from the works on lossless case by letting the legitimate receiver reconstruct the source not perfectly, but within a distortion level.

The most relevant works to our work here are [14, 112]. Reference [112] studies the secure lossy transmission of a source over a degraded wiretap channel when both the legitimate receiver and the eavesdropper have side information about the source. In [112], in addition to the degradedness of the eavesdropper's channel output with respect to the legitimate user's channel output, the eavesdropper's side information is also degraded with respect to the legitimate user's side information. For this setting, [112] provides a single-letter characterization of the distortion and equivo-

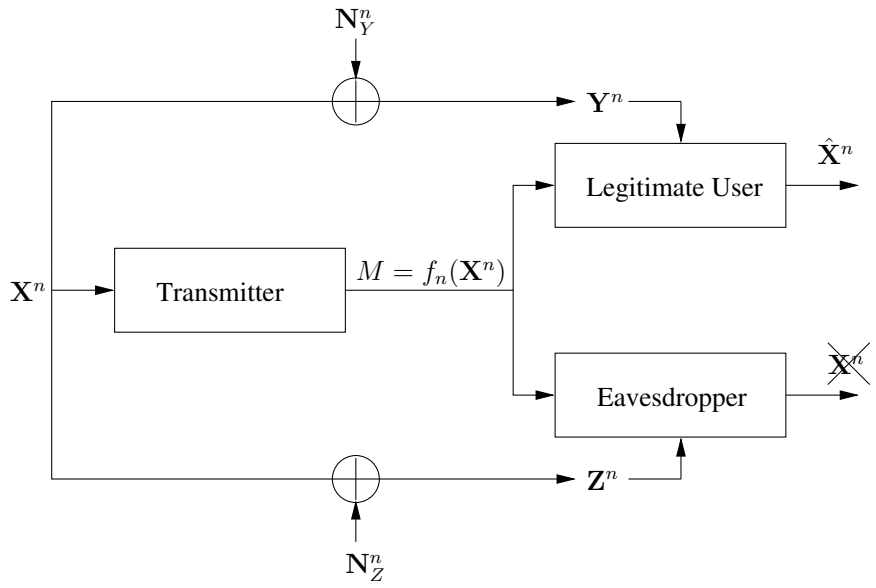

Figure 13.1: Secure lossy source coding problem for a vector Gaussian model.

cation region, where the separation principle (between source coding and channel coding) holds. In [14], the setting of [112] is partially generalized by assuming that there is no degradedness order between the side information of the legitimate user and the eavesdropper. On the other hand, as opposed to the *noisy* wiretap channel of [112], in [14], the channel between the transmitter and the receivers is assumed to be *noiseless*. For this setting, [14] provides a single-letter characterization of the rate, equivocation, and distortion region.

Here, we study the setting of [14] for jointly Gaussian source and side information, where the transmitter has a vector Gaussian source which is jointly Gaussian with the vector Gaussian side information of both the legitimate receiver and the eavesdropper. As mentioned earlier, a single-letter characterization of the rate, equivocation, and distortion region for this setting is given in [14]. By individually optimizing the rate and equivocation constraints of this single-letter description

for the vector Gaussian model at hand, we obtain an outer bound for the rate-equivocation region. On the other hand, we note that a joint optimization would yield the exact rate-equivocation region. As a consequence of these individual optimizations, we obtain the maximum achievable equivocation at the eavesdropper when there is no constraint on the transmission rate. We show that even hough there is no rate constraint, the maximum equivocation cannot be attained by an uncoded scheme. Moreover, using this maximum equivocation result, we show that, in general, Wyner-Ziv coding is not optimal for the secure lossy source coding problem, although it would be optimal in the absence of an eavesdropper.

13.2 Secure Lossy Source Coding

Here, we describe the secure lossy source coding problem and state the existing results. Let $\{(X_i, Y_i, Z_i)\}_{i=1}^n$ denote i.i.d. tuples drawn from a distribution $p(x, y, z)$. The transmitter, the legitimate user and the eavesdropper observe $X^n \in \mathcal{X}^n, Y^n \in \mathcal{Y}^n$, and $Z^n \in \mathcal{Z}^n$, respectively. The transmitter wants to convey information to the legitimate user in a way that the legitimate user can reconstruct the source X^n within a certain distortion, and meanwhile the eavesdropper is kept ignorant of the source X^n as much as possible as measured by the equivocation. We note that if there was no eavesdropper, this setting would reduce to the Wyner-Ziv problem [113], for which a single-letter characterization for the minimum transmission rate of the transmitter for each distortion level exists.

The distortion of the reconstructed sequence at the legitimate user is mea-

sured by the function $d^n(X^n, \hat{X}^n)$ where $\hat{X}^n \in \hat{\mathcal{X}}^n$ denotes the legitimate user's reconstruction of the source X^n. We consider the function $d^n(X^n, \hat{X}^n)$ that has the following form

$$d^n(X^n, \hat{X}^n) = \frac{1}{n} \sum_{i=1}^{n} d(X_i, \hat{X}_i) \tag{13.1}$$

where $d(a, b)$ is a non-negative finite-valued function. The confusion of the eavesdropper is measured by the following equivocation term

$$\frac{1}{n} H(X^n | Z^n, M) \tag{13.2}$$

where $M \in \mathcal{M}$, which is a function of the source X^n, denotes the signal sent by the transmitter.

An (n, R) code for secure lossy source coding consists of an encoding function $f_n : \mathcal{X}^n \to \mathcal{M} = \{1, \ldots, 2^{nR}\}$ at the transmitter and a decoding function at the legitimate user $g_n : \mathcal{M} \times \mathcal{Y}^n \to \hat{\mathcal{X}}^n$. A rate, equivocation and distortion tuple (R, R_e, D) is achievable if there exists an (n, R) code satisfying

$$\lim_{n \to \infty} \frac{1}{n} H(X^n | Z^n, M) \geq R_e \tag{13.3}$$

$$\lim_{n \to \infty} E[d(X^n, \hat{X}^n)] \leq D \tag{13.4}$$

The set of all achievable (R, R_e, D) tuples is denoted by $\mathcal{R}^*$ which is given by the following theorem.

Theorem 13.1 ([14, Theorem 1]) $(R, R_e, D) \in \mathcal{R}^*$ *iff*

$$R \geq I(V;X|Y) \tag{13.5}$$

$$R_e \leq H(X|V,Y) + I(X;Y|U) - I(X;Z|U) \tag{13.6}$$

$$D \geq E[d(X, \hat{X}(V,Y))] \tag{13.7}$$

for some U, V *satisfying the Markov chain* $U \to V \to X \to Y, Z$*, and a function* $\hat{X}(V,Y)$*.*

The achievable scheme that attains the region $\mathcal{R}^*$ has the same spirit as the Wyner-Ziv scheme [113] in the sense that both achievable schemes use binning to exploit the side information at the legitimate user, and consequently, to reduce the rate requirement. The difference of the achievable scheme that attains $\mathcal{R}^*$ comes from the additional binning necessitated by the presence of an eavesdropper. In particular, the transmitter generates sequences (U^n, V^n) and bins both sequences. The transmitter sends these two bin indices. Using these bin indices, the legitimate user identifies the right (U^n, V^n) sequences, and reconstructs X^n within the required distortion. On the other hand, using the bin indices of (U^n, V^n), the eavesdropper identifies only the right U^n sequence, and consequently, U does not contribute to the equivocation, see (13.6)[1]. Indeed, this achievable scheme can be viewed as if it is using a rate-splitting technique to send the message M, since M has two coordinates, one for the bin index of U^n, and one for the bin index of V^n. This perspective reveals

[1]The fact that the eavesdropper can decode U^n sequence can be obtained by observing that for a (U,V) selection, if $I(U;Y) \geq I(U;Z)$, there is no loss of optimality of setting $U = \phi$ which will yield a larger region.

the similarity of the achievable scheme that attains $\mathcal{R}^*$ and the one that attains the capacity-equivocation region of the wiretap channel [3] where also rate-splitting is used. In particular, in the latter case, the message W is divided into two parts W_{ne}, W_e such that W_{ne} is sent by the sequence U^n and W_e is sent by the sequence V^n. The eavesdropper decodes W_{ne} whereas the other message W_e contributes to the secrecy.

We note that Theorem 13.1 holds for continuous (X^n, Y^n, Z^n) by replacing the discrete entropy term $H(X|V,Y)$ with the differential entropy term $h(X|V,Y)$. To avoid the negative equivocation that might arise because of the use of differential entropy, we replace equivocation with the mutual information leakage to the eavesdropper I_e defined by

$$\lim_{n\to\infty} \frac{1}{n} I(X^n; Z^n, M) \tag{13.8}$$

Once we are interested in the mutual information leakage to the eavesdropper, a rate, mutual information leakage, and distortion (R, I_e, D) tuple is said to be achievable if there exists an (n, R) code such that

$$\lim_{n\to\infty} \frac{1}{n} I(X^n; Z^n, M) \leq I_e \tag{13.9}$$

$$\lim_{n\to\infty} E[d(X^n, \hat{X}^n)] \leq D \tag{13.10}$$

The set of all achievable (R, I_e, D) tuples is denoted by $\mathcal{R}$. Using Theorem 13.1, the region $\mathcal{R}$ can be stated as follows.

Theorem 13.2 ([14]) $(R, I_e, D) \in \mathcal{R}$ *iff*

$$R \geq I(V;X|Y) \tag{13.11}$$

$$I_e \geq I(V;X) - I(V;Y|U) + I(X;Z|U) \tag{13.12}$$

$$D \geq E[d(X, \hat{X}(V,Y))] \tag{13.13}$$

for some U, V *satisfying the following Markov chain*

$$U \to V \to X \to Y, Z \tag{13.14}$$

and a function $\hat{X}(V,Y)$.

13.3 Vector Gaussian Sources

Now we study the secure lossy source coding problem for jointly Gaussian $\{(\mathbf{X}_i, \mathbf{Y}_i, \mathbf{Z}_i)\}_{i=1}^n$ where the tuples $\{(\mathbf{X}_i, \mathbf{Y}_i, \mathbf{Z}_i)\}_{i=1}^n$ are independent across time, i.e., across the index i, and each tuple is drawn from the same jointly Gaussian distribution $p(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$. In other words, we consider the case where $\mathbf{X}_i$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}_X \succ \mathbf{0}$, and the side information at the legitimate user $\mathbf{Y}_i$ and the eavesdropper $\mathbf{Z}_i$ are jointly Gaussian with the source $\mathbf{X}_i$. In particular, we assume that $\mathbf{Y}_i, \mathbf{Z}_i$ have the following form

$$\mathbf{Y}_i = \mathbf{X}_i + \mathbf{N}_{Y,i} \tag{13.15}$$

$$\mathbf{Z}_i = \mathbf{X}_i + \mathbf{N}_{Z,i} \tag{13.16}$$

where $\mathbf{N}_{Y,i}$ and $\mathbf{N}_{Z,i}$ are independent zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_Y \succ \mathbf{0}$ and $\mathbf{\Sigma}_Z \succ \mathbf{0}$, respectively, and $(\mathbf{N}_{Y,i}, \mathbf{N}_{Z,i})$ and $\mathbf{X}_i$ are independent. We note that the side information given by (13.15)-(13.16) are not in the most general form. In the most general case, we have

$$\mathbf{Y}_i = \mathbf{H}_Y \mathbf{X}_i + \mathbf{N}_{Y,i} \tag{13.17}$$

$$\mathbf{Z}_i = \mathbf{H}_Z \mathbf{X}_i + \mathbf{N}_{Z,i} \tag{13.18}$$

for some $\mathbf{H}_Y, \mathbf{H}_Z$ matrices. However, until Section 13.5, we consider the form of side information given by (13.15)-(13.16), and obtain our results for this model. In Section 13.5, we generalize our results to the most general case given by (13.17)-(13.18). We note that since the rate, information leakage and distortion region is invariant with respect to the correlation between $\mathbf{N}_{Y,i}$ and $\mathbf{N}_{Z,i}$, the correlation between $\mathbf{N}_{Y,i}$ and $\mathbf{N}_{Z,i}$ is immaterial.

The distortion of the reconstructed sequence $\{\hat{\mathbf{X}}_i\}_{i=1}^n$ is measured by the mean square error matrix:

$$E\left[\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)^\top\right] \tag{13.19}$$

Hence, the distortion constraint is represented by a positive semi-definite matrix $\mathbf{D}$, which is achievable if there is an (n, R) code such that

$$\frac{1}{n}\sum_{i=1}^{n} E\left[\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)^\top\right] \preceq \mathbf{D} \tag{13.20}$$

Throughout this chapter, we assume that $\mathbf{0} \preceq \mathbf{D} \preceq \mathbf{K}_{X|Y}$. Since the mean square error is minimized by the minimum mean square error (MMSE) estimator which is given by the conditional mean, we assume that the legitimate user applies this optimal estimator, i.e., the legitimate user selects its reconstruction function $\{\hat{\mathbf{X}}_i\}_{i=1}^n$ as

$$\hat{\mathbf{X}}_i = E\left[\mathbf{X}_i | \mathbf{Y}^n, f_n(\mathbf{X}^n)\right] \tag{13.21}$$

Once the estimator of the legitimate user is set as (13.21), using Theorem 13.2, a single-letter description of the region $\mathcal{R}$ for a vector Gaussian source can be given as follows.

Theorem 13.3 $(R, I_e, \mathbf{D}) \in \mathcal{R}$ *iff*

$$R \geq I(V; \mathbf{X}|\mathbf{Y}) \tag{13.22}$$

$$I_e \geq I(V; \mathbf{X}) - I(V; \mathbf{Y}|U) + I(\mathbf{X}; \mathbf{Z}|U) \tag{13.23}$$

$$\mathbf{D} \succeq \mathbf{K}_{X|VY} \tag{13.24}$$

for some U, V satisfying the following Markov chain

$$U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \tag{13.25}$$

We also define the region $\mathcal{R}(\mathbf{D})$ as the union of the (R, I_e) pairs that are achievable when the distortion constraint matrix is set to $\mathbf{D}$. Our main result is an outer bound

for the region $\mathcal{R}(\mathbf{D})$, hence for the region $\mathcal{R}$.

Theorem 13.4 *When* $\mathbf{D} \preceq \mathbf{K}_{X|Y}$*, we have*

$$\mathcal{R}(\mathbf{D}) \subseteq \mathcal{R}^o(\mathbf{D}) \tag{13.26}$$

where $\mathcal{R}^o(\mathbf{D})$ *is given by the union of* (R, I_e) *that satisfy*

$$R \geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_Y|}{|\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y|} \tag{13.27}$$

$$I_e \geq \min_{\substack{\mathbf{0} \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.28}$$

and $\mathbf{F}(\mathbf{D}) = \mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y$.

We will prove Theorem 13.4 in Section 13.4. In the remainder of this section, we provide interpretations and discuss some implications of Theorem 13.4.

The outer bound in Theorem 13.4 is obtained by minimizing the constraints on R and I_e individually, i.e., the rate lower bound in (13.27) is obtained by minimizing the rate constraint in (13.22) and the mutual information leakage lower bound in (13.28) is obtained by minimizing the mutual information leakage constraint in (13.23) separately. However, to characterize the rate and mutual information leakage region $\mathcal{R}(\mathbf{D})$, one needs to minimize the rate constraint in (13.22) and the mutual leakage information constraint in (13.23) jointly, not separately. In particular, since the region $\mathcal{R}(\mathbf{D})$ is convex in the pairs (R, I_e) as per a time-sharing argument, joint optimization of the rate constraint in (13.22) and the mutual information leakage

constraint in (13.23) can be carried out by considering the tangent lines to the region $\mathcal{R}(\mathbf{D})$, i.e., by solving the following optimization problem

$$L(\mu_1,\mu_2) = \min_{(R,I_e)\in\mathcal{R}(\mathbf{D})} \ \mu_1 R + \mu_2 I_e \tag{13.29}$$

$$= \min_{\substack{U\to V\to\mathbf{X}\to\mathbf{Y},\mathbf{Z}\\ \mathbf{K}_{X|VY}\preceq\mathbf{D}}} \mu_1\left[I(V;\mathbf{X}) - I(V;\mathbf{Y})\right] + \mu_2\left[I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U)\right] \tag{13.30}$$

for all values of μ_1,μ_2, where $\mu_j\in[0,\infty),\ j=1,2$. As of now, we have been unable to solve the optimization problem $L(\mu_1,\mu_2)$ for all values of (μ_1,μ_2). However, as stated in Theorem 13.4, we solve the optimization problems $L(0,\mu_2)$ and $L(\mu_1,0)$ by showing the optimality of jointly Gaussian $(U,V,\mathbf{X})$ to evaluate the corresponding cost functions. In other words, our outer bound in Theorem 13.4 can be written as follows:

$$R \geq L(1,0) \tag{13.31}$$

$$I_e \geq L(0,1) \tag{13.32}$$

We note that the constraint in (13.27), and hence $L(1,0)$, gives us the Wyner-Ziv rate distortion function [113] for the vector Gaussian sources. Moreover, we note that $L(0,1)$ gives us the minimum mutual information leakage to the eavesdropper when the legitimate user wants to reconstruct the source within a fixed distortion constraint $\mathbf{D}$ while there is no concern on the transmission rate R. Denoting the minimum mutual information leakage to the eavesdropper when the legitimate user

needs to reconstruct the source within a fixed distortion constraint $\mathbf{D}$ by $I_e^{\min}(\mathbf{D})$, the corresponding result can be stated as follows.

Theorem 13.5 *When* $\mathbf{D} \preceq \mathbf{K}_{X|Y}$*, we have*

$$I_e^{\min}(\mathbf{D}) = \min_{\substack{\mathbf{0} \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.33}$$

where $\mathbf{F}(\mathbf{D}) = \mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y$.

Theorem 13.5 implies that if the transmitter's aim is to minimize the mutual information leakage to the eavesdropper without concerning itself with the rate it costs as long as the legitimate receiver is able to reconstruct the source within a distortion constraint $\mathbf{D}$, the use of jointly Gaussian $(U, V, \mathbf{X})$ is optimal. Since in Theorem 13.5, there is no rate constraint, one natural question to ask is whether $I_e^{\min}(\mathbf{D})$ can be achieved by an uncoded transmission scheme. Now, we address this question in a broader context by letting the encoder use any *instantaneous* encoding function in the form of $g_i(\mathbf{X}_i)$ where $g_i(\cdot)$ can be a deterministic or a stochastic mapping. When $g_i(\cdot)$ is chosen to be stochastic, we assume it to be independent across time. We note that the uncoded transmission can be obtained from instantaneous encoding by selecting $g_i(\cdot)$ to be a linear function. Similarly, uncoded transmission with artificial noise can be obtained from instantaneous encoding by selecting $g_i(x) = \alpha x + N$, where N denotes the noise. Hence, if the encoder uses an instantaneous encoding scheme, the transmitted signal is given by

$M = [\ g_1(\mathbf{X}_1), \ldots, g_n(\mathbf{X}_n)\ ]$. Let $I_e^{\text{ins}}(\mathbf{D})$ be the minimum information leakage to the eavesdropper when the legitimate user is able to reconstruct the source with a distortion constraint $\mathbf{D}$ while the encoder uses an instantaneous encoding. The following example demonstrates that, in general, $I_e^{\min}(\mathbf{D})$ cannot be achieved by instantaneous encoding.

Example 13.1 *Consider the scalar case, where the side information at the legitimate user and the eavesdropper are given as follows*

$$Y_i = X_i + N_{y,i} \tag{13.34}$$

$$Z_i = X_i + N_{z,i} \tag{13.35}$$

where $X_i, N_{y,i}$ and $N_{z,i}$ are zero-mean Gaussian random variables with variances σ_x^2, σ_y^2 and σ_z^2, respectively. $\{X_i\}_{i=1}^n, \{N_{y,i}\}_{i=1}^n$ and $\{N_{z,i}\}_{i=1}^n$ are independent. We assume that $\sigma_y^2 < \sigma_z^2$, which implies that we can assume $X \to Y \to Z$ since the scalar model in (13.34)-(13.35) is statistically degraded, or in other words, the correlation between $N_{y,i}$ and $N_{z,i}$ does not affect the achievable (R, I_e, D) region. Using Theorem 13.3, $I_e^{\min}(D)$ for the scalar Gaussian channel under consideration can be found as follows

$$I_e^{\min}(D) = \min_{\substack{U \to V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(V;X) - I(V;Y|U) + I(X;Z|U) \tag{13.36}$$

$$= \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(V;X) - I(V;Y) + I(X;Z) \tag{13.37}$$

where in (13.37), we used the Markov chain $U \to V \to X \to Y \to Z$.

As shown in Appendix 13.7.1, the information leakage to the eavesdropper when the encoder uses an instantaneous mapping is given by

$$I_e^{\text{ins}}(D) = \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(X; V, Z) \tag{13.38}$$

$$= \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(V; X) - I(V; Z) + I(X; Z) \tag{13.39}$$

where (13.39) is obtained by using the Markov chain $V \to X \to Z$.

Using (13.37) and (13.39), we have

$$\begin{aligned} I_e^{\text{ins}}(D) - I_e^{\min}(D) &= \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(V; X) - I(V; Z) + I(X; Z) \\ &\quad - \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(V; X) - I(V; Y) + I(X; Z) \qquad (13.40) \\ &\ge \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(V; Y) - I(V; Z) \qquad (13.41) \\ &= \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \le D}} I(V; Y|Z) \qquad (13.42) \end{aligned}$$

where (13.42) comes from the Markov chain $V \to Y \to Z$. Next, we note the following lemma.

Lemma 13.1 *For jointly Gaussian (X, Y, Z) satisfying the Markov chain $X \to$*

$Y \to Z$ and $\Pr[Y = Z] \neq 1$, if $D < \sigma^2_{x|y}$, we have

$$\min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{x|vy} \leq D}} I(V;Y|Z) > 0 \tag{13.43}$$

The proof of Lemma 13.1 can be found in Appendix 13.7.2. The proof of Lemma 13.1 starts with the observation that (13.43) is zero iff we have the Markov chain $V \to Z \to Y$. On the other hand, since we already have the Markov chain $V \to X \to Y \to Z$, and Y and Z are not identical, we show in Appendix 13.7.2 that the Markov chain $V \to Z \to Y$ is possible iff V and X are independent. However, if $D < \sigma^2_{x|y}$, any V that is independent of X is not feasible. Hence, Lemma 13.1 follows. Lemma 13.1 implies that in general, we have $I_e^{\text{ins}}(D) \neq I_e^{\min}(D)$, i.e., $I_e^{\min}(\mathbf{D})$ cannot be achieved by instantaneous encoding.

This example shows that an uncoded transmission is not optimal even when there is no rate constraint. This is due to the presence of an eavesdropper; the presence of an eavesdropper necessitates the use of a coded scheme.

Another question that Theorem 13.5 brings about is whether the minimum in (13.33) is achieved by a non-trivial $\mathbf{K}_{X|U}$. By a trivial selection for $\mathbf{K}_{X|U}$ we mean either $\mathbf{K}_{X|U} = \mathbf{K}_X$ or $\mathbf{K}_{X|U} = \mathbf{K}_{X|V}$. The former corresponds to the selection $U = \phi$ and the latter corresponds to the selection $U = V$. We note that although (13.33) is monotonically decreasing in $\mathbf{K}_{X|V}$ in the positive semi-definite sense, (13.33) is neither monotonically increasing nor monotonically decreasing in $\mathbf{K}_{X|U}$ in the positive semi-definite sense. Hence, due to this lack of monotonicity of (13.33) in $\mathbf{K}_{X|U}$, in general, we expect that both $U \neq \phi$ and $U \neq V$ may be necessary to attain the

minimum in (13.33). The following example demonstrates that in general $U \neq \phi$ and $U \neq V$ may be necessary.

Example 13.2 *Consider the Gaussian source* $\mathbf{X} = [\, X_1 \;\; X_2 \,]^\top$ *where* X_1 *and* X_2 *are independent. The side information at the legitimate receiver and the eavesdropper are given by*

$$Y_\ell = X_\ell + N_{Y,\ell}, \quad \ell = 1, 2 \tag{13.44}$$

$$Z_\ell = X_\ell + N_{Z,\ell}, \quad \ell = 1, 2 \tag{13.45}$$

where $N_{Y,\ell}$ *and* $N_{Z,\ell}$ *are zero-mean Gaussian random variables with variances* $\sigma^2_{Y,\ell}$ *and* $\sigma^2_{Z,\ell}$*, respectively. Moreover,* $N_{Y,1}$ *and* $N_{Y,2}$ *are independent, and also so are* $N_{Z,1}$ *and* $N_{Z,2}$*. We assume that noise variances satisfy*

$$\sigma^2_{Y,1} < \sigma^2_{Z,1} \tag{13.46}$$

$$\sigma^2_{Z,2} < \sigma^2_{Y,2} \tag{13.47}$$

which, in view of the fact that correlation between the noise at the legitimate receiver and the noise at the eavesdropper does not affect the rate, distortion and information leakage region, lets us assume the following Markov chains

$$X_1 \to Y_1 \to Z_1 \tag{13.48}$$

$$X_2 \to Z_2 \to Y_2 \tag{13.49}$$

Moreover, we assume that the distortion constraint $\mathbf{D}$ *is a diagonal matrix with diagonal entries* D_1 *and* D_2*. In this case, the minimum information leakage is given by*

$$I_e^{\min}(D_1, D_2) = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1; X_1) - I(V_1; Y_1) + I(X_1; Z_1)$$
$$+ \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; X_2) + I(X_2; Z_2|V_2) \tag{13.50}$$

whose proof can be found in Appendix 13.7.3. The minimum information leakage in (13.50) corresponds the selections $U = (\phi, V_2)$ *and* $V = (V_1, V_2)$*, where* (U_1, V_1) *and* (U_2, V_2) *are independent. This selection of* (U, V) *corresponds to neither* $U = \phi$ *nor* $U = V$*.*

Next, we obtain the minimum information leakage that arises when we set either $U = \phi$ *or* $U = V$*, and show that the minimum information leakage arising from these selections are strictly larger than the minimum information leakage in (13.50), which will imply the suboptimality of* $U = \phi$ *and* $U = V$*. When we set* $U = \phi$*, the minimum information leakage is given by*

$$I_e^{\min-\phi}(D_1, D_2) = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1; X_1) - I(V_1; Y_1) + I(X_1; Z_1)$$
$$+ \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; X_2) - I(V_2; Y_2) + I(X_2; Z_2) \tag{13.51}$$

whose proof is given in Appendix 13.7.4. When we set $U = V$*, the minimum infor-*

mation leakage is given by

$$I_e^{\min-\mathrm{S}}(D_1, D_2) = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1; X_1) + I(X_1; Z_1|V_1)$$

$$+ \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; X_2) + I(X_2; Z_2|V_2) \tag{13.52}$$

whose proof can be found in Appendix 13.7.4.

Now, we compare the minimum information leakage in (13.50) with (13.51) and (13.52) to show that the selections $U = \phi$ and $U = V$ are sub-optimal in general. Using (13.50) and (13.51), we get

$$I_e^{\min-\phi}(D_1, D_2) - I_e^{\min}(D_1, D_2)$$

$$= \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; X_2) - I(V_2; Y_2) + I(X_2; Z_2)$$

$$- \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; X_2) + I(X_2; Z_2|V_2) \tag{13.53}$$

$$\geq \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(X_2; Z_2) - I(X_2; Z_2|V_2) - I(V_2; Y_2) \tag{13.54}$$

$$= \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; Z_2) - I(V_2; Y_2) \tag{13.55}$$

$$= \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; Z_2|Y_2) \tag{13.56}$$

$$> 0 \tag{13.57}$$

where (13.55)-(13.56) follow from the Markov chain

$$V_2 \to X_2 \to Z_2 \to Y_2 \tag{13.58}$$

and (13.57) comes from Lemma 13.1. Thus, in general, we have $I_e^{\min-\phi}(D_1, D_2) \neq I_e^{\min}(D_1, D_2)$*, or in other words, in general,* $U = \phi$ *is sub-optimal.*

Next, we consider the selection $U = V$*. Using (13.50) and (13.52), we have*

$$\begin{aligned}
&I_e^{\min-\mathrm{S}}(D_1, D_2) - I_e^{\min}(D_1, D_2) \\
&\quad = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(V_1; X_1) + I(X_1; Z_1|V_1) \\
&\qquad - \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(V_1; X_1) - I(V_1; Y_1) + I(X_1; Z_1) && (13.59) \\
&\qquad \ge \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(X_1; Z_1|V_1) + I(V_1; Y_1) - I(X_1; Z_1) && (13.60) \\
&\qquad = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(V_1; Y_1) - I(V_1; Z_1) && (13.61) \\
&\qquad = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(V_1; Y_1|Z_1) && (13.62) \\
&\qquad > 0 && (13.63)
\end{aligned}$$

where (13.61)-(13.62) follow from the Markov chain

$$V_1 \to X_1 \to Y_1 \to Z_1 \tag{13.64}$$

and (13.63) comes from Lemma 13.1. Thus, in general, we have $I_e^{\min-\mathrm{S}}(D_1, D_2) \neq I_e^{\min}(D_1, D_2)$*, or in other words, in general,* $U = V$ *is sub-optimal.*

Example 13.2 shows that, in general, we might need two covariance matrices, and hence two different auxiliary random variables, to attain the minimum information leakage. Indeed, if we have either $U = V$ or $U = \phi$, the corresponding achievable scheme is identical to the Wyner-Ziv scheme [113]. Hence, the necessity of two different auxiliary random variables implies that, in general, Wyner-Ziv scheme [113] is suboptimal.

13.4 Proof of Theorem 13.4

We now provide the proof of Theorem 13.4. As mentioned in the previous section, this outer bound is obtained by minimizing the rate constraint in (13.22) and the mutual information leakage constraint in (13.23) separately. We first consider the rate constraint in (13.22) as follows

$$R \geq L(1,0) = \min_{\substack{V \to \mathbf{X} \to \mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V;\mathbf{X}|\mathbf{Y}) \tag{13.65}$$

$$= \min_{\substack{V \to \mathbf{X} \to \mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} h(\mathbf{X}|\mathbf{Y}) - h(\mathbf{X}|V,\mathbf{Y}) \tag{13.66}$$

$$= \min_{\substack{V \to \mathbf{X} \to \mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} \frac{1}{2}\log|(2\pi e)\mathbf{K}_{X|Y}| - h(\mathbf{X}|V,\mathbf{Y}) \tag{13.67}$$

$$= \min_{\mathbf{K}_{X|VY} \preceq \mathbf{D}} \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{K}_{X|VY}|} \tag{13.68}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \tag{13.69}$$

where (13.68) comes from the fact that $h(\mathbf{X}|V,\mathbf{Y})$ is maximized by jointly Gaussian $(V,\mathbf{X},\mathbf{Y})$, and (13.69) comes from the monotonicity of $|\cdot|$ in positive semi-definite matrices. Now we introduce the following lemma.

Lemma 13.2

$$\frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|}=\frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|}-\frac{1}{2}\log\frac{|\mathbf{K}_X+\mathbf{\Sigma}_Y|}{|\mathbf{F}(\mathbf{D})+\mathbf{\Sigma}_Y|} \tag{13.70}$$

The proof of Lemma 13.2 is given in Appendix 13.7.5. Lemma 13.2 and (13.69) imply (13.27).

Next, we consider the mutual information leakage constraint in (13.23) as follows

$$I_e \geq L(0,1)=\min_{\substack{U\to V\to\mathbf{X}\to\mathbf{Y},\mathbf{Z}\\ \mathbf{K}_{X|VY}\preceq\mathbf{D}}} I(V;\mathbf{X})-I(V;\mathbf{Y}|U)+I(\mathbf{X};\mathbf{Z}|U) \tag{13.71}$$

We note that the cost function of $L(0,1)$ can be rewritten as follows

$$C(L)=I(V;\mathbf{X})-I(V;\mathbf{Y})+I(U;\mathbf{Y})+I(\mathbf{X};\mathbf{Z}|U) \tag{13.72}$$

$$=I(V;\mathbf{X}|\mathbf{Y})+[I(U;\mathbf{Y})+I(\mathbf{X};\mathbf{Z}|U)] \tag{13.73}$$

where (13.72) comes from the Markov chain $U\to V\to\mathbf{Y}$ and (13.73) comes from the Markov chain $V\to\mathbf{X}\to\mathbf{Y}$. We note that the first term in (13.73) is minimized by a jointly Gaussian $(V,\mathbf{X})$ as we already showed in obtaining the lower bound for the rate given by (13.27) above in (13.65)-(13.69). On the other hand, the

remaining term of (13.73) in the bracket is maximized by a jointly Gaussian $(U, \mathbf{X})$ as shown in [51]. Thus, a tension between these two terms arises if $(U, V, \mathbf{X})$ is selected to be jointly Gaussian. In spite of this tension, we will still show that a jointly Gaussian $(U, V, \mathbf{X})$ is the minimizer of $L(0, 1)$. Instead of directly showing this, we first characterize the minimum mutual information leakage when $(U, V, \mathbf{X})$ is restricted to be jointly Gaussian, and show that this cannot be attained by any other distribution for $(U, V, \mathbf{X})$. We note that any jointly Gaussian $(U, V, \mathbf{X})$ can be written as

$$V = \mathbf{A}_V \mathbf{X} + \mathbf{N}_V \tag{13.74}$$

$$U = \mathbf{A}_U \mathbf{X} + \mathbf{N}_U \tag{13.75}$$

where $\mathbf{N}_V, \mathbf{N}_U$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_V, \mathbf{\Sigma}_U$, respectively. Moreover, $\mathbf{N}_V, \mathbf{N}_U$ are independent of $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$, but can be dependent on each other. Before characterizing the minimum mutual information leakage when $(U, V, \mathbf{X})$ is restricted to be jointly Gaussian, we introduce the following lemma.

Lemma 13.3 *When $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ and V is Gaussian, we have the following facts.*

- $\mathbf{\Sigma}_Y - \mathbf{D} \succ \mathbf{0}$*, i.e.,* $\mathbf{\Sigma}_Y - \mathbf{D}$ *is positive definite, and hence, non-singular.*
- *We have the following equivalence:*

$$\mathbf{K}_{X|VY} \preceq \mathbf{D} \iff \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D}) \tag{13.76}$$

The proof of Lemma 13.3 is given in Appendix 13.7.6. Using Lemma 13.3, the minimum mutual information leakage to the eavesdropper when $(U, V, \mathbf{X})$ is restricted to be jointly Gaussian can be written as follows:

$$L^G = \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ (U,V,\mathbf{X}) \text{ is jointly Gaussian} \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U) \tag{13.77}$$

We note that the minimization in (13.77) can be written as a minimization of the cost function in (13.77) over all possible $\mathbf{A}_U, \mathbf{A}_V, \mathbf{\Sigma}_U, \mathbf{\Sigma}_V$ matrices by expressing $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ in terms of $\mathbf{A}_U, \mathbf{A}_V, \mathbf{\Sigma}_U, \mathbf{\Sigma}_V$. Instead of considering this tedious optimization problem, we consider the following one:

$$\bar{L}^G = \min_{\substack{\mathbf{0} \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.78}$$

We note that due to the Markov chain $U \to V \to \mathbf{X}$, we always have $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$. A proof of this fact is given in Appendix 13.7.7. Besides this inequality, $\mathbf{K}_{X|V}$ and $\mathbf{K}_{X|U}$ might have further interdependencies which are not considered in the optimization problem in (13.78). Since neglecting these further interdependencies among $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ enlarges the feasible set of the optimization problem in (13.77), we have, in general,

$$L^G \geq \bar{L}^G \tag{13.79}$$

On the other hand, it can be shown that the value of $\bar{L}^G$ can be obtained by some jointly Gaussian $(U, V, \mathbf{X})$ satisfying the Markov chain $U \to V \to \mathbf{X}$, as stated in the following lemma.

Lemma 13.4

$$L^G = \bar{L}^G \tag{13.80}$$

The proof of Lemma 13.4 is given in Appendix 13.7.8.

Now we study the optimization problem $\bar{L}^G$ in (13.78) in more detail. Let $\mathbf{K}^*_{X|V}$ and $\mathbf{K}^*_{X|U}$ be the minimizers for the optimization problem $\bar{L}^G$. They need to satisfy the following KKT conditions.

Lemma 13.5 *If $\mathbf{K}^*_{X|V}$ and $\mathbf{K}^*_{X|U}$ are the minimizers for the optimization problem $\bar{L}^G$, they need to satisfy*

$$(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U + \mathbf{M}_D = (\mathbf{K}^*_{X|V})^{-1} \tag{13.81}$$

$$(\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_X = (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U \tag{13.82}$$

$$\mathbf{M}_U(\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V}) = (\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V})\mathbf{M}_U = \mathbf{0} \tag{13.83}$$

$$\mathbf{M}_D(\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V}) = (\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V})\mathbf{M}_D = \mathbf{0} \tag{13.84}$$

$$\mathbf{M}_X(\mathbf{K}_X - \mathbf{K}^*_{X|U}) = (\mathbf{K}_X - \mathbf{K}^*_{X|U})\mathbf{M}_X = \mathbf{0} \tag{13.85}$$

for some positive semi-definite matrices $\mathbf{M}_U, \mathbf{M}_D, \mathbf{M}_X$.

The proof of Lemma 13.5 is given in Appendix 13.7.9.

Next, we use channel enhancement [4]. In particular, we enhance the legitimate user's side information as follows.

$$(\mathbf{K}^*_{X|U} + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U \tag{13.86}$$

This new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ has some useful properties which are listed in the following lemma.

Lemma 13.6 *We have the following facts.*

- $\mathbf{0} \preceq \tilde{\mathbf{\Sigma}}_Y$
- $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y, \tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$
- $(\mathbf{K}^*_{X|V} + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U$
- $(\mathbf{K}^*_{X|U} + \tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{K}^*_{X|V} + \tilde{\mathbf{\Sigma}}_Y) = (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y)^{-1}(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)$
- $(\mathbf{K}^*_{X|U} + \tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y) = (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Z)^{-1}(\mathbf{K}_X + \mathbf{\Sigma}_Z)$
- $(\mathbf{K}^*_{X|V} + \tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{F}(\mathbf{D}) + \tilde{\mathbf{\Sigma}}_Y) = (\mathbf{K}^*_{X|V})^{-1}\mathbf{F}(\mathbf{D})$

The proof of Lemma 13.6 is given in Appendix 13.7.10. Using this new covariance $\tilde{\mathbf{\Sigma}}_Y$, we define the *enhanced* side information at the legitimate user $\tilde{\mathbf{Y}}$ as follows

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y \tag{13.87}$$

where $\tilde{\mathbf{N}}_Y$ is a zero-mean Gaussian random vector with covariance matrix $\tilde{\mathbf{\Sigma}}_Y$. Since we have $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y$ and $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$ as stated in the second statement of Lemma 13.6,

without loss of generality, we can assume that the following Markov chain exists.

$$\mathbf{X} \rightarrow \tilde{\mathbf{Y}} \rightarrow \mathbf{Y}, \mathbf{Z} \tag{13.88}$$

Assuming that the Markov chain in (13.88) exists does not incur any loss of generality because the rate, mutual information leakage and distortion region $\mathcal{R}$ depends only on the conditional marginal distributions $p(\mathbf{Y}|\mathbf{X}), p(\mathbf{Z}|\mathbf{X})$ but not on the conditional joint distribution $p(\mathbf{Y}, \mathbf{Z}|\mathbf{X})$. Now, we define the following optimization problem:

$$\bar{L} = \min_{\substack{U \rightarrow V \rightarrow \mathbf{X} \rightarrow \tilde{\mathbf{Y}} \rightarrow \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}|U) + I(\mathbf{X}; \mathbf{Z}|U) \tag{13.89}$$

We note that we have $I(V; \mathbf{Y}|U) \leq I(V; \tilde{\mathbf{Y}}|U)$ due to the Markov chain in (13.88), which leads to the following fact:

$$L^G = \bar{L}^G \geq L(0, 1) \geq \bar{L} \tag{13.90}$$

Moreover, unlike the original optimization problem $L(0, 1)$ in (13.71), we can find the minimizer of the new optimization problem $\bar{L}$ explicitly, as stated in the following lemma.

Lemma 13.7

$$\bar{L} = \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D}) + \tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.91}$$

We note that Lemma 13.7 implies that $U = \phi$ and a Gaussian V leading to $\mathbf{K}_{X|V} = \mathbf{F}(\mathbf{D})$ is the minimizer of the optimization problem $\bar{L}$. The proof of Lemma 13.7 is given in Appendix 13.7.11.

Next, we show that indeed $L^G = \bar{L}^G = \bar{L}$ which, in view of (13.90), will imply $L(0,1) = \bar{L} = \bar{L}^G = L^G$. To this end, using Lemma 13.7, we have

$$\bar{L} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D}) + \tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.92}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}^*_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}^*_{X|V} + \tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.93}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}^*_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}^*_{X|U} + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}^*_{X|V} + \tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.94}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}^*_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y|}{|\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.95}$$

$$= \bar{L}^G = L^G \tag{13.96}$$

where (13.93) comes from the last statement of Lemma 13.6, (13.94) follows from the fifth statement of Lemma 13.6, and (13.95) comes from the fourth statement of Lemma 13.6. In view of (13.90), (13.96) implies that $L(0,1) = L^G$; completing the proof of Theorem 13.4 as well as the proof of Theorem 13.5 due to the fact that $I_e^{\min} = L(0,1)$.

13.5 General Case

We now consider the general case where the side information are given by

$$\mathbf{Y} = \mathbf{H}_Y \mathbf{X} + \mathbf{N}_Y \tag{13.97}$$

$$\mathbf{Z} = \mathbf{H}_Z \mathbf{X} + \mathbf{N}_Z \tag{13.98}$$

where without loss of generality, we can assume that the covariance matrices of Gaussian vectors $\mathbf{N}_Y$ and $\mathbf{N}_Z$ are given by identity matrices. We denote the singular value decomposition of $\mathbf{H}_Y$ and $\mathbf{H}_Z$ by $\mathbf{H}_Y = \mathbf{Q}_Y \mathbf{\Lambda}_Y \mathbf{R}_Y^\top$ and $\mathbf{H}_Z = \mathbf{Q}_Z \mathbf{\Lambda}_Z \mathbf{R}_Z^\top$, respectively. Since any invertible transformation applied to the side information does not change the rate, information leakage, and distortion region, the side information given by (13.97)-(13.98) and the side information obtained by multiplying (13.97)-(13.98) by $\mathbf{Q}_Y^\top, \mathbf{Q}_Z^\top$, respectively, yield the same rate, information leakage and distortion region. In other words, the side information given by (13.97)-(13.98) and the side information given by

$$\bar{\mathbf{Y}} = \mathbf{\Lambda}_Y \mathbf{R}_Y^\top \mathbf{X} + \bar{\mathbf{N}}_Y \tag{13.99}$$

$$\bar{\mathbf{Z}} = \mathbf{\Lambda}_Z \mathbf{R}_Z^\top \mathbf{X} + \bar{\mathbf{N}}_Z \tag{13.100}$$

yield the same rate, information leakage and distortion region, where the covariance matrices of $\bar{\mathbf{N}}_Y, \bar{\mathbf{N}}_Z$ are given by identity matrices. Next, we claim that there is no loss of generality to assume that the side information $\bar{\mathbf{Y}}$ and $\bar{\mathbf{Z}}$ have the same length as the source $\mathbf{X}$. To this end, assume that the length of $\bar{\mathbf{Y}}$ is smaller than the length

of $\mathbf{X}$. In this case, simply, we can concatenate $\bar{\mathbf{Y}}$ with some zero vector to ensure that both $\bar{\mathbf{Y}}$ and $\mathbf{X}$ have the same length. Next, assume that the length of $\bar{\mathbf{Y}}$ is larger than the length of $\mathbf{X}$. In this case, $\mathbf{\Lambda}_Y$ will definitely have at least $\text{length}(\bar{\mathbf{Y}}) - \text{length}(\mathbf{X})$ diagonal elements which are zero, and hence the corresponding entries in $\bar{\mathbf{Y}}$ will come from only the noise. Since noise components are independent, dropping these elements of $\bar{\mathbf{Y}}$ does not change the rate, information leakage and distortion region. Thus, without loss of generality, we can assume that $\text{length}(\bar{\mathbf{Y}}) = \text{length}(\mathbf{X})$, and hence without loss of generality, we can assume that $\mathbf{\Lambda}_Y$ is a square matrix. The same argument applies to the eavesdropper's side information, and hence, without loss of generality, we can also assume that $\mathbf{\Lambda}_Z$ is a square matrix. Next, we define the following side information

$$\bar{\mathbf{Y}}_\alpha = (\mathbf{\Lambda}_Y + \alpha \mathbf{I})\mathbf{R}_Y^\top \mathbf{X} + \bar{\mathbf{N}}_Y \tag{13.101}$$

$$\bar{\mathbf{Z}}_\alpha = (\mathbf{\Lambda}_Z + \alpha \mathbf{I})\mathbf{R}_Z^\top \mathbf{X} + \bar{\mathbf{N}}_Z \tag{13.102}$$

where $\alpha > 0$. We note that $(\mathbf{\Lambda}_Y + \alpha \mathbf{I})$ and $(\mathbf{\Lambda}_Y + \alpha \mathbf{I})$ are invertible matrices. Since multiplying the side information in (13.101)-(13.98) by some invertible matrices does not change the rate, information leakage and distortion region, the side information in (13.101)-(13.102) and the following side information

$$\bar{\bar{\mathbf{Y}}}_\alpha = \mathbf{X} + \bar{\mathbf{N}}_{Y,\alpha} \tag{13.103}$$

$$\bar{\bar{\mathbf{Z}}}_\alpha = \mathbf{X} + \bar{\mathbf{N}}_{Z,\alpha} \tag{13.104}$$

have the same rate, information leakage and distortion region, where the covariance matrices of $\bar{\mathbf{N}}_{Y,\alpha}$ and $\bar{\mathbf{N}}_{Z,\alpha}$ are given by

$$\mathbf{\Sigma}_{Y,\alpha} = \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-2}\mathbf{R}_Y^\top \tag{13.105}$$

$$\mathbf{\Sigma}_{Z,\alpha} = \mathbf{R}_Z(\mathbf{\Lambda}_Z + \alpha\mathbf{I})^{-2}\mathbf{R}_Z^\top \tag{13.106}$$

respectively. For a given distortion constraint $\mathbf{D}$, we denote the rate and information leakage region for the side information model given in (13.97)-(13.98) by $\mathcal{R}_o(\mathbf{D})$, where the subscript o stands for the "original system", and for the side information model given in (13.103)-(13.104) by $\mathcal{R}_\alpha(\mathbf{D})$. We have the following relationship between $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$.

Lemma 13.8

$$\mathcal{R}_o(\mathbf{D}) \subseteq \lim_{\alpha\to 0} \mathcal{R}_\alpha(\mathbf{D}) \tag{13.107}$$

The proof of Lemma 13.8 is given in Appendix 13.7.12. Next, using Theorem 13.4, we obtain an outer bound for the region $\lim_{\alpha\to 0} \mathcal{R}_\alpha(\mathbf{D})$, where this outer bound also serves as an outer bound for the region $\mathcal{R}_o(\mathbf{D})$ due to Lemma 13.8. The corresponding result is stated in the following theorem.

Theorem 13.6 *If* $\mathbf{D} \preceq \mathbf{K}_{X|Y}$*, any* $(R, I_e) \in \mathcal{R}_o(\mathbf{D})$ *satisfies*

$$R \geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}_o(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_X\mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y\mathbf{F}_o(\mathbf{D})\mathbf{H}_Y^\top + \mathbf{I}|} \tag{13.108}$$

$$\begin{aligned} I_e \geq \min_{\substack{\mathbf{0}\preceq\mathbf{K}_{X|V}\preceq\mathbf{K}_{X|U}\preceq\mathbf{K}_X \\ \mathbf{K}_{X|V}\preceq\mathbf{F}_o(\mathbf{D})}} & \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y\mathbf{K}_{X|V}\mathbf{H}_Y^\top + \mathbf{I}|} \\ & + \frac{1}{2}\log|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}| \end{aligned} \tag{13.109}$$

where $\mathbf{F}_o(\mathbf{D}) = (\mathbf{D}^{-1} - \mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}$.

The proof of Theorem 13.6 is given in Appendix 13.7.13. We prove Theorem 13.6 in two steps. In the first step, by using Theorem 13.4, we obtain an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$, and in the second step, we obtain the limit of this outer bound as $\alpha \to 0$. As the outer bound in Theorem 13.6 basically comes from the outer bound in Theorem 13.4, all our previous comments and remarks about Theorem 13.4 are also valid for the outer bound in Theorem 13.6. Similar to Theorem 13.4, Theorem 13.6 also provides the minimum information leakage to the eavesdropper when the rate constraint on the transmitter is removed. Denoting the corresponding minimum information leakage by $I_e^{\min}(\mathbf{D})$, we have the following theorem.

Theorem 13.7 *If* $\mathbf{D} \preceq \mathbf{K}_{X|Y}$*, we have*

$$\begin{aligned} I_e^{\min}(\mathbf{D}) \geq \min_{\substack{\mathbf{0}\preceq\mathbf{K}_{X|V}\preceq\mathbf{K}_{X|U}\preceq\mathbf{K}_X \\ \mathbf{K}_{X|V}\preceq\mathbf{F}_o(\mathbf{D})}} & \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y\mathbf{K}_{X|V}\mathbf{H}_Y^\top + \mathbf{I}|} \\ & + \frac{1}{2}\log|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}| \end{aligned} \tag{13.110}$$

where $\mathbf{F}_o(\mathbf{D}) = (\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}$.

As Theorem 13.7 basically comes from Theorem 13.5, all our previous comments and remarks about Theorem 13.5 are also valid for Theorem 13.7.

13.6 Conclusions

In this chapter, we study secure lossy source coding for vector Gaussian sources, where the transmitter sends information about the source in a way that the legitimate user can reconstruct the source within a distortion level by using its side information. Meanwhile, the transmitter wants to keep the mutual information leakage to the eavesdropper to a minimum, where the eavesdropper also has a side information about the source. We obtain an outer bound for the achievable rate, mutual information leakage, and distortion region. We obtain the minimum mutual information leakage to the eavesdropper when the legitimate user needs to reconstruct the source within a certain distortion while there is no constraint on the transmission rate.

13.7 Appendix

13.7.1 Proof of (13.38)

We first define the following function

$$R(D) = \min_{\substack{V \to X \to Y,Z \\ \sigma^2_{X|VY} \le D}} I(X; V, Z) \tag{13.111}$$

which is monotonically decreasing, continuous and convex in D. Next, we note that when an instantaneous encoding scheme is used, the minimum-mean-square-error estimator is given by

$$\hat{X}_i = E\left[X_i | g_1(X_1), \ldots, g_n(X_n), Y^n\right] \tag{13.112}$$

$$= E\left[X_i | g_i(X_i), Y_i\right] \tag{13.113}$$

where (13.113) comes from the independence of $(X_i, g_i(X_i), Y_i)$ across time. Consequently, when an instantaneous encoding scheme is used, the minimum-mean-square-error is given by

$$\sigma^2_{X_i|g_i(X_i)Y_i} = E\left[\left(X_i - E\left[X_i|g_i(X_i), Y_i\right]\right)^2\right] \tag{13.114}$$

Assume that there exists an instantaneous encoding scheme that achieves the distortion level D:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \sigma^2_{X_i|g_i(X_i)Y_i} \leq D \tag{13.115}$$

We now obtain a lower bound for the minimum information leakage for this instantaneous encoding scheme as follows

$$\lim_{n\to\infty} \frac{1}{n} I(X^n; M, Z^n) = \lim_{n\to\infty} \frac{1}{n} I(X^n; g_1(X_1), \ldots, g_n(X_n), Z^n) \tag{13.116}$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} I(X_i; g_i(X_i), Z_i) \tag{13.117}$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} I(X_i; V_i, Z_i) \tag{13.118}$$

$$\geq \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} R\left(\sigma^2_{X_i|V_iY_i}\right) \tag{13.119}$$

$$\geq \lim_{n\to\infty} R\left(\frac{1}{n} \sum_{i=1}^{n} \sigma^2_{X_i|V_iY_i}\right) \tag{13.120}$$

$$= R\left(\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \sigma^2_{X_i|V_iY_i}\right) \tag{13.121}$$

$$\geq R(D) \tag{13.122}$$

where (13.117) comes from the independence of $(X_i, g_i(X_i), Z_i)$ across time, (13.118) follows by setting $V_i = g_i(X_i)$, (13.119) comes from the definition of $R(D)$, (13.120) is due to the convexity of $R(D)$ in D, (13.121) follows from the fact that $R(D)$ is continuous in D, and (13.122) comes from (13.115) and the fact that $R(D)$ is monotonically decreasing in D.

13.7.2 Proof of Lemma 13.1

We first introduce two lemmas that will be used in the proof of Lemma 13.1. Throughout this appendix, we use notation $A \perp\!\!\!\perp B$ to denote "A and B are independent" to shorten the presentation.

Lemma 13.9 *Let Q, T, W be arbitrary random variables. If we have $Q \to T \to T + W$ and $T \perp\!\!\!\perp W$. Then, we have $(Q, T) \perp\!\!\!\perp W$.*

Proof: Since a set of random variables is independent iff their joint characteristic function is the product of their individual characteristic functions, to prove

Lemma 13.9, it is sufficient to show the following.

$$E\left[e^{s_1Q+s_2T+s_3W}\right] = E\left[e^{s_1Q+s_2T}\right] E\left[e^{s_3W}\right], \quad \forall(s_1, s_2, s_3) \tag{13.123}$$

We can show this as follows

$$\begin{aligned}
E\left[e^{s_1Q+s_2T+s_3W}\right] &= E\left[E\left[e^{s_1Q+s_2T+s_3W}\middle|T\right]\right] && (13.124)\\
&= E\left[e^{(s_2-s_3)T}\ E\left[e^{s_1Q+s_3(T+W)}\middle|T\right]\right] && (13.125)\\
&= E\left[e^{(s_2-s_3)T}\ E\left[e^{s_1Q}\middle|T\right] E\left[e^{s_3(T+W)}\middle|T\right]\right] && (13.126)\\
&= E\left[e^{s_2T}\ E\left[e^{s_1Q}\middle|T\right] E\left[e^{s_3W}\middle|T\right]\right] && (13.127)\\
&= E\left[e^{s_2T}\ E\left[e^{s_1Q}\middle|T\right] E\left[e^{s_3W}\right]\right] && (13.128)\\
&= E\left[e^{s_2T}\ E\left[e^{s_1Q}\middle|T\right]\right] E\left[e^{s_3W}\right] && (13.129)\\
&= E\left[e^{s_1Q+s_2T}\right] E\left[e^{s_3W}\right] && (13.130)
\end{aligned}$$

where (13.126) comes from the Markov chain $Q \to T \to T+W$ and (13.128) follows from the fact that $T \perp\!\!\!\perp W$. Equation (13.130) implies the independence between (Q, T) and W; completing the proof of Lemma 13.9. □

Lemma 13.10 *Let Q, T, W be random variables satisfying $(T, Q) \perp\!\!\!\perp W$ and $Q \perp\!\!\!\perp T + W$. Then, we have $Q \perp\!\!\!\perp T$.*

Proof: Similar to the proof of Lemma 13.9, here also we use the fact that a set of random variables is independent iff their joint characteristic function is the product of their individual characteristic functions. To this end, since $(T, Q) \perp\!\!\!\perp W$,

we have

$$E\left[e^{s_1W+s_2T+s_3Q}\right] = E\left[e^{s_1W}\right] E\left[e^{s_2T+s_3Q}\right], \quad \forall(s_1, s_2, s_3) \tag{13.131}$$

If we set $s_1 = s_2$ in (13.131), we get

$$E\left[e^{s_2W+s_2T+s_3Q}\right] = E\left[e^{s_2W}\right] E\left[e^{s_2T+s_3Q}\right], \quad \forall(s_2, s_3) \tag{13.132}$$

On the other hand, since $Q \perp\!\!\!\perp T + W$, we have

$$E\left[e^{s_2W+s_2T+s_3Q}\right] = E\left[e^{s_2(W+T)}\right] E\left[e^{s_3Q}\right] \tag{13.133}$$

$$= E\left[e^{s_2W}\right] E\left[e^{s_2T}\right] E\left[e^{s_3Q}\right] \tag{13.134}$$

where (13.134) comes from the fact that $T \perp\!\!\!\perp W$. In view of (13.132) and (13.134), we have

$$E\left[e^{s_2T+s_3Q}\right] = E\left[e^{s_2T}\right] E\left[e^{s_3Q}\right] \tag{13.135}$$

which implies that $T \perp\!\!\!\perp Q$; completing the proof of Lemma 13.10. □

We now prove Lemma 13.1. We note that we have $I(V;Y|Z) = 0$ iff the Markov chain $V \to Z \to Y$ holds. We prove by contradiction that when $D < \sigma^2_{x|y}$, the Markov chain $V \to Z \to Y$ is not possible. To this end, we note that the side

information at the eavesdropper can be written as

$$Z = X + N_y + \tilde{N}_z \tag{13.136}$$

or in other words, we have $N_z = N_y + \tilde{N}_z$ where $\tilde{N}_z$ is a Gaussian random variable independent of (X, N_y) with variance $\sigma_z^2 - \sigma_y^2 > 0$. Next, we note that the Markov chain $V \to X \to Y \to Z$ implies $(V, X) \perp\!\!\!\perp (N_y, \tilde{N}_z)$ in view of Lemma 13.9. Since Y, Z are jointly Gaussian, Y can be written as

$$Y = \alpha Z + (Y - \alpha Z) \tag{13.137}$$

where $\alpha = E[YZ]/E[Z^2]$, and as a consequence of this α choice, we have $Z \perp\!\!\!\perp Y - \alpha Z$. Hence, if we have the Markov chain

$$V \to Z \to Y = \alpha Z + (Y - \alpha Z) \tag{13.138}$$

then, Lemma 13.9 implies that $V \perp\!\!\!\perp Y - \alpha Z$, where $Y - \alpha Z$ is

$$Y - \alpha Z = (1 - \alpha)X + (1 - \alpha)N_y - \tilde{N}_z \tag{13.139}$$

Since $(V, X) \perp\!\!\!\perp (N_y, \tilde{N}_z)$, we have $(V, X) \perp\!\!\!\perp (1 - \alpha)N_y - \tilde{N}_z$, and also $V \perp\!\!\!\perp (1 - \alpha)X + (1 - \alpha)N_y - \tilde{N}_z$ due to the assumption that the Markov chain $V \to Z \to Y$ holds. Hence, in view of Lemma 13.10, we have $V \perp\!\!\!\perp X$. Moreover, since we have the Markov chain $V \to X \to Y$, $V \perp\!\!\!\perp X$ implies that $V \perp\!\!\!\perp (X, Y)$. Hence, if

$V \perp\!\!\!\perp (X, Y)$, we have $\sigma^2_{x|vy} = \sigma^2_{x|y}$. However, if $D < \sigma^2_{x|y}$, $V \perp\!\!\!\perp X$ is not feasible, and this implies that the Markov chain $V \to Z \to Y$ is not possible; completing the proof of Lemma 13.1.

13.7.3 Proof of (13.50)

Here, we provide the proof of (13.50). To this end, we consider a slightly more general case where the joint distribution of the source and side information is given by

$$p(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \prod_{i=1}^{L} p(x_i, y_i, z_i) \tag{13.140}$$

and the distortion constraint is imposed with a diagonal matrix $\mathbf{D}$ whose diagonal entries are denoted by $D_1, \ldots, D_L$. From Theorem 13.3, the minimum information leakage is given by

$$I_e^{\min} = \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma^2_{X_i|VY^L} \le D_i,\ i=1,\ldots,L}} I(V; \mathbf{X}) - I(V; \mathbf{Y}|U) + I(\mathbf{X}; \mathbf{Z}|U) \tag{13.141}$$

We first introduce the following auxiliary random variables

$$U_i = UY^{i-1}Z_{i+1}^L, \qquad i = 1, \ldots, L \tag{13.142}$$

$$V_i = VY^{i-1}X_{i+1}^L, \qquad i = 1, \ldots, L \tag{13.143}$$

which satisfy the Markov chain

$$U_i \to V_i \to X_i \to Y_i, Z_i \tag{13.144}$$

which follows from (13.140) and the Markov chain $U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z}$.

Next, we introduce the following two lemmas.

Lemma 13.11 ([3, Lemma 7]) *Let S^n, T^n be length-n random vectors, and W be an arbitrary random variable. We have*

$$\sum_{i=1}^{n} I(T_{i+1}^n; S_i | W S^{i-1}) = \sum_{i=1}^{n} I(S^{i-1}; T_i | W T_{i+1}^n) \tag{13.145}$$

Using Lemma 13.11, the following lemma can be proved.

Lemma 13.12

$$I(W; S^n) - I(W; T^n) = \sum_{i=1}^{n} I(W; S_i | S^{i-1} T_{i+1}^n) - I(W; T_i | S^{i-1} T_{i+1}^n) \tag{13.146}$$

Now, we proceed with (13.141) as follows

$$I_e^{\min} = \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma^2_{X_i|VY^L} \le D_i,\ i=1,\ldots,L}} I(V; \mathbf{X}) - I(V; \mathbf{Y}|U) + I(\mathbf{X}; \mathbf{Z}|U) \tag{13.147}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma^2_{X_i|VY^L} \le D_i,\ i=1,\ldots,L}} I(V; \mathbf{X}) - I(V; \mathbf{Y}) + I(U; \mathbf{Y}) - I(U; \mathbf{Z}) + I(\mathbf{X}; \mathbf{Z}) \tag{13.148}$$

$$= \min_{\substack{U\to V\to \mathbf{X}\to \mathbf{Y},\mathbf{Z} \\ \sigma^2_{X_i|VY^L}\le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V;X_i|Y^{i-1},X_{i+1}^L) - I(V;Y_i|Y^{i-1},X_{i+1}^L) + \sum_{i=1}^{L} I(U;Y_i|Y^{i-1},Z_{i+1}^L) - I(U;Z_i|Y^{i-1},Z_{i+1}^L) + I(\mathbf{X};\mathbf{Z}) \tag{13.149}$$

$$= \min_{\substack{U\to V\to \mathbf{X}\to \mathbf{Y},\mathbf{Z} \\ \sigma^2_{X_i|VY^L}\le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V;X_i|Y^{i-1},X_{i+1}^L) - I(V;Y_i|Y^{i-1},X_{i+1}^L) + \sum_{i=1}^{L} I(U;Y_i|Y^{i-1},Z_{i+1}^L) - I(U;Z_i|Y^{i-1},Z_{i+1}^L) + I(X_i;Z_i) \tag{13.150}$$

$$= \min_{\substack{U\to V\to \mathbf{X}\to \mathbf{Y},\mathbf{Z} \\ \sigma^2_{X_i|VY^L}\le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(Y^{i-1},X_{i+1}^L,V;X_i) - I(Y^{i-1},X_{i+1}^L,V;Y_i) + \sum_{i=1}^{L} I(Y^{i-1},Z_{i+1}^L,U;Y_i) - I(Y^{i-1},Z_{i+1}^L,U;Z_i) + I(X_i;Z_i) \tag{13.151}$$

$$= \min_{\substack{U\to V\to \mathbf{X}\to \mathbf{Y},\mathbf{Z} \\ \sigma^2_{X_i|VY^L}\le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i;X_i) - I(V_i;Y_i) + I(U_i;Y_i) - I(U_i;Z_i) + I(X_i;Z_i) \tag{13.152}$$

$$= \min_{\substack{U\to V\to \mathbf{X}\to \mathbf{Y},\mathbf{Z} \\ \sigma^2_{X_i|VY^L}\le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i;X_i) - I(V_i;Y_i|U_i) + I(X_i;Z_i|U_i) \tag{13.153}$$

$$\ge \min_{\substack{U_i\to V_i\to X_i\to Y_i,Z_i \\ \sigma^2_{X_i|V_iY_i}\le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i;X_i) - I(V_i;Y_i|U_i) + I(X_i;Z_i|U_i) \tag{13.154}$$

where (13.148) comes from the Markov chain $U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z}$, (13.149) follows from Lemma 13.12, (13.150) and (13.151) are due to (13.140), (13.152) follows from the definitions of U_i, V_i in (13.142) and (13.143), respectively, (13.153) comes from

(13.144), and (13.154) follows from

$$\sigma^2_{X_i|VY^L} \geq \sigma^2_{X_i|VY^L X^L_{i+1}} \tag{13.155}$$

$$= \sigma^2_{X_i|VY^i X^L_{i+1}} \tag{13.156}$$

$$= \sigma^2_{X_i|V_i Y_i} \tag{13.157}$$

where (13.155) follows from the fact that conditioning reduces MMSE (which will be shown in Appendix 13.7.7), (13.156) comes from the following Markov chain

$$X_i, V, Y^i \to X^L_{i+1} \to Y^L_{i+1} \tag{13.158}$$

which is a consequence of (13.140) and the Markov chain $U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z}$, and (13.157) is obtained by using the definition of V_i given in (13.143). Hence, (13.154) implies that when the joint distribution of the source and side information can be factorized as in (13.140), the minimum information leakage is given by

$$I_e^{\min} = \min_{\substack{U_i \to V_i \to X_i \to Y_i, Z_i \\ \sigma^2_{X_i|V_i Y_i} \leq D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i; X_i) - I(V_i; Y_i|U_i) + I(X_i; Z_i|U_i) \tag{13.159}$$

We now specialize (13.159) for the case given in Example 13.2, where $L = 2$ and we have the following Markov chains

$$X_1 \to Y_1 \to Z_1 \tag{13.160}$$

$$X_2 \to Z_2 \to Y_2 \tag{13.161}$$

Under these conditions, the minimum information leakage is given by

$$
\begin{aligned}
I_e^{\min} &= \min_{\substack{U_1 \to V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1;X_1) - I(V_1;Y_1|U_1) + I(X_1;Z_1|U_1) \\
&\quad + \min_{\substack{U_2 \to V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2;X_2) - I(V_2;Y_2|U_2) + I(X_2;Z_2|U_2) \qquad (13.162) \\
&= \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1;X_1) - I(V_1;Y_1) + I(X_1;Z_1) \\
&\quad + \min_{\substack{U_2 \to V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2;X_2) - I(V_2;Y_2|U_2) + I(X_2;Z_2|U_2) \qquad (13.163) \\
&= \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1;X_1) - I(V_1;Y_1) + I(X_1;Z_1) \\
&\quad + \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2;X_2) + I(X_2;Z_2|V_2) \qquad (13.164)
\end{aligned}
$$

where (13.163)-(13.164) come from the following Markov chains

$$U_1 \to V_1 \to X_1 \to Y_1 \to Z_1 \qquad (13.165)$$

$$U_2 \to V_2 \to X_2 \to Z_2 \to Y_2 \qquad (13.166)$$

respectively; completing the proof.

13.7.4 Proofs of (13.51) and (13.52)

We first prove (13.51). To this end, we note that when the joint distribution of the source and side information is given by

$$p(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \prod_{i=1}^{L} p(x_i, y_i, z_i) \tag{13.167}$$

and the distortion constraint is imposed by a diagonal matrix $\mathbf{D}$ with diagonal entries $D_1, \ldots, D_L$, the minimum information leakage is given by

$$I_e^{\min} = \min_{\substack{U_i \to V_i \to X_i \to Y_i, Z_i \\ \sigma^2_{X_i|V_iY_i} \le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i; X_i) - I(V_i; Y_i|U_i) + I(X_i; Z_i|U_i) \tag{13.168}$$

as shown in Appendix 13.7.3 (in particular, see (13.159)). When we set $U = \phi$, in other words, when we set $U_1 = \phi, \ldots, U_L = \phi$, (13.168) reduces to

$$I_e^{\min-\phi} = \min_{\substack{V_i \to X_i \to Y_i, Z_i \\ \sigma^2_{X_i|V_iY_i} \le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i; X_i) - I(V_i; Y_i) + I(X_i; Z_i) \tag{13.169}$$

which is the desired result in (13.51).

Next, we prove (13.52) by using (13.168). When we set $U = V$, in other words, when we set $U_1 = V_1, \ldots, U_L = V_L$ in (13.168), we get

$$I_e^{\min} = \min_{\substack{U_i \to V_i \to X_i \to Y_i, Z_i \\ \sigma^2_{X_i|V_iY_i} \le D_i,\ i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i; X_i) + I(X_i; Z_i|V_i) \tag{13.170}$$

which is the desired result in (13.52).

13.7.5 Proof of Lemma 13.2

We note that since $\mathbf{X}, \mathbf{Y}$ are jointly Gaussian, we have [114, page 155]

$$\mathbf{K}_{X|Y} = \mathbf{K}_X - \mathbf{K}_{XY}\mathbf{K}_Y^{-1}\mathbf{K}_{YX} \tag{13.171}$$

$$= \mathbf{K}_X - \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{K}_X \tag{13.172}$$

$$= \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \tag{13.173}$$

where (13.172) comes from the fact that $\mathbf{Y} = \mathbf{X} + \mathbf{N}_Y$. Next, we have the following chain of equalities

$$\frac{|\mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}|}{|\mathbf{F}(\mathbf{D})(\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y)^{-1}|} = \frac{|\mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y|}{|\mathbf{F}(\mathbf{D})(\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y|} \tag{13.174}$$

$$= \frac{|\mathbf{K}_{X|Y}|}{|(\mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y)\mathbf{\Sigma}_Y^{-1}(\mathbf{\Sigma}_Y - \mathbf{D})|} \tag{13.175}$$

$$= \frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \tag{13.176}$$

where (13.175) follows from the definition of $\mathbf{F}(\mathbf{D})$, i.e., $\mathbf{F}(\mathbf{D}) = \mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y$. Equation (13.176) implies (13.70); completing the proof of Lemma 13.2.

13.7.6 Proof of Lemma 13.3

We first prove the first statement of the lemma. To this end, using (13.173), we have

$$\mathbf{K}_{X|Y} = \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \tag{13.177}$$

$$= \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \tag{13.178}$$

Hence, using (13.178), the constraint $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ can be expressed as

$$\mathbf{D} \preceq \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \tag{13.179}$$

which is

$$\mathbf{\Sigma}_Y(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \preceq \mathbf{\Sigma}_Y - \mathbf{D} \tag{13.180}$$

where $\mathbf{\Sigma}_Y(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \succ \mathbf{0}$ implying $\mathbf{\Sigma}_Y - \mathbf{D} \succ \mathbf{0}$. Hence, $\mathbf{\Sigma}_Y - \mathbf{D}$ is non-singular, and $(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}$ exists.

Next, we prove the second statement of the lemma. To this end, we note that since $(V, \mathbf{X}, \mathbf{Y})$ are jointly Gaussian, $\mathbf{Y} = \mathbf{X} + \mathbf{N}_Y$, and V is independent of $\mathbf{N}_Y$, $\mathbf{K}_{X|VY}$ is given by [114, page 155]

$$\mathbf{K}_{X|VY} = \mathbf{K}_X - [\ \mathbf{K}_{XV}\ \ \mathbf{K}_X\ ]\ \mathbf{M}^{-1}\ [\ \mathbf{K}_{XV}\ \ \mathbf{K}_X\ ]^\top \tag{13.181}$$

where $\mathbf{M}$ is given by

$$\mathbf{M} = \begin{bmatrix} \mathbf{K}_V & \mathbf{K}_{VX} \\ \mathbf{K}_{XV} & \mathbf{K}_Y \end{bmatrix} \tag{13.182}$$

Using block matrix inversion lemma [115, page 45], $\mathbf{M}^{-1}$ can be obtained as

$$\mathbf{M}^{-1} = \begin{bmatrix} \mathbf{K}_V^{-1} + \mathbf{K}_V^{-1}\mathbf{K}_{VX}\boldsymbol{\Delta}_M^{-1}\mathbf{K}_{XV}\mathbf{K}_V^{-1} & -\mathbf{K}_V^{-1}\mathbf{K}_{VX}\boldsymbol{\Delta}_M^{-1} \\ -\boldsymbol{\Delta}_M^{-1}\mathbf{K}_{XV}\mathbf{K}_V^{-1} & \boldsymbol{\Delta}_M^{-1} \end{bmatrix} \tag{13.183}$$

where $\boldsymbol{\Delta}_M$ is given by

$$\boldsymbol{\Delta}_M = \mathbf{K}_Y - \mathbf{K}_{XV}\mathbf{K}_V^{-1}\mathbf{K}_{VX} \tag{13.184}$$

$$= \mathbf{K}_X - \mathbf{K}_{XV}\mathbf{K}_V^{-1}\mathbf{K}_{VX} + \boldsymbol{\Sigma}_Y \tag{13.185}$$

$$= \mathbf{K}_{X|V} + \boldsymbol{\Sigma}_Y \tag{13.186}$$

where the last equality follows from the fact that $\mathbf{K}_{X|V} = \mathbf{K}_X - \mathbf{K}_{XV}\mathbf{K}_V^{-1}\mathbf{K}_{VX}$. Using (13.183) and (13.186), we get

$$\begin{bmatrix} \mathbf{K}_{XV} & \mathbf{K}_X \end{bmatrix} \mathbf{M}^{-1} = \begin{bmatrix} \boldsymbol{\Sigma}_Y\boldsymbol{\Delta}_M^{-1}\mathbf{K}_{XV}\mathbf{K}_V^{-1} & \mathbf{I} - \boldsymbol{\Sigma}_Y\boldsymbol{\Delta}_M^{-1} \end{bmatrix} \tag{13.187}$$

using this in conjunction with (13.186), we obtain

$$\begin{bmatrix} \mathbf{K}_{XV} & \mathbf{K}_X \end{bmatrix} \mathbf{M}^{-1} \begin{bmatrix} \mathbf{K}_{XV} & \mathbf{K}_X \end{bmatrix}^\top = \mathbf{K}_X - \boldsymbol{\Sigma}_Y + \boldsymbol{\Sigma}_Y\boldsymbol{\Delta}_M^{-1}\boldsymbol{\Sigma}_Y \tag{13.188}$$

Using (13.188) in (13.181), we have

$$\mathbf{K}_{X|VY} = \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y \mathbf{\Delta}_M^{-1} \mathbf{\Sigma}_Y \tag{13.189}$$

$$= \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y (\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y)^{-1} \mathbf{\Sigma}_Y \tag{13.190}$$

where (13.190) follows from (13.186). Thus, using (13.190), the constraint $\mathbf{K}_{X|VY} \preceq \mathbf{D}$ can be expressed as follows

$$\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y (\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y)^{-1} \mathbf{\Sigma}_Y \preceq \mathbf{D} \tag{13.191}$$

from which, since $\mathbf{\Sigma}_Y - \mathbf{D} \succ \mathbf{0}$, the following order can be obtained

$$\mathbf{K}_{X|V} \preceq \mathbf{\Sigma}_Y (\mathbf{\Sigma}_Y - \mathbf{D})^{-1} \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y = \mathbf{F}(\mathbf{D}) \tag{13.192}$$

which completes the proof of Lemma 13.3.

13.7.7 Conditioning Reduces MMSE

Here, we prove that conditioning reduces MMSE. To this end, we introduce the following lemma.

Lemma 13.13 *Let* $\mathbf{U}$ *and* $\mathbf{V}$ *be any two* n*-dimensional random vectors and* $g : \mathbb{R}^n \to \mathbb{R}^n$*. Then,*

$$E\left[g(\mathbf{V}) g^\top(\mathbf{V}) | \mathbf{U} = \mathbf{u}\right] \succeq E\left[g(\mathbf{V}) | \mathbf{U} = \mathbf{u}\right] E\left[g^\top(\mathbf{V}) | \mathbf{U} = \mathbf{u}\right] \tag{13.193}$$

Proof: The proof of this lemma comes from the following fact

$$\mathbf{0} \preceq E\left[\left(g(\mathbf{V}) - E\left[g(\mathbf{V})|\mathbf{U}=\mathbf{u}\right]\right)\left(g(\mathbf{V}) - E\left[g(\mathbf{V})|\mathbf{U}=\mathbf{u}\right]\right)^{\top}|\mathbf{U}=\mathbf{u}\right] \tag{13.194}$$

$$= E\left[g(\mathbf{V})g^{\top}(\mathbf{V})|\mathbf{U}=\mathbf{u}\right] - E\left[g(\mathbf{V})|\mathbf{U}=\mathbf{u}\right]E\left[g^{\top}(\mathbf{V})|\mathbf{U}=\mathbf{u}\right] \tag{13.195}$$

□

We now prove the fact that conditioning reduces MMSE.

Lemma 13.14 *If* $U \rightarrow V \rightarrow \mathbf{X}$*, then* $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$*.*

Proof: We have

$$\mathbf{K}_{X|V} = E\left[\mathbf{X}\mathbf{X}^{\top}\right] - E\left[E\left[\mathbf{X}|\mathbf{V}\right]E\left[\mathbf{X}^{\top}|\mathbf{V}\right]\right] \tag{13.196}$$

$$= E\left[\mathbf{X}\mathbf{X}^{\top}\right] - E\left[E\left[E\left[\mathbf{X}|\mathbf{V}\right]E\left[\mathbf{X}^{\top}|\mathbf{V}\right]|\mathbf{U}\right]\right] \tag{13.197}$$

$$\preceq E\left[\mathbf{X}\mathbf{X}^{\top}\right] - E\left[E\left[E\left[\mathbf{X}|\mathbf{V}\right]|\mathbf{U}\right]E\left[E\left[\mathbf{X}^{\top}|\mathbf{V}\right]|\mathbf{U}\right]\right] \tag{13.198}$$

$$= E\left[\mathbf{X}\mathbf{X}^{\top}\right] - E\left[E\left[\mathbf{X}|\mathbf{U}\right]E\left[\mathbf{X}^{\top}|\mathbf{U}\right]\right] \tag{13.199}$$

where (13.198) comes from Lemma 13.13 and (13.199) comes from the following fact

$$E\left[E\left[\mathbf{X}|\mathbf{V}\right]|\mathbf{U}\right] = E\left[\mathbf{X}|\mathbf{U}\right] \tag{13.200}$$

which is a consequence of the Markov chain $U \rightarrow V \rightarrow \mathbf{X}$. □

13.7.8 Proof of Lemma 13.4

We now prove Lemma 13.4. Since any jointly Gaussian $(U, V, \mathbf{X})$ triple satisfying the Markov chain $U \to V \to \mathbf{X}$ also satisfies $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$ due to Lemma 13.14, the feasible set of $\bar{L}^G$ already contains all jointly Gaussian (U, V) pairs satisfying the Markov chain $U \to V \to \mathbf{X}$. Hence, we have $L^G \geq \bar{L}^G$. Next, we show that $\bar{L}^G \geq L^G$ to complete the proof of Lemma 13.4. To do so, we need to show that for any jointly Gaussian $(U, V, \mathbf{X})$ with conditional covariance matrices $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ satisfying $\mathbf{0} \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X$ and $\mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})$, there exists another jointly Gaussian (U^G, V^G) pair such that this pair has the following properties

- $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$
- $\mathbf{K}_{X|U^G} = \mathbf{K}_{X|U}$
- $U^G \to V^G \to \mathbf{X}$

To this end, we note that (U^G, V^G) can be represented as

$$V^G = \mathbf{A}_V \mathbf{X} + \mathbf{N}_V \tag{13.201}$$

$$U^G = \mathbf{A}_U \mathbf{X} + \mathbf{N}_U \tag{13.202}$$

where $(\mathbf{N}_U, \mathbf{N}_V)$ and $\mathbf{X}$ are independent, $\mathbf{N}_U, \mathbf{N}_V$ are zero-mean Gaussian random vectors with identity covariance matrices. The cross covariance of $\mathbf{N}_U$ and $\mathbf{N}_V$ is given by $\mathbf{\Sigma}_{UV} = E\left[\mathbf{N}_U \mathbf{N}_V^\top\right]$, which needs to be selected accordingly to ensure that $U^G \to V^G \to \mathbf{X}$.

The conditional covariance $\mathbf{K}_{X|V^G}$ is given by [114, page 155]

$$\mathbf{K}_{X|V^G} = \mathbf{K}_X - \mathbf{K}_{XV^G}\mathbf{K}_{V^G}^{-1}\mathbf{K}_{V^GX} \tag{13.203}$$

Since we are seeking a V^G such that $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$, we set $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$ in (13.203) yielding

$$\mathbf{K}_{X|V} = \mathbf{K}_X - \mathbf{K}_{XV^G}\mathbf{K}_{V^G}^{-1}\mathbf{K}_{V^GX} \tag{13.204}$$

$$= \mathbf{K}_X - \mathbf{K}_X\mathbf{A}_V^\top(\mathbf{A}_V\mathbf{K}_X\mathbf{A}_V^\top + \mathbf{I})^{-1}\mathbf{A}_V\mathbf{K}_X \tag{13.205}$$

which is equivalent to

$$\mathbf{K}_X^{-1}(\mathbf{K}_X - \mathbf{K}_{X|V})\mathbf{K}_X^{-1} = \mathbf{A}_V^\top(\mathbf{A}_V\mathbf{K}_X\mathbf{A}_V^\top + \mathbf{I})^{-1}\mathbf{A}_V \tag{13.206}$$

Next, we note the Woodbury matrix identity [53].

Lemma 13.15 ([53, page 17])

$$\left(\mathbf{A} + \mathbf{CBC}^\top\right)^{-1} = \mathbf{A}^{-1} - \mathbf{A}^{-1}\mathbf{C}\left(\mathbf{B}^{-1} + \mathbf{C}^\top\mathbf{A}^{-1}\mathbf{C}\right)^{-1}\mathbf{C}^\top\mathbf{A}^{-1} \tag{13.207}$$

Using Woodbury matrix identity, we get

$$\left(\mathbf{A}_V\mathbf{K}_X\mathbf{A}_V^\top + \mathbf{I}\right)^{-1} = \mathbf{I} - \mathbf{A}_V(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V)^{-1}\mathbf{A}_V^\top \tag{13.208}$$

using which in (13.206), we get

$$\mathbf{K}_X^{-1}(\mathbf{K}_X - \mathbf{K}_{X|V})\mathbf{K}_X^{-1} = \mathbf{A}_V^\top \left[\mathbf{I} - \mathbf{A}_V(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V)^{-1}\mathbf{A}_V^\top\right]\mathbf{A}_V \tag{13.209}$$

$$= \mathbf{A}_V^\top\mathbf{A}_V - \mathbf{A}_V^\top\mathbf{A}_V(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V)^{-1}\mathbf{A}_V^\top\mathbf{A}_V \tag{13.210}$$

$$= \mathbf{A}_V^\top\mathbf{A}_V - \mathbf{A}_V^\top\mathbf{A}_V(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V)^{-1}\left(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V - \mathbf{K}_X^{-1}\right) \tag{13.211}$$

$$= \mathbf{A}_V^\top\mathbf{A}_V(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V)^{-1}\mathbf{K}_X^{-1} \tag{13.212}$$

$$= \left(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V - \mathbf{K}_X^{-1}\right)(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V)^{-1}\mathbf{K}_X^{-1} \tag{13.213}$$

$$= \mathbf{K}_X^{-1} - \mathbf{K}_X^{-1}(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V)^{-1}\mathbf{K}_X^{-1} \tag{13.214}$$

which implies

$$\mathbf{K}_{X|V} = \left(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top\mathbf{A}_V\right)^{-1} \tag{13.215}$$

which, in turn, implies

$$\mathbf{A}_V^\top\mathbf{A}_V = \mathbf{K}_{X|V}^{-1} - \mathbf{K}_X^{-1} \tag{13.216}$$

Hence, if we select $\mathbf{A}_V$ as satisfying (13.216), we get $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$. Similarly, if we select $\mathbf{A}_U$ to satisfy

$$\mathbf{A}_U^\top\mathbf{A}_U = \mathbf{K}_{X|U}^{-1} - \mathbf{K}_X^{-1} \tag{13.217}$$

then, we also have $\mathbf{K}_{X|U^G} = \mathbf{K}_{X|U}$.

Next, we will explicitly construct $\mathbf{A}_V$ and $\mathbf{A}_U$ matrices to satisfy (13.216) and (13.217), respectively. To this end, we introduce the following lemma, which will be used subsequently.

Lemma 13.16 ([116]) *Let* $\mathbf{A}, \mathbf{B}$ *be two real symmetric positive semi-definite matrices. Then, there exists a non-singular matrix* $\mathbf{W}$ *such that*

$$\mathbf{A} = \mathbf{W}^\top \mathbf{\Lambda}_A \mathbf{W} \tag{13.218}$$

$$\mathbf{B} = \mathbf{W}^\top \mathbf{\Lambda}_B \mathbf{W} \tag{13.219}$$

$$\tag{13.220}$$

where $\mathbf{\Lambda}_A$ *and* $\mathbf{\Lambda}_B$ *are diagonal matrices.*

Lemma 13.16 states that two real symmetric positive semi-definite matrices can be diagonalized simultaneously. Using this fact in (13.216)-(13.217), we get

$$\mathbf{K}_{X|V}^{-1} - \mathbf{K}_X^{-1} = \mathbf{W}^\top \mathbf{\Lambda}_V^2 \mathbf{W} \tag{13.221}$$

$$\mathbf{K}_{X|U}^{-1} - \mathbf{K}_X^{-1} = \mathbf{W}^\top \mathbf{\Lambda}_U^2 \mathbf{W} \tag{13.222}$$

for some non-singular matrix $\mathbf{W}$, and diagonal matrices $\mathbf{\Lambda}_U, \mathbf{\Lambda}_V$. Since $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$, we have $\mathbf{K}_{X|V}^{-1} \succeq \mathbf{K}_{X|U}^{-1}$, which, in view of (13.221)-(13.222) imply

$$\mathbf{W}^\top \left(\mathbf{\Lambda}_V^2 - \mathbf{\Lambda}_U^2 \right) \mathbf{W} \succeq \mathbf{0} \tag{13.223}$$

Since $\mathbf{W}$ is non-singular, (13.223) implies that

$$\mathbf{\Lambda}_V \succeq \mathbf{\Lambda}_U \tag{13.224}$$

Finally, we choose

$$\mathbf{A}_V = \mathbf{\Lambda}_V \mathbf{W} \tag{13.225}$$

$$\mathbf{A}_U = \mathbf{\Lambda}_U \mathbf{W} \tag{13.226}$$

which, in view of (13.216)-(13.217) and (13.221)-(13.222), imply $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$ and $\mathbf{K}_{X|U^G} = \mathbf{K}_{X|U}$.

Next, we show that a proper selection the cross-covariance matrix $\mathbf{\Sigma}_{UV}$ would yield the desired Markov chain $U^G \to V^G \to \mathbf{X}$. To this end, we introduce the following matrix

$$\mathbf{A}_{UV} = \mathbf{\Lambda}_U \mathbf{\Lambda}_V^\dagger \tag{13.227}$$

where the diagonal matrix $\mathbf{\Lambda}_V^\dagger$ is defined as follows:

$$\Lambda_{V,ii}^\dagger = \begin{cases} \frac{1}{\Lambda_{V,ii}}, & \text{if } \Lambda_{V,ii} \neq 0 \\ 0, & \text{otherwise} \end{cases} \tag{13.228}$$

Since $\mathbf{\Lambda}_U \preceq \mathbf{\Lambda}_V$, we have $\mathbf{\Lambda}_U \mathbf{\Lambda}_V^{\dagger} \mathbf{\Lambda}_V = \mathbf{\Lambda}_U$. Hence, we have

$$\mathbf{A}_{UV} \mathbf{A}_V = \mathbf{A}_U \tag{13.229}$$

We also note the following

$$\mathbf{A}_{UV} \mathbf{A}_{UV}^{\top} = \mathbf{\Lambda}_U \big(\mathbf{\Lambda}_V^{\dagger}\big)^2 \mathbf{\Lambda}_U \preceq \mathbf{I} \tag{13.230}$$

since $\mathbf{\Lambda}_U \preceq \mathbf{\Lambda}_V$.

Now, we are ready to show that U^G and V^G satisfy the Markov chain $U^G \rightarrow V^G \rightarrow \mathbf{X}$ by specifying $\mathbf{\Sigma}_{UV}$. We set $\mathbf{N}_U$ as follows

$$\mathbf{N}_U = \mathbf{A}_{UV} \mathbf{N}_V + \tilde{\mathbf{N}} \tag{13.231}$$

where $\tilde{\mathbf{N}}$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{I} - \mathbf{A}_{UV} \mathbf{A}_{UV}^{\top}$, and is independent of $\mathbf{N}_V$. In view of (13.231), we have

$$\begin{aligned} U^G &= \mathbf{A}_U \mathbf{X} + \mathbf{N}_U && (13.232) \\ &= \mathbf{A}_{UV} \mathbf{A}_V \mathbf{X} + \mathbf{A}_{UV} \mathbf{N}_V + \tilde{\mathbf{N}} && (13.233) \\ &= \mathbf{A}_{UV} V^G + \tilde{\mathbf{N}} && (13.234) \end{aligned}$$

which implies that (U^G, V^G) satisfy the Markov chain $U^G \rightarrow V^G \rightarrow \mathbf{X}$; completing the proof.

13.7.9 Proof of Lemma 13.5

The Lagrangian for the optimization problem $\bar{L}^G$ is given as follows

$$\begin{aligned}\mathcal{L}\left(\bar{L}^G\right) = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_{X|U}+\mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V}+\mathbf{\Sigma}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_{X|U}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} - \mathrm{tr}(\mathbf{M}_0\mathbf{K}_{X|V}) \\ - \mathrm{tr}(\mathbf{M}_U(\mathbf{K}_{X|U}-\mathbf{K}_{X|V})) - \mathrm{tr}(\mathbf{M}_X(\mathbf{K}_X-\mathbf{K}_{X|U})) \\ - \mathrm{tr}(\mathbf{M}_D(\mathbf{F}(\mathbf{D})-\mathbf{K}_{X|V})) \qquad (13.235)\end{aligned}$$

where the positive semi-definite matrices $\mathbf{M}_0, \mathbf{M}_U, \mathbf{M}_D, \mathbf{M}_X$ are the Lagrange multipliers for the following constraints

$$\mathbf{K}_{X|V} \succeq \mathbf{0} \qquad (13.236)$$

$$\mathbf{K}_{X|U} - \mathbf{K}_{X|V} \succeq \mathbf{0} \qquad (13.237)$$

$$\mathbf{F}(\mathbf{D}) - \mathbf{K}_{X|V} \succeq \mathbf{0} \qquad (13.238)$$

$$\mathbf{K}_X - \mathbf{K}_{X|U} \succeq \mathbf{0} \qquad (13.239)$$

respectively. Let $\mathbf{K}^*_{X|V}$ and $\mathbf{K}^*_{X|U}$ be the minimizers of the optimization problem $\bar{L}^G$. Using (13.235), the KKT conditions can be found as follows.

$$\nabla_{\mathbf{K}_{X|V}}\mathcal{L}(\bar{L}^G)\mid_{\mathbf{K}_{X|V}=\mathbf{K}^*_{X|V}} = \mathbf{0} \qquad (13.240)$$

$$\nabla_{\mathbf{K}_{X|U}}\mathcal{L}(\bar{L}^G)\mid_{\mathbf{K}_{X|U}=\mathbf{K}^*_{X|U}} = \mathbf{0} \qquad (13.241)$$

$$\mathrm{tr}(\mathbf{M}_0\mathbf{K}^*_{X|V}) = 0 \qquad (13.242)$$

$$\mathrm{tr}(\mathbf{M}_U(\mathbf{K}^*_{X|U}-\mathbf{K}^*_{X|V})) = 0 \qquad (13.243)$$

$$\mathrm{tr}(\mathbf{M}_D(\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V})) = 0 \tag{13.244}$$

$$\mathrm{tr}(\mathbf{M}_X(\mathbf{K}_X - \mathbf{K}^*_{X|U})) = 0 \tag{13.245}$$

We first note that we have $\mathbf{K}^*_{X|V} \succ \mathbf{0}$, otherwise $\bar{L}^G \to \infty$. Hence, using the fact that if $\mathbf{A} \succeq \mathbf{0}, \mathbf{B} \succeq \mathbf{0}$, $\mathrm{tr}(\mathbf{AB}) \geq 0$, and (13.242), we get $\mathbf{M}_0 = \mathbf{0}$. Next, using the fact that $\mathbf{M}_0 = \mathbf{0}$ in (13.240), we get the KKT condition given in (13.81). Equation (13.241) implies (13.82). Finally, using the fact that $\mathbf{A} \succeq \mathbf{0}, \mathbf{B} \succeq \mathbf{0}$, $\mathrm{tr}(\mathbf{AB}) = \mathrm{tr}(\mathbf{BA}) \geq 0$ in (13.243)-(13.245), we can get the KKT conditions given in (13.83)-(13.85), respectively.

13.7.10 Proof of Lemma 13.6

We start with the second statement of the lemma. To this end, we note that (13.82) and (13.86) imply the following.

$$(\mathbf{K}^*_{X|U} + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U \tag{13.246}$$

$$= (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_X \tag{13.247}$$

Next, using the fact that if $\mathbf{A} \succ \mathbf{0}, \mathbf{B} \succ \mathbf{0}$ and $\mathbf{A} \succeq \mathbf{B}$, we have $\mathbf{A}^{-1} \preceq \mathbf{B}^{-1}$ in conjunction with the fact that $\mathbf{M}_U \succeq \mathbf{0}, \mathbf{M}_X \succeq \mathbf{0}$, we can obtain the second statement of the lemma from (13.246)-(13.247).

Next, we consider the third statement of the lemma as follows

$$\mathbf{K}^*_{X|V} + \tilde{\mathbf{\Sigma}}_Y = \mathbf{K}^*_{X|V} + \left[(\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} - \mathbf{K}^*_{X|U} \tag{13.248}$$

$$= \mathbf{K}^*_{X|V} + \left[\mathbf{I} + (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y)\mathbf{M}_U\right]^{-1} (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y) - \mathbf{K}^*_{X|U} \tag{13.249}$$

$$= \mathbf{K}^*_{X|V} + \left[\mathbf{I} + (\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V} + \mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)\mathbf{M}_U\right]^{-1} (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y) - \mathbf{K}^*_{X|U} \tag{13.250}$$

$$= \mathbf{K}^*_{X|V} + \left[\mathbf{I} + (\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)\mathbf{M}_U\right]^{-1} (\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y) - \mathbf{K}^*_{X|U} \tag{13.251}$$

$$= \mathbf{K}^*_{X|V} + \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} (\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1}(\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y) - \mathbf{K}^*_{X|U} \tag{13.252}$$

$$= \mathbf{K}^*_{X|V} + \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} (\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1}(\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V}) + \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} - \mathbf{K}^*_{X|U} \tag{13.253}$$

$$= \mathbf{K}^*_{X|V} + \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right] (\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V}) + \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} - \mathbf{K}^*_{X|U} \tag{13.254}$$

$$= \mathbf{K}^*_{X|V} + (\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V}) + \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} - \mathbf{K}^*_{X|U} \tag{13.255}$$

$$= \left[(\mathbf{K}^*_{X|V} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} \tag{13.256}$$

where (13.248) comes from (13.246), (13.251) and (13.254) follow from (13.83).

Now, we consider the fourth statement of the lemma as follows

$$(\mathbf{K}^*_{X|U} + \tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{K}^*_{X|V} + \tilde{\mathbf{\Sigma}}_Y) = \mathbf{I} + (\mathbf{K}^*_{X|U} + \tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{K}^*_{X|V} - \mathbf{K}^*_{X|U}) \tag{13.257}$$

$$= \mathbf{I} + \left[(\mathbf{K}^*_{X|U} + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right] (\mathbf{K}^*_{X|V} - \mathbf{K}^*_{X|U}) \tag{13.258}$$

$$= \mathbf{I} + (\mathbf{K}^*_{X|U} + \boldsymbol{\Sigma}_Y)^{-1}(\mathbf{K}^*_{X|V} - \mathbf{K}^*_{X|U}) \tag{13.259}$$

$$= (\mathbf{K}^*_{X|U} + \boldsymbol{\Sigma}_Y)^{-1}(\mathbf{K}^*_{X|V} + \boldsymbol{\Sigma}_Y) \tag{13.260}$$

where (13.258) follows from (13.246), and (13.259) comes from (13.83).

Next, we consider the fifth statement of the lemma as follows

$$(\mathbf{K}^*_{X|U} + \tilde{\boldsymbol{\Sigma}}_Y)^{-1}(\mathbf{K}_X + \tilde{\boldsymbol{\Sigma}}_Y) = \mathbf{I} + (\mathbf{K}^*_{X|U} + \tilde{\boldsymbol{\Sigma}}_Y)^{-1}(\mathbf{K}_X - \mathbf{K}^*_{X|U}) \tag{13.261}$$

$$= \mathbf{I} + \left[(\mathbf{K}^*_{X|U} + \boldsymbol{\Sigma}_Z)^{-1} + \mathbf{M}_X\right](\mathbf{K}_X - \mathbf{K}^*_{X|U}) \tag{13.262}$$

$$= \mathbf{I} + (\mathbf{K}^*_{X|U} + \boldsymbol{\Sigma}_Z)^{-1}(\mathbf{K}_X - \mathbf{K}^*_{X|U}) \tag{13.263}$$

$$= (\mathbf{K}^*_{X|U} + \boldsymbol{\Sigma}_Z)^{-1}(\mathbf{K}_X + \boldsymbol{\Sigma}_Z) \tag{13.264}$$

where (13.262) comes from (13.247), and (13.263) is due to (13.85).

Now, we prove the last statement of the lemma. To this end, we note that the third statement of this lemma and (13.81) imply the following

$$(\mathbf{K}^*_{X|V} + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} + \mathbf{M}_D = (\mathbf{K}^*_{X|V})^{-1} \tag{13.265}$$

which will be used in the sequel. Now, the last statement of this lemma follows from

$$(\mathbf{K}^*_{X|V} + \tilde{\boldsymbol{\Sigma}}_Y)^{-1}(\mathbf{F}(\mathbf{D}) + \tilde{\boldsymbol{\Sigma}}_Y) = \mathbf{I} + (\mathbf{K}^*_{X|V} + \tilde{\boldsymbol{\Sigma}}_Y)^{-1}(\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V}) \tag{13.266}$$

$$= \mathbf{I} + \left[(\mathbf{K}^*_{X|V})^{-1} - \mathbf{M}_D\right](\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V}) \tag{13.267}$$

$$= \mathbf{I} + (\mathbf{K}^*_{X|V})^{-1}(\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V}) \tag{13.268}$$

$$= (\mathbf{K}^*_{X|V})^{-1}\mathbf{F}(\mathbf{D}) \tag{13.269}$$

where (13.267) comes from (13.265), and (13.268) is due to (13.84).

Finally, we note that (13.265) also implies the first statement of the lemma; completing the proof.

13.7.11 Proof of Lemma 13.7

We first consider the cost function of the optimization problem $\bar{L}$

$$C(\bar{L}) = I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}|U) + I(\mathbf{X};\mathbf{Z}|U) \tag{13.270}$$

$$= I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(U;\tilde{\mathbf{Y}}) + I(\mathbf{X};\mathbf{Z}) - I(U;\mathbf{Z}) \tag{13.271}$$

$$= I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(U;\tilde{\mathbf{Y}},\mathbf{Z}) + I(\mathbf{X};\mathbf{Z}) - I(U;\mathbf{Z}) \tag{13.272}$$

$$= I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(U;\tilde{\mathbf{Y}}|\mathbf{Z}) + I(\mathbf{X};\mathbf{Z}) \tag{13.273}$$

$$\geq I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(\mathbf{X};\mathbf{Z}) \tag{13.274}$$

where (13.271)-(13.272) come from the following Markov chain

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y},\mathbf{Z} \tag{13.275}$$

and (13.274) comes from the non-negativity of the mutual information. On the other hand, (13.274) can be obtained from (13.89) by choosing $U = \phi$, i.e., we have

$$\bar{L} \leq \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(\mathbf{X};\mathbf{Z}) \tag{13.276}$$

Hence, (13.274) and (13.276) imply the following

$$\bar{L} = \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(\mathbf{X};\mathbf{Z}) \tag{13.277}$$

$$= \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V;\mathbf{X}|\tilde{\mathbf{Y}}) + I(\mathbf{X};\mathbf{Z}) \tag{13.278}$$

where (13.278) comes from the Markov chain $V \to \mathbf{X} \to \tilde{\mathbf{Y}}$. We note that the optimization problem in (13.278) is similar to the one we already studied in (13.65)-(13.69). Indeed, if the constraint $\mathbf{K}_{X|VY} \preceq \mathbf{D}$ in (13.278) was $\mathbf{K}_{X|V\tilde{Y}} \preceq \mathbf{D}$, both optimization problems would be identical, and using the analysis in (13.65)-(13.69), we could conclude that (13.278) is minimized by a Gaussian V satisfying $\mathbf{K}_{X|V\tilde{Y}} \preceq \mathbf{D}$. However, the difference between these two constraints necessitates a new proof, and indeed, showing the optimality of Gaussian V for the optimization problem in (13.278) is not as straightforward as showing the optimality of Gaussian V for the optimization problem in (13.65).

We find the minimizer for the optimization problem $\bar{L}$ in two steps. In the first step, for a given feasible V, we explicitly construct a feasible Gaussian $\bar{V}$ which provides the same value for the cost function of $\bar{L}$ as the original V does. Thus, this

first step implies that restricting V to be Gaussian does not change the optimum value of the optimization problem $\bar{L}$. Consequently, in the second step of the proof, we minimize $\bar{L}$ over all feasible Gaussian V. To this end, we note that the cost function of the optimization problem $\bar{L}$ can be written as

$$C(\bar{L}) = h(\tilde{\mathbf{Y}}|V) - h(\mathbf{X}|V) + c \tag{13.279}$$

for some constant c, which is independent of V. From now on, we focus on the difference of the two differential entropy terms in (13.279). Next, we note that using Lemma 5.17, we have

$$h(\tilde{\mathbf{Y}}|V) - h(\mathbf{X}|V) = \frac{1}{2}\int_{\mathbf{0}}^{\tilde{\mathbf{\Sigma}}_Y} \mathbf{J}(\mathbf{X}+\mathbf{N}|V)d\mathbf{\Sigma}_N \tag{13.280}$$

where $\mathbf{N}$ is zero-mean Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N$ satisfying $\mathbf{0} \preceq \mathbf{\Sigma}_N$. Next, we find upper and lower bounds for (13.280). We note that Lemma 5.16 implies the following upper bound for $\mathbf{J}(\mathbf{X}+\mathbf{N}|V)$

$$\mathbf{J}(\mathbf{X}+\mathbf{N}|V) \preceq \left[\mathbf{J}^{-1}(\mathbf{X}|V) + \mathbf{\Sigma}_N\right]^{-1} \tag{13.281}$$

Using (13.281) in (13.280) in conjunction with Lemma 5.8, we get

$$h(\tilde{\mathbf{Y}}|V) - h(\mathbf{X}|V) \leq \frac{1}{2}\log\frac{|\mathbf{J}^{-1}(\mathbf{X}|V) + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{J}^{-1}(\mathbf{X}|V)|} \tag{13.282}$$

We note that due to Lemma 5.13, we have $\mathbf{J}(\mathbf{X}|V) \succeq \mathbf{K}_{X|V}^{-1} \succ \mathbf{0}$, i.e., (13.282) is

well-defined. Similarly, using Lemma 5.16, we have

$$\mathbf{J}^{-1}(\mathbf{X}+\tilde{\mathbf{N}}_Y|V)-\tilde{\mathbf{\Sigma}}_Y \succeq \mathbf{J}^{-1}(\mathbf{X}+\mathbf{N}|V)-\mathbf{\Sigma}_N, \quad \mathbf{\Sigma}_N \preceq \tilde{\mathbf{\Sigma}}_Y \tag{13.283}$$

which implies

$$\mathbf{J}(\mathbf{X}+\mathbf{N}|V) \succeq \left[\mathbf{J}^{-1}(\mathbf{X}+\tilde{\mathbf{N}}_Y|V)-\tilde{\mathbf{\Sigma}}_Y+\mathbf{\Sigma}_N\right]^{-1} \tag{13.284}$$

Using (13.284) in (13.280) in conjunction with Lemma 5.8, we get

$$h(\tilde{\mathbf{Y}}|V)-h(\mathbf{X}|V) \geq \frac{1}{2}\log\frac{|\mathbf{J}^{-1}(\mathbf{X}+\tilde{\mathbf{N}}_Y|V)|}{|\mathbf{J}^{-1}(\mathbf{X}+\tilde{\mathbf{N}}_Y|V)-\tilde{\mathbf{\Sigma}}_Y|} \tag{13.285}$$

Now, we rewrite the bounds in (13.282) and (13.285). To this end, we define the following function

$$f(t)=\frac{1}{2}\log\frac{|\mathbf{K}(t)+\tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}(t)|}, \quad 0 \leq t \leq 1 \tag{13.286}$$

where the matrix $\mathbf{K}(t)$ is given as follows

$$\mathbf{K}(t)=t\mathbf{J}^{-1}(\mathbf{X}|V)+(1-t)\left[\mathbf{J}^{-1}(\mathbf{X}+\tilde{\mathbf{N}}_Y|V)-\tilde{\mathbf{\Sigma}}_Y\right] \tag{13.287}$$

Hence, using $f(t)$ in (13.286), the bounds in (13.282) and (13.285) can be rewritten

as follows:

$$f(0) \leq h(\tilde{\mathbf{Y}}|V) - h(\mathbf{X}|V) \leq f(1) \tag{13.288}$$

Since $f(t)$ is continuous in t, there exists t^* such that

$$f(t^*) = h(\tilde{\mathbf{Y}}|V) - h(\mathbf{X}|V) \tag{13.289}$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}(t^*) + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}(t^*)|} \tag{13.290}$$

where $\mathbf{K}(t^*)$ is bounded as follows

$$\mathbf{J}^{-1}(\mathbf{X}|V) \preceq \mathbf{K}(t^*) \preceq \mathbf{J}^{-1}(\mathbf{X} + \tilde{\mathbf{N}}_Y|V) - \tilde{\mathbf{\Sigma}}_Y \tag{13.291}$$

$$\preceq \mathbf{J}^{-1}(\mathbf{X} + \mathbf{N}_Y|V) - \mathbf{\Sigma}_Y \tag{13.292}$$

where we used the fact that $0 \leq t^* \leq 1$ and Lemma 5.16. Thus, (13.290) implies that if we pick a Gaussian $\bar{V}$ satisfying $\mathbf{K}_{X|\bar{V}} = \mathbf{K}(t^*)$, it provides the same value for the cost function of $\bar{L}$ as the original V does.

Next, we check whether this Gaussian $\bar{V}$ is feasible, i.e., whether it satisfies $\mathbf{K}_{X|\bar{V}Y} \preceq \mathbf{D}$. To this end, using Lemma 5.21, we get

$$\mathbf{K}_{X|\bar{V}Y} = \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y \mathbf{J}(\mathbf{Y}|\bar{V}) \mathbf{\Sigma}_Y \tag{13.293}$$

Since $\bar{V}$ is Gaussian, Lemma 5.13 implies that

$$\mathbf{J}(\mathbf{Y}|\bar{V}) = \mathbf{K}_{Y|\bar{V}}^{-1} \tag{13.294}$$

$$= (\mathbf{K}_{X|\bar{V}} + \mathbf{\Sigma}_Y)^{-1} \tag{13.295}$$

where (13.295) follows from the fact that $(\bar{V}, \mathbf{X})$ and $\mathbf{N}_Y$ are independent. Moreover, due to (13.292), we have $\mathbf{K}_{X|\bar{V}} \preceq \mathbf{J}^{-1}(\mathbf{Y}|V) - \mathbf{\Sigma}_Y$, which together with (13.295) imply the following

$$\mathbf{J}(\mathbf{Y}|\bar{V}) \succeq \mathbf{J}(\mathbf{Y}|V) \tag{13.296}$$

Using (13.296) in (13.293), we get

$$\mathbf{K}_{X|\bar{V}Y} \preceq \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y \mathbf{J}(\mathbf{Y}|V) \mathbf{\Sigma}_Y \tag{13.297}$$

$$= \mathbf{K}_{X|VY} \tag{13.298}$$

$$\preceq \mathbf{D} \tag{13.299}$$

where (13.298) follows from Lemma 5.21 and (13.299) is due to the assumption that V is feasible, i.e., $\mathbf{K}_{X|VY} \preceq \mathbf{D}$. Equation (13.299) implies that the constructed Gaussian random vector $\bar{V}$ is feasible, i.e., for each feasible V, there exists a feasible Gaussian $\bar{V}$ which provides the same value for the cost function of $\bar{L}$; completing the first step of the proof.

Hence, in view of this first step of the proof, we can restrict V to be Gaussian

which leads to the following form for $\bar{L}$:

$$\bar{L} = \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ V \text{ is Gaussian} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(\mathbf{X};\mathbf{Z}) \tag{13.300}$$

$$= \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ V \text{ is Gaussian} \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}) + I(\mathbf{X};\mathbf{Z}) \tag{13.301}$$

$$= \min_{\mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}_{X|V} + \tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.302}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D}) + \tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{13.303}$$

where (13.301) follows from Lemma 13.3, and (13.303) comes from the fact that

$$\frac{|\mathbf{K}_{X|V} + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}_{X|V}|} \tag{13.304}$$

is monotonically decreasing in the positive semi-definite matrices $\mathbf{K}_{X|V}$; completing the proof of Lemma 13.7.

13.7.12 Proof of Lemma 13.8

We note that due to Theorem 13.3, we already have single-letter descriptions for the regions $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$. Thus, to prove Lemma 13.8, it suffices to show that for any given feasible (U, V), these two regions satisfy the relationship given in Lemma 13.8. We first note the following Markov chains

$$U \to V \to \mathbf{X} \to \bar{\bar{\mathbf{Y}}}_\alpha \to \mathbf{Y} \tag{13.305}$$

$$U \to V \to \mathbf{X} \to \bar{\bar{\mathbf{Z}}}_\alpha \to \mathbf{Z} \tag{13.306}$$

Next, we show that any feasible (U, V) for the region $\mathcal{R}_o(\mathbf{D})$ is also feasible for the region $\lim_{\alpha\to 0} \mathcal{R}_\alpha(\mathbf{D})$. To this end, we note that

$$\mathbf{D} \succeq \mathbf{K}_{X|VY} \tag{13.307}$$

$$\succeq \mathbf{K}_{X|VY\bar{\bar{Y}}_\alpha} \tag{13.308}$$

$$= \mathbf{K}_{X|V\bar{\bar{Y}}_\alpha} \tag{13.309}$$

where (13.308) is due to the fact that conditioning reduces MMSE and (13.309) follows from the Markov chain in (13.305). It can be shown that $\lim_{\alpha\to 0} \mathbf{K}_{X|V\bar{\bar{Y}}_\alpha}$ exists and is equal to $\mathbf{K}_{X|VY}$. Hence, this observation and (13.309) imply that (U, V) is also feasible for the region $\lim_{\alpha\to 0} \mathcal{R}_\alpha(\mathbf{D})$.

Next, we show that for a given (U, V), any rate inside the region $\mathcal{R}_o(\mathbf{D})$ is also inside $\lim_{\alpha\to 0} \mathcal{R}_\alpha(\mathbf{D})$. To this end, for a given (U, V), we denote the minimum achievable rates in $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$ by R_o and R_α, respectively. Due to Theorem 13.3, we have

$$R_o - R_\alpha = [I(V;\mathbf{X}) - I(V;\mathbf{Y})] - [I(V;\mathbf{X}) - I(V;\bar{\bar{\mathbf{Y}}}_\alpha)] \tag{13.310}$$

$$= I(V;\bar{\bar{\mathbf{Y}}}_\alpha) - I(V;\mathbf{Y}) \tag{13.311}$$

$$= I(V;\bar{\bar{\mathbf{Y}}}_\alpha|\mathbf{Y}) \tag{13.312}$$

$$\geq 0 \tag{13.313}$$

where (13.312) comes from the Markov chain in (13.305). Equation (13.312) implies that any achievable rate within the region $\mathcal{R}_o(\mathbf{D})$ is also included in the region $\lim_{\alpha\to 0}\mathcal{R}_\alpha(\mathbf{D})$.

Finally, we show that for a given (U,V), any achievable information leakage inside the region $\mathcal{R}_o(\mathbf{D})$ is also inside $\lim_{\alpha\to 0}\mathcal{R}_\alpha(\mathbf{D})$. To this end, for a given (U,V), we denote the minimum information leakage in $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$ by $I_{e,o}$ and $I_{e,\alpha}$, respectively. Due to Theorem 13.3, we have

$$
\begin{aligned}
&I_{e,o}-I_{e,\alpha}\\
&=[I(V;\mathbf{X})-I(V;\mathbf{Y}|U)+I(\mathbf{X};\mathbf{Z}|U)]-\left[I(V;\mathbf{X})-I(V;\bar{\bar{\mathbf{Y}}}_\alpha|U)+I(\mathbf{X};\bar{\bar{\mathbf{Z}}}_\alpha|U)\right] && (13.314)\\
&=\left[I(V;\bar{\bar{\mathbf{Y}}}_\alpha|U)-I(V;\mathbf{Y}|U)\right]+\left[I(\mathbf{X};\mathbf{Z}|U)-I(\mathbf{X};\bar{\bar{\mathbf{Z}}}_\alpha|U)\right] && (13.315)\\
&=I(V;\bar{\bar{\mathbf{Y}}}_\alpha|U,\mathbf{Y})+\left[I(\mathbf{X};\mathbf{Z}|U)-I(\mathbf{X};\bar{\bar{\mathbf{Z}}}_\alpha|U)\right] && (13.316)\\
&\geq I(\mathbf{X};\mathbf{Z}|U)-I(\mathbf{X};\bar{\bar{\mathbf{Z}}}_\alpha|U) && (13.317)\\
&\geq I(\mathbf{X};\mathbf{Z})-I(\mathbf{X};\bar{\bar{\mathbf{Z}}}_\alpha) && (13.318)\\
&=\frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_X\mathbf{H}_Z^\top+\mathbf{I}|-\frac{1}{2}\log\frac{|\mathbf{K}_X+\mathbf{R}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})^{-2}\mathbf{R}_Z^\top|}{|\mathbf{R}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})^{-2}\mathbf{R}_Z^\top|} && (13.319)\\
&=\frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_X\mathbf{H}_Z^\top+\mathbf{I}|\\
&\quad-\frac{1}{2}\log\frac{|\mathbf{K}_X+\mathbf{R}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})^{-1}\mathbf{Q}_Z^\top\mathbf{Q}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})^{-1}\mathbf{R}_Z^\top|}{|\mathbf{R}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})^{-1}\mathbf{Q}_Z^\top\mathbf{Q}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})^{-1}\mathbf{R}_Z^\top|} && (13.320)\\
&=\frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_X\mathbf{H}_Z^\top+\mathbf{I}|-\frac{1}{2}\log|\mathbf{Q}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})\mathbf{R}_Z^\top\mathbf{K}_X\mathbf{R}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})\mathbf{Q}_Z^\top+\mathbf{I}| && (13.321)
\end{aligned}
$$

where (13.316) comes from the Markov chain in (13.305) and (13.318) follows from

the Markov chain in (13.306). Equation (13.321) implies that

$$\lim_{\alpha\to 0} I_{e,o} - I_{e,\alpha}$$
$$\geq \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_X\mathbf{H}_Z^\top + \mathbf{I}| - \lim_{\alpha\to 0}\frac{1}{2}\log|\mathbf{Q}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})\mathbf{R}_Z^\top\mathbf{K}_X\mathbf{R}_Z(\mathbf{\Lambda}_Z+\alpha\mathbf{I})\mathbf{Q}_Z^\top + \mathbf{I}| \tag{13.322}$$
$$= \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_X\mathbf{H}_Z^\top + \mathbf{I}| - \frac{1}{2}\log|\mathbf{Q}_Z\mathbf{\Lambda}_Z\mathbf{R}_Z^\top\mathbf{K}_X\mathbf{R}_Z\mathbf{\Lambda}_Z\mathbf{Q}_Z^\top + \mathbf{I}| \tag{13.323}$$
$$= \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_X\mathbf{H}_Z^\top + \mathbf{I}| - \frac{1}{2}\log|\mathbf{H}_Z\mathbf{K}_X\mathbf{H}_Z^\top + \mathbf{I}| \tag{13.324}$$
$$= 0 \tag{13.325}$$

where (13.323) comes from the continuity of the determinant in positive semi-definite matrices. Equation (13.325) implies that any achievable information leakage in the region $\mathcal{R}_o(\mathbf{D})$ is also inside the region $\lim_{\alpha\to 0}\mathcal{R}_\alpha(\mathbf{D})$; completing the proof of Lemma 13.8.

13.7.13 Proof of Theorem 13.6

We start the proof of Theorem 13.6 by first expressing Theorem 13.4 for the side information model given by (13.103)-(13.104). In other words, we first provide an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$ by using Theorem 13.4. To this end, to be able to use Theorem 13.4, we need $\mathbf{D} \preceq \mathbf{K}_{X|\bar{\mathbf{Y}}_\alpha}$. However, since we originally have $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ and $\mathbf{K}_{X|\bar{\mathbf{Y}}_\alpha} \preceq \mathbf{K}_{X|Y}$, where the latter one follows from the Markov chain $\mathbf{X} \to \bar{\mathbf{Y}}_\alpha \to \mathbf{Y}$ and the fact that conditioning reduces MMSE, $\mathbf{K}_{X|\bar{\mathbf{Y}}_\alpha} - \mathbf{D}$ might be indefinite. However, the only place we use the condition $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ is to be able

to show the equivalence between $\mathbf{K}_{X|VY} \preceq \mathbf{D}$ and $\mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})$ for Gaussian V in Lemma 13.3. In particular, we only need the fact that $\mathbf{\Sigma}_Y - \mathbf{D}$ is non-singular to show this equivalence, and which is implied by $\mathbf{D} \preceq \mathbf{K}_{X|Y}$. However, still there might be distortion matrices $\mathbf{D}$ for which although we have non-singular $\mathbf{\Sigma}_Y - \mathbf{D}$, the condition $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ is not satisfied. Hence, if we can find an α^* such that

$$\mathbf{\Sigma}_{Y,\alpha} - \mathbf{D} \succ \mathbf{0}, \quad 0 < \alpha \leq \alpha^* \tag{13.326}$$

we can still use Theorem 13.4 to obtain an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$. Now, we establish the existence of such an α^*. Using the assumption $\mathbf{D} \preceq \mathbf{K}_{X|Y}$, we have

$$\mathbf{D} \preceq \mathbf{K}_{X|Y} = (\mathbf{K}_X^{-1} + \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1} \tag{13.327}$$

where the equality follows from (13.215). Equation (13.327) implies that

$$\mathbf{0} \prec \mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y \tag{13.328}$$

$$= \mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top \tag{13.329}$$

where we use the singular value decomposition of $\mathbf{H}_Y$. Thus, since $\mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top$ is strictly positive definite, there exists $0 < \beta$ such that

$$\mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top \succ \beta^2 \mathbf{I} \tag{13.330}$$

$$= \beta^2 \mathbf{R}_Y \mathbf{R}_Y^\top \tag{13.331}$$

which implies

$$\mathbf{D}^{-1} \succ \mathbf{R}_Y(\mathbf{\Lambda}_Y^2 + \beta^2)\mathbf{R}_Y^\top \tag{13.332}$$

which, in turn, implies the existence of an α^* such that

$$\mathbf{D}^{-1} \succ \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha)^2\mathbf{R}_Y^\top, \quad 0 < \alpha \leq \alpha^* \tag{13.333}$$

Hence, using the definition of $\mathbf{\Sigma}_{Y,\alpha}$ in (13.333), we get

$$\mathbf{D}^{-1} \succ \mathbf{\Sigma}_{Y,\alpha}^{-1}, \quad 0 < \alpha \leq \alpha^* \tag{13.334}$$

which is equivalent to the desired condition in (13.326) which is needed to use Theorem 13.4 to obtain an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$. Hence, assuming that $0 < \alpha \leq \alpha^*$, an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$ can be written as the union of rate and information leakage (R, I_e) pairs satisfying

$$R \geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|\bar{Y}_\alpha}|}{|\mathbf{D}|} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}_\alpha(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_{Y,\alpha}|}{|\mathbf{F}_\alpha(\mathbf{D}) + \mathbf{\Sigma}_{Y,\alpha}|} \tag{13.335}$$

$$I_e \geq \min_{\substack{0 \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}_\alpha(\mathbf{D})}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_{Y,\alpha}|}{|\mathbf{K}_{X|V} + \mathbf{\Sigma}_{Y,\alpha}|} + \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_{Z,\alpha}|}{|\mathbf{\Sigma}_{Z,\alpha}|} \tag{13.336}$$

where $\mathbf{F}_\alpha(\mathbf{D}) = \mathbf{\Sigma}_{Y,\alpha}(\mathbf{\Sigma}_{Y,\alpha} - \mathbf{D})^{-1}\mathbf{\Sigma}_{Y,\alpha} - \mathbf{\Sigma}_{Y,\alpha}$. We now find the limiting region that comes from the one described by (13.335)-(13.336) as $\alpha \to 0$. To this end,we

introduce the following lemma that will be used subsequently.

Lemma 13.17

$$\lim_{\alpha\to 0} \mathbf{K}_{X|\bar{\bar{Y}}_\alpha} = \mathbf{K}_{X|Y} \tag{13.337}$$

$$\lim_{\alpha\to 0} \mathbf{F}_\alpha(\mathbf{D}) = (\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1} \tag{13.338}$$

The proof of Lemma 13.17 is given in Appendix 13.7.14.

We first consider the rate bound in (13.335) as follows

$$\lim_{\alpha\to 0} \frac{1}{2} \log \frac{|\mathbf{K}_{X|\bar{\bar{Y}}_\alpha}|}{|\mathbf{D}|} = \frac{1}{2} \log \frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \tag{13.339}$$

which follows from the continuity of the determinant in positive semi-definite matrices and (13.337). Similarly, for the second expression in the rate bound in (13.335), we have

$$\begin{aligned}
&\lim_{\alpha\to 0} \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{F}_\alpha(\mathbf{D})|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{\Sigma}_{Y,\alpha}|}{|\mathbf{F}_\alpha(\mathbf{D}) + \mathbf{\Sigma}_{Y,\alpha}|} \\
&= \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \lim_{\alpha\to 0} \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{\Sigma}_{Y,\alpha}|}{|\mathbf{F}_\alpha(\mathbf{D}) + \mathbf{\Sigma}_{Y,\alpha}|} && (13.340) \\
&= \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \lim_{\alpha\to 0} \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-2}\mathbf{R}_Y^\top|}{|\mathbf{F}_\alpha(\mathbf{D}) + \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-2}\mathbf{R}_Y^\top|} && (13.341) \\
&= \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} \\
&\quad - \lim_{\alpha\to 0} \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{Q}_Y^\top \mathbf{Q}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{R}_Y^\top|}{|\mathbf{F}_\alpha(\mathbf{D}) + \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{Q}_Y^\top \mathbf{Q}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{R}_Y^\top|} && (13.342)
\end{aligned}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}|}$$
$$- \lim_{\alpha\to 0}\frac{1}{2}\log\frac{|\mathbf{Q}_Y(\mathbf{\Lambda}_Y+\alpha\mathbf{I})\mathbf{R}_Y^\top\mathbf{K}_X\mathbf{R}_Y(\mathbf{\Lambda}_Y+\alpha\mathbf{I})\mathbf{Q}_Y^\top+\mathbf{I}|}{|\mathbf{Q}_Y(\mathbf{\Lambda}_Y+\alpha\mathbf{I})\mathbf{R}_Y^\top\mathbf{F}_\alpha(\mathbf{D})\mathbf{R}_Y(\mathbf{\Lambda}_Y+\alpha\mathbf{I})\mathbf{Q}_Y^\top+\mathbf{I}|} \tag{13.343}$$
$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}|} - \frac{1}{2}\log\frac{|\mathbf{Q}_Y\mathbf{\Lambda}_Y\mathbf{R}_Y^\top\mathbf{K}_X\mathbf{R}_Y\mathbf{\Lambda}_Y\mathbf{Q}_Y^\top+\mathbf{I}|}{|\mathbf{Q}_Y\mathbf{\Lambda}_Y\mathbf{R}_Y^\top(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}\mathbf{R}_Y\mathbf{\Lambda}_Y\mathbf{Q}_Y^\top+\mathbf{I}|} \tag{13.344}$$
$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_X\mathbf{H}_Y^\top+\mathbf{I}|}{|\mathbf{H}_Y(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}\mathbf{H}_Y^\top+\mathbf{I}|} \tag{13.345}$$

where (13.340) is due to the continuity of the determinant in positive semi-definite matrices and (13.338), (13.341) comes from the definition of $\mathbf{\Sigma}_{Y,\alpha}$, (13.344) comes from the continuity of the determinant in positive semi-definite matrices and (13.338), and (13.345) is obtained by using the singular value decomposition of $\mathbf{H}_Y$. Hence, (13.339) and (13.345) imply that any rate R inside the region $\lim_{\alpha\to 0}\mathcal{R}_\alpha(\mathbf{D})$ satisfies

$$R \geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \tag{13.346}$$
$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_X\mathbf{H}_Y^\top+\mathbf{I}|}{|\mathbf{H}_Y(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}\mathbf{H}_Y^\top+\mathbf{I}|} \tag{13.347}$$

Following a similar analysis, the limit of the information leakage in (13.336) can be found as

$$\min_{\substack{\mathbf{0}\preceq\mathbf{K}_{X|V}\preceq\mathbf{K}_{X|U}\preceq\mathbf{K}_X \\ \mathbf{K}_{X|V}\preceq(\mathbf{D}^{-1}-\mathbf{H}_Y^\top\mathbf{H}_Y)^{-1}}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top+\mathbf{I}|}{|\mathbf{H}_Y\mathbf{K}_{X|V}\mathbf{H}_Y^\top+\mathbf{I}|}$$
$$+ \frac{1}{2}\log|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top+\mathbf{I}| \tag{13.348}$$

which implies that any information leakage I_e inside the region $\lim_{\alpha\to 0}\mathcal{R}_\alpha(\mathbf{D})$ should be larger than (13.348); completing the proof of Theorem 13.6.

13.7.14 Proof of Lemma 13.17

We first prove the following lemma which will be used subsequently.

Lemma 13.18 *Let* $\mathbf{K}(\alpha) = (\mathbf{A} + f(\alpha)\mathbf{B})^{-1},\ 0 < \alpha \leq \alpha^*$, *where* $\mathbf{A} \succ f(\alpha)\mathbf{B} \succeq \mathbf{0},\ 0 \leq \alpha \leq \alpha^*$ *and* $f(\alpha)$ *is continuous in* α. *Then, we have*

$$\lim_{\alpha\to 0}\mathbf{K}(\alpha) = (\mathbf{A} + f(0)\mathbf{B})^{-1} \tag{13.349}$$

Proof: In the proof of this lemma, we use the fact that if $\lim_{n\to\infty}\mathbf{C}^n = \mathbf{0}$, we have

$$(\mathbf{I} + \mathbf{C})^{-1} = \sum_{n=0}^{\infty}(-1)^n\mathbf{C}^n \tag{13.350}$$

where $\mathbf{C}^0 = \mathbf{I}$ [115, page 19]. Now, we consider

$$\mathbf{K}(\alpha) = (\mathbf{A} + f(\alpha)\mathbf{B})^{-1} \tag{13.351}$$

$$= \mathbf{A}^{-1/2}(\mathbf{I} + f(\alpha)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^{-1}\mathbf{A}^{-1/2} \tag{13.352}$$

where due to $\mathbf{A} \succ f(\alpha)\mathbf{B} \succeq \mathbf{0}$, we have $\mathbf{I} \succ f(\alpha)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2} \succeq \mathbf{0}$ which implies

$$\lim_{n\to\infty}\left(f(\alpha)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2}\right)^n = \mathbf{0} \tag{13.353}$$

Hence, we can use (13.350) in (13.352) to get

$$\mathbf{K}(\alpha) = \mathbf{A}^{-1/2}\left[\sum_{n=0}^{\infty}(-1)^n f^n(\alpha)(\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^n\right]\mathbf{A}^{-1/2} \tag{13.354}$$

which implies

$$\lim_{\alpha\to 0}\mathbf{K}(\alpha) = \lim_{\alpha\to 0}\mathbf{A}^{-1/2}\left[\sum_{n=0}^{\infty}(-1)^n f^n(\alpha)(\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^n\right]\mathbf{A}^{-1/2} \tag{13.355}$$

$$= \mathbf{A}^{-1/2}\left[\sum_{n=0}^{\infty}(-1)^n f^n(0)(\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^n\right]\mathbf{A}^{-1/2} \tag{13.356}$$

$$= \mathbf{A}^{-1/2}\left[\mathbf{I} + f(0)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2}\right]^{-1}\mathbf{A}^{-1/2} \tag{13.357}$$

$$= (\mathbf{A} + f(0)\mathbf{B})^{-1} \tag{13.358}$$

where (13.357) comes from (13.350); completing the proof of Lemma 13.18. □

We now consider (13.337) in Lemma 13.17 as follows

$$\mathbf{K}_{X|\bar{\mathbf{Y}}_\alpha} = \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_{Y,\alpha})^{-1}\mathbf{\Sigma}_{Y,\alpha} \tag{13.359}$$

$$= (\mathbf{K}_X^{-1} + \mathbf{\Sigma}_{Y,\alpha}^{-1})^{-1} \tag{13.360}$$

$$= \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^2\mathbf{R}_Y^\top\right]^{-1} \tag{13.361}$$

$$= \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y\mathbf{\Lambda}_Y^2\mathbf{R}_Y^\top + \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top\right]^{-1} \tag{13.362}$$

where $0 < \alpha \leq \alpha^*$. Equation (13.359) comes from (13.173), (13.361) is due to the definition of $\mathbf{\Sigma}_{Y,\alpha}$. We note that $\mathbf{K}_X^{-1} + \mathbf{R}_Y\mathbf{\Lambda}_Y^2\mathbf{R}_Y^\top \succ \mathbf{0}$, and thus, α^* can be selected

to ensure that

$$\mathbf{K}_X^{-1} + \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top \succ \mathbf{R}_Y (2\alpha \mathbf{\Lambda}_Y + \alpha^2 \mathbf{I}) \mathbf{R}_Y^\top \tag{13.363}$$

for all $0 \leq \alpha \leq \alpha^*$. Hence, we can use Lemma 13.18 in (13.362) to get

$$\begin{aligned}
\lim_{\alpha \to 0} \mathbf{K}_{X|\bar{\mathbf{Y}}_\alpha} &= \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top\right]^{-1} && (13.364)\\
&= \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y \mathbf{\Lambda}_Y \mathbf{Q}_Y^\top \mathbf{Q}_Y \mathbf{\Lambda}_Y \mathbf{R}_Y^\top\right]^{-1} && (13.365)\\
&= (\mathbf{K}_X^{-1} + \mathbf{H}_Y^T \mathbf{H}_Y)^{-1} && (13.366)\\
&= \mathbf{K}_{X|Y} && (13.367)
\end{aligned}$$

where (13.366) comes from the singular value decomposition of $\mathbf{H}_Y$ and (13.367) is due to (13.215); completing the proof of (13.337).

Next, we consider (13.338) in Lemma 13.17 as follows

$$\begin{aligned}
\mathbf{F}_\alpha(\mathbf{D}) &= \mathbf{\Sigma}_{Y,\alpha}(\mathbf{\Sigma}_{Y,\alpha} - \mathbf{D})^{-1}\mathbf{\Sigma}_{Y,\alpha} - \mathbf{\Sigma}_{Y,\alpha} && (13.368)\\
&= \mathbf{\Sigma}_{Y,\alpha}(\mathbf{\Sigma}_{Y,\alpha} - \mathbf{D})^{-1}\mathbf{D} && (13.369)\\
&= (\mathbf{D}^{-1} - \mathbf{\Sigma}_{Y,\alpha}^{-1})^{-1} && (13.370)\\
&= (\mathbf{D}^{-1} - \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^2\mathbf{R}_Y^\top)^{-1} && (13.371)\\
&= \left[\mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top - \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top\right]^{-1} && (13.372)\\
&= \left[\mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y \mathbf{Q}_Y^\top \mathbf{Q}_Y \mathbf{\Lambda}_Y \mathbf{R}_Y^\top - \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top\right]^{-1} && (13.373)\\
&= \left[\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y - \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top\right]^{-1} && (13.374)
\end{aligned}$$

where $0 < \alpha \leq \alpha^*$. Equation (13.371) comes from the definition of $\mathbf{\Sigma}_{Y,\alpha}$ and (13.374) is obtained by using the singular value decomposition of $\mathbf{H}_Y$. We note that $\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y$ is strictly positive definite as (13.328) indicates, and hence, there exists an α^* such that

$$\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y \succ \mathbf{R}_Y (2\alpha \mathbf{\Lambda}_Y + \alpha^2 \mathbf{I}) \mathbf{R}_Y^\top \tag{13.375}$$

for all $0 \leq \alpha \leq \alpha^*$. Consequently, we can use Lemma 13.18 in (13.374) to get

$$\lim_{\alpha \to 0} \mathbf{F}_\alpha(\mathbf{D}) = (\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1} \tag{13.376}$$

which completes the proof of Lemma 13.17.

Chapter 14

Secure Lossy Source Coding under Relative Equivocation

14.1 Introduction

In this chapter, we revisit the problem of secure lossy source coding with side information that we considered in the previous chapter. In this problem, the transmitter wants to describe the source to the legitimate user within a distortion level while keeping the source hidden from the eavesdropper as much as possible, where both the legitimate user and the eavesdropper have some side information. In all previous works studying the secure lossy source coding problem, the secrecy is measured by either the equivocation of the source at the eavesdropper (see [14, 112] and our work in Chapter 13) or the equivocation of the legitimate user's reconstruction of the source at the eavesdropper (see [117]).

In this chapter, first, we argue that both of these secrecy measures have drawbacks, especially if one wants to quantify the relative confusion of the eavesdropper about the source with respect to the legitimate user. In secure channel coding problems (resp. secure lossless source coding problems), due to the perfect recovery of the message (resp. the source) at the legitimate user, the equivocation of the message (resp. the source) accurately measures the relative equivocation of the eavesdropper. However, in the context of secure *lossy* source coding, since the legitimate user does not reconstruct the source perfectly, but only within a distortion, the equivocation

of the source at the eavesdropper cannot accurately measure the relative confusion of the eavesdropper with respect to the legitimate user. Consequently, we argue that the relative equivocation is a better measure of secrecy for the secure lossy source coding problem.

Once we adopt the relative equivocation as the secrecy measure, we obtain the single-letter description of the rate, relative equivocation and distortion region for the secure lossy source coding problem. To this end, we show that the coding scheme proposed in [14], where the same problem is studied when the equivocation of the source at the eavesdropper is used as the secrecy measure, attains the rate, relative equivocation and distortion region.

Next, we specialize the single-letter description we obtain to the degraded and reversely degraded cases. Although the single-letter description of the rate, relative equivocation and distortion region involves two auxiliary random variables, when it is specialized to either degraded or reversely degraded cases, a single auxiliary random variable is sufficient for the single-letter description. The latter fact implies that Wyner-Ziv scheme [113] is optimal for both degraded and reversely degraded cases, though it might not be optimal for the general case. In the final part of the chapter, we address this issue, and provide a model for which two auxiliary random variables are needed; implying that Wyner-Ziv scheme is not optimal in general.

14.2 The Secrecy Measure

Let $\{(X_i, Y_i, Z_i)\}_{i=1}^n$ denote i.i.d. tuples drawn from a distribution $p(x, y, z)$. The transmitter, legitimate user and the eavesdropper observe $X^n \in \mathcal{X}^n, Y^n \in \mathcal{Y}^n$, and $Z^n \in \mathcal{Z}^n$, respectively. The transmitter wants to convey information to the legitimate user in a way that the legitimate user can reconstruct the source X^n within a certain distortion while keeping the source from the eavesdropper as secret as possible (see Figure 14.1). We note that if there was no eavesdropper, this setting would reduce to the Wyner-Ziv problem [113].

The distortion of the reconstructed sequence at the legitimate user is measured by the function $d^n(X^n, \hat{X}^n)$ where $\hat{X}^n \in \hat{\mathcal{X}}^n$ denotes the legitimate user's reconstruction of the source X^n. We consider functions $d^n(X^n, \hat{X}^n)$ that have the following form

$$d^n(X^n, \hat{X}^n) = \frac{1}{n} \sum_{i=1}^{n} d(X_i, \hat{X}_i) \tag{14.1}$$

where $d(a, b)$ is a non-negative finite-valued function.

In the previous works [14, 112] on secure lossy source coding with side information (as well as our work in Chapter 13), the objective was to maximize the uncertainty of the eavesdropper about the source X^n, and consequently, the equivocation of the source at the eavesdropper was chosen as the measure of secrecy:

$$\frac{1}{n} H(X^n | M, Z^n) \tag{14.2}$$

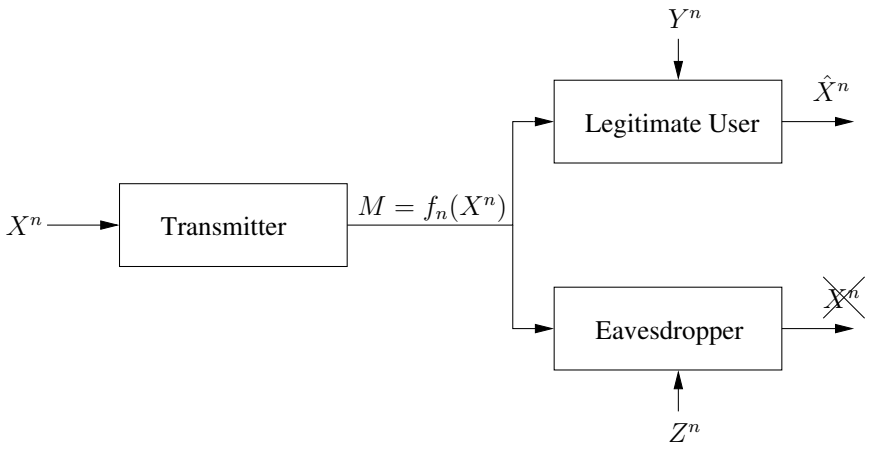

Figure 14.1: Secure lossy source coding with side information.

where $M \in \mathcal{M}$, which is a function of the source X^n, denotes the signal sent by the transmitter. In this paper, we propose to use *relative equivocation* of the source at the eavesdropper with respect to the legitimate user

$$\frac{1}{n}\big[H(X^n|M, Z^n) - H(X^n|M, Y^n)\big] \tag{14.3}$$

To measure secrecy by using the equivocation of the source at the eavesdropper given by (14.2) is indeed inspired by the secure transmission of uniformly distributed messages over a wiretap channel (see Figure 14.2), where secrecy is measured by the equivocation of the message at the eavesdropper

$$\frac{1}{n}H(W|Z^n) \tag{14.4}$$

We note that in the wiretap channel, the legitimate user correctly decodes the message W, and hence due to Fano's lemma, we have $\lim_{n\to\infty}(1/n)H(W|Y^n) = 0$. Thus, the equivocation of the message at the eavesdropper for the wiretap channel

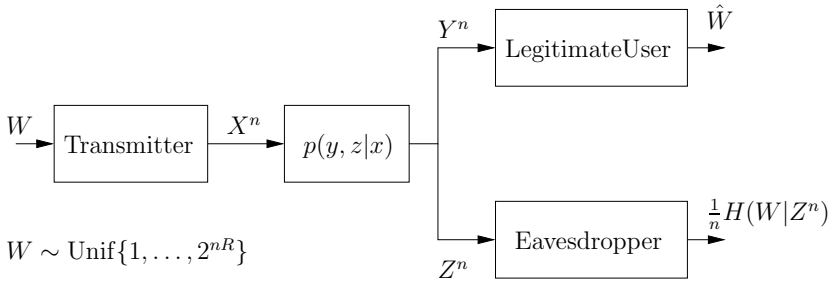

Figure 14.2: Wiretap channel.

given by (14.4) is equivalent to

$$\frac{1}{n}\left[H(W|Z^n) - H(W|Y^n)\right] \tag{14.5}$$

as $n \to \infty$. In other words, as $n \to \infty$, the equivocation of the message at the eavesdropper given by (14.4) is equivalent to the relative equivocation of the message at the eavesdropper with respect to the legitimate user given by (14.5).

In our case, since the legitimate user does not reconstruct the source in a lossless manner, the legitimate user will have some confusion about the source. In other words, as long as the distortion between the source and its reconstruction at the legitimate user is non-zero, the legitimate user will have a non-zero equivocation, i.e., we have $\lim_{n\to\infty}(1/n)H(X^n|M, Y^n) \neq 0$. Hence, as opposed to the wiretap channel, in our case, if we use the equivocation of the source at the eavesdropper given by (14.2) as the secrecy measure, we do not have an equivalence between (14.2) and the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (14.3). In other words, although in the wiretap channel, the equivocation at the eavesdropper tells us not only how much the eavesdropper

is confused about the message but also the relative confusion of the eavesdropper with respect to the legitimate user, in the secure lossy source coding problem, the equivocation at the eavesdropper tells us just how much the eavesdropper is confused about the source, but not the relative confusion of the eavesdropper with respect to the legitimate user.

Moreover, although the equivocation of the source at the eavesdropper given by (14.2) cannot indicate whether the eavesdropper has a better reconstruction of the source or not, *for some models of source and side information*, the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (14.3) would indicate whether the eavesdropper has a better reconstruction of the source than the legitimate user. The following example identifies some models of source and side information where this claim holds.

Example 14.1 *In this example, we consider the degraded and reversely degraded models. For the degraded model, we have the following Markov chain*

$$X_i \to Y_i \to Z_i, \quad i = 1, \ldots, n \tag{14.6}$$

and for the reversely degraded model, we have the following Markov chain

$$X_i \to Z_i \to Y_i, \quad i = 1, \ldots, n \tag{14.7}$$

We assume that in both models, both the legitimate user and the eavesdropper have the same reconstruction alphabet $\hat{\mathcal{X}}^n$ *and use the same distortion metric* $d^n(x^n, \hat{x}^n) =$

$(1/n)\sum_{i=1}^{n} d(x_i, \hat{x}_i)$. *We denote the minimum achievable distortion by the legitimate user and the eavesdropper by* d_Y *and* d_Z*, respectively. We have the following order between* d_Y *and* d_Z *for the models under consideration in this example.*

Lemma 14.1 *When both the legitimate user and the eavesdropper use the same reconstruction alphabet and the same distortion metric, the following orders hold.*

- *If* $X_i \to Y_i \to Z_i,\ i = 1, \ldots, n$*, we have* $d_Y \leq d_Z$*.*
- *If* $X_i \to Z_i \to Y_i,\ i = 1, \ldots, n$*, we have* $d_Y \geq d_Z$*.*

The proof of Lemma 14.1 is given in Appendix 14.8.1.

Now, we consider the degraded model. For the degraded model, as Lemma 14.1 states, the minimum achievable distortion by the legitimate user is less than the minimum achievable distortion by the eavesdropper, i.e., $d_Y \leq d_Z$*. Consequently, we expect that the eavesdropper is more confused about the source than the legitimate user, i.e., the relative equivocation of the source at the eavesdropper with respect to the legitimate user is positive. Indeed, this expectation is right as seen through*

$$H(X^n|M, Z^n) - H(X^n|M, Y^n) = H(X^n|M, Z^n) - H(X^n|M, Y^n, Z^n) \tag{14.8}$$

$$= I(X^n; Y^n|M, Z^n) \tag{14.9}$$

$$\geq 0 \tag{14.10}$$

where (14.8) is due to the Markov chain $M \to X^n \to Y^n \to Z^n$*.*

Similarly, for the reversely degraded model, as Lemma 14.1 states, the minimum achievable distortion by the eavesdropper is less than the minimum achievable

distortion by the legitimate user, i.e., $d_Z \leq d_Y$, and consequently, the legitimate user is more confused about the source than the legitimate user, i.e., the relative equivocation at the eavesdropper with respect to the legitimate user is negative:

$$H(X^n|M,Z^n) - H(X^n|M,Y^n) = H(X^n|M,Z^n,Y^n) - H(X^n|M,Y^n) \tag{14.11}$$

$$= -I(X^n;Z^n|M,Y^n) \tag{14.12}$$

$$\leq 0 \tag{14.13}$$

where (14.11) is due to the Markov chain $M \to X^n \to Z^n \to Y^n$.

We note that although this example shows that *for some models of source and side information*, the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (14.3) indicates whether the eavesdropper will have a better reconstruction of the source than the legitimate user, we do not expect it to hold for all source and side information models. For example, if there is a model with vector source and side information, and the model is neither degraded nor reversely degraded, then using the relative equivocation, we might not understand whether the legitimate user or the eavesdropper is able to reconstruct a specific component of the source in a better way. Indeed, to understand the relative qualities of the reconstructions of the source at the legitimate user and the eavesdropper, the most appropriate secrecy metric to use is the minimum attainable distortion of the eavesdropper's reconstruction of the source. However, this formulation does not seem to be tractable for now, especially, if one considers the fact that even for the degraded case, this problem is still open [110].

Before adopting the relative equivocation given by (14.3) as the secrecy metric to formulate the problem of secure lossy source coding with side information, we discuss another possible secrecy metric [117] which considers the equivocation of the reconstructed sequence at the eavesdropper:

$$\frac{1}{n}H(\hat{X}^n|M, Z^n) \tag{14.14}$$

Although this secrecy measure is useful in the sense that it can tell us how much information the eavesdropper has about the legitimate user's reconstruction, and hence to what extent, the eavesdropper can reproduce the legitimate user's reconstruction, this secrecy measure also has some shortcomings. First, we note that although the equivocation of the reconstructed source at the eavesdropper measures the capability of the eavesdropper to reproduce the legitimate user's reconstruction, it does not measure the capability of the eavesdropper to reproduce the source itself. Hence, the use of the equivocation of the legitimate user's reconstruction as the measure of secrecy might be misleading, because the equivocation of the reconstructed source might have a non-zero value indicating that the eavesdropper cannot duplicate the legitimate user's reconstruction, while the eavesdropper has a better reconstruction of the source than the legitimate user. The following example demonstrates this observation.

Example 14.2 *In this example, we consider the reversely degraded model introduced in Example 14.1. In the reversely degraded model, the eavesdropper has a better side information than the legitimate user, and consequently, is less confused than*

the legitimate user. Moreover, as Lemma 14.1 states, for the reversely degraded model, we have $d_Z \leq d_Y$, i.e., the eavesdropper has a better reconstruction of the source than the legitimate user. On the other hand, due to the non-negativity of the entropy, we have $H(\hat{X}^n|M, Z^n) \geq 0$ indicating that the eavesdropper might not be able to reproduce the legitimate user's reconstruction of the source. This results from the fact that the reconstructed sequence $\hat{X}^n$ depends on Y^n, where this dependence cannot be resolved by conditioning on Z^n. Hence, the use of equivocation of legitimate user's reconstruction might be misleading.

Another point about the equivocation of the reconstructed sequence at the eavesdropper given by (14.14) is that it depends on the entire joint distribution of the source X^n and side information Y^n and Z^n, i.e., $p(x^n, y^n, z^n)$. It is well-known that the minimum achievable distortions by the legitimate user and the eavesdropper, i.e., d_Y and d_Z, depend only on the distributions $p(x^n, y^n)$ and $p(x^n, z^n)$, respectively, but not on the joint distribution $p(x^n, y^n, z^n)$. Hence, by using the equivocation of the reconstructed sequence at the eavesdropper given by (14.14), we might get different equivocations for models that have identical distortion pairs (d_Y, d_Z). In particular, consider two models with joint distributions $p_1(x^n, y^n, z^n)$ and $p_2(x^n, y^n, z^n)$, for which although the joint distributions $p_1(x^n, y^n, z^n)$ and $p_2(x^n, y^n, z^n)$ are not identical, we have $p_1(x^n, y^n) = p_2(x^n, y^n)$ and $p_1(x^n, z^n) = p_2(x^n, z^n)$. Let d_Y^i be the minimum achievable distortion by the legitimate user in the model described by $p_i(x^n, y^n, z^n)$, and similarly, let d_Z^i be the minimum achievable distortion by the eavesdropper in the model described by $p_i(x^n, y^n, z^n)$. Due to the equalities

$p_1(x^n, y^n) = p_2(x^n, y^n)$ and $p_1(x^n, z^n) = p_2(x^n, z^n)$, we have $d_Y^1 = d_Y^2$ and $d_Z^1 = d_Z^2$. On the other hand, in general, we have $H_1(\hat{X}^n|M, Z^n) \neq H_2(\hat{X}^n|M, Z^n)$[1] because the equivocation of the reconstructed sequence at the eavesdropper given by (14.14) depends on the joint distribution, and the joint distributions for these models are not identical, i.e., $p_1(x^n, y^n, z^n) \neq p_2(x^n, y^n, z^n)$. Hence, the equivocation of the reconstructed sequence at the eavesdropper might be regarded as an inconsistent measure of secrecy because although the relative qualities of the reconstructions of the legitimate user and the eavesdropper do not change from one model to the other, the equivocation of the reconstructed sequence at the eavesdropper might change.

14.3 Single-letter Characterization

Now, we formulate the secure lossy source coding problem when the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (14.3) is used as the merit of secrecy. An (n, R) code for secure lossy source coding consists of an encoding function $f_n : \mathcal{X}^n \to \mathcal{M} = \{1, \ldots, 2^{nR}\}$ at the transmitter and a decoding function at the legitimate user $g_n : \mathcal{M} \times \mathcal{Y}^n \to \hat{\mathcal{X}}^n$. A rate, relative equivocation and distortion tuple (R, Δ, D) is achievable if there exists an (n, R) code satisfying

$$\lim_{n\to\infty} \frac{1}{n}\big[H(X^n|M, Z^n) - H(X^n|M, Y^n)\big] \geq \Delta \tag{14.15}$$

$$\lim_{n\to\infty} E[d^n(X^n, \hat{X}^n)] \leq D \tag{14.16}$$

[1] $H_i(\hat{X}^n|M, Z^n)$ denotes the conditional entropy term that is computed according to the distribution $p_i(m, x^n, y^n, z^n, \hat{x}^n)$.

where $M = f_n(X^n) \in \mathcal{M}$. The set of all achievable (R, Δ, D) tuples is denoted by $\mathcal{R}^*$. We obtain a single-letter characterization of the region $\mathcal{R}^*$ as stated in the following theorem.

Theorem 14.1 $(R, \Delta, D) \in \mathcal{R}^*$ *iff*

$$R \geq I(V;X) - I(V;Y) \tag{14.17}$$

$$\Delta \leq I(X;Y|U) - I(X;Z|U) \tag{14.18}$$

$$D \geq E[d(X, \hat{X}(V,Y))] \tag{14.19}$$

for some U, V *satisfying the following Markov chain*

$$U \to V \to X \to Y, Z \tag{14.20}$$

and a function $\hat{X}(V,Y)$.

The proof of Theorem 14.1 is given in Appendix 14.8.2. We show the achievability of the region $\mathcal{R}^*$ by using the coding scheme proposed in [14], where the problem of secure lossy source coding with side information was studied when the secrecy of the source is measured by its equivocation at the eavesdropper given in (14.2). We note that the two problems, the one that we consider by using the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (14.3) as the secrecy measure and the other one studied in [14] that uses the equivocation of the source at the eavesdropper given by (14.2) as the secrecy measure, are not identical, and hence, having the optimum coding scheme

for the latter problem does not imply that it will be an optimum solution for our problem that uses the relative equivocation given by (14.3) as the secrecy measure. Since here we show that the coding scheme in [14] can also achieve the region $\mathcal{R}^*$, our result implies that maximizing the equivocation at the eavesdropper given by (14.2) is equivalent to maximizing the difference between the equivocations of the legitimate user and the eavesdropper given by (14.3).

The coding scheme achieving the region $\mathcal{R}^*$ is similar to the Wyner-Ziv scheme [113] in the sense that both schemes, by means of binning, make use of the side information at the legitimate user to reduce the transmission rate. The difference between these two schemes is that although the Wyner-Ziv scheme uses a single-binning, the coding scheme achieving the region $\mathcal{R}^*$ uses a double-binning, where the additional binning is necessary due to the secrecy consideration in our problem. In particular, in our problem, the transmitter generates sequences (U^n, V^n) and bins both sequences. The bin indices of these two sequences are delivered to the legitimate user. Using these bin indices, the legitimate user identifies the right (U^n, V^n) sequences, and reconstructs X^n within the required distortion. On the other hand, using the bin indices of (U^n, V^n), the eavesdropper identifies only the right U^n sequence, and consequently, U does not contribute to the equivocation, see (14.18)[2].

[2]The fact that the eavesdropper can decode U^n sequence can be obtained by observing that for a (U, V) selection, if $I(U;Y) \geq I(U;Z)$, there is no loss of optimality of setting $U = \phi$ which will yield a larger region.

14.4 Degraded and Reversely Degraded Cases

We now consider the degraded and reversely degraded cases. In the degraded case, the source and side information satisfy the Markov chain in (14.6) and in the reversely degraded case, they satisfy the Markov chain in (14.7).

For the degraded case, Theorem 14.1 can be specialized into the following form.

Corollary 14.1 *In the degraded case,* $(R, \Delta, D) \in \mathcal{R}^*$ *iff*

$$R \geq I(V;X) - I(V;Y) \tag{14.21}$$

$$\Delta \leq I(X;Y) - I(X;Z) \tag{14.22}$$

$$D \geq E[d(X, \hat{X}(V,Y))] \tag{14.23}$$

for some V *satisfying the following Markov chain* $V \rightarrow X \rightarrow Y \rightarrow Z$ *and a function* $\hat{X}(V,Y)$.

This corollary can be obtained from Theorem 14.1 by noting the fact that $I(X;Y|U) - I(X;Z|U) \leq I(X;Y) - I(X;Z)$ in view of the Markov chain in (14.6), where the equality can be attained by setting $U = \phi$. Corollary 14.1 implies that in the degraded case, the relative equivocation is not affected by the choice of V, and hence, there is no tension between the achievable rate and the achievable relative equivocation originating from the choice of V. This also implies that the use of optimal compression rate for the given distortion level is optimal. In other words, the use of Wyner-Ziv coding [113] is optimal, and the region $\mathcal{R}^*$ for a fixed distortion

D can be expressed as the union of rate and relative equivocation pairs (R, Δ)

$$R \geq R_{WZ}(D) \tag{14.24}$$

$$\Delta \leq I(X;Y) - I(X;Z) \tag{14.25}$$

where $R_{WZ}(D)$ is the Wyner-Ziv rate distortion function given by

$$R_{WZ}(D) = \min_{\substack{V \to X \to Y \\ E\left[d(X,\hat{X}(V,Y))\right] \leq D}} I(V;X) - I(V;Y) \tag{14.26}$$

The following example obtains the rate and relative equivocation region for the degraded scalar Gaussian model.

Example 14.3 *In this example, we consider the degraded scalar Gaussian model. In this model, there is an i.i.d. Gaussian source* $\{X_i\}_{i=1}^n$ *with zero-mean and variance* σ_X^2*. The side information are given by*

$$Y_i = X_i + N_{Y,i} \tag{14.27}$$

$$Z_i = X_i + N_{Z,i} \tag{14.28}$$

where $\{N_{Y,i}\}_{i=1}^n$ *and* $\{N_{Z,i}\}_{i=1}^n$ *are i.i.d. Gaussian random variables with zero-mean and variance* σ_Y^2 *and* σ_Z^2*, respectively.* X_i *and* $(N_{Y,i}, N_{Z,i})$ *are independent for each* i*. We assume that* $\sigma_Y^2 < \sigma_Z^2$*. Thus, without loss of generality, we can assume that*

the Markov chain

$$X_i \to Y_i \to Z_i \tag{14.29}$$

holds, since the correlation between $N_{Y,i}$ and $N_{Z,i}$ does not change the rate, relative equivocation and distortion region. Hence, in view of the Markov chain in (14.29), the rate, relative equivocation and distortion region of this model follows from Corollary 14.1.

Before evaluating the region in Corollary 14.1 for the degraded scalar Gaussian model, we specify the distortion metric. For this model, the distortion of the reconstructed sequence is measured by its mean square error, i.e., $d(x, \hat{x}) = (x - \hat{x})^2$. Since the mean square error is minimized by the conditional mean, the legitimate user selects its reconstruction function as

$$\hat{X}_i = E\left[X_i | Y^n, f_n(X^n)\right] \tag{14.30}$$

which implies that the distortion constraint in Corollary 14.1 can be expressed as

$$\sigma^2_{X|VY} \leq D \tag{14.31}$$

Hence, we can obtain the rate and relative equivocation region of the degraded scalar Gaussian model by evaluating the region defined by (14.21)-(14.22) and (14.31), which results in the region stated in the following corollary.

Corollary 14.2 *In the degraded scalar Gaussian model,* $(R, \Delta) \in \mathcal{R}^*(D)$ *iff*

$$R \geq R_{\mathrm{WZ}}(D) = \frac{1}{2} \log \frac{\sigma_X^2 \sigma_Y^2}{D\left(\sigma_X^2 + \sigma_Y^2\right)} \tag{14.32}$$

$$\Delta \leq \frac{1}{2} \log \frac{\sigma_X^2 + \sigma_Y^2}{\sigma_Y^2} - \frac{1}{2} \log \frac{\sigma_X^2 + \sigma_Z^2}{\sigma_Z^2} \tag{14.33}$$

We note that in Corollary 14.2, the relative equivocation is constant, i.e., does not interact with the rate. This also implies that we can always transmit at the Wyner-Ziv rate.

Next, we specialize Theorem 14.1 for the reversely degraded model as follows.

Corollary 14.3 *In the reversely degraded case,* $(R, \Delta, D) \in \mathcal{R}^*$ *iff*

$$R \geq I(V;X) - I(V;Y) \tag{14.34}$$

$$\Delta \leq I(X;Y|V) - I(X;Z|V) \tag{14.35}$$

$$D \geq E[d(X, \hat{X}(V,Y))] \tag{14.36}$$

for some V *satisfying the following Markov chain* $V \to X \to Z \to Y$ *and a function* $\hat{X}(V,Y)$.

This corollary can be obtained from Theorem 14.1 by noting the fact that $I(X;Y|U) - I(X;Z|U) \leq I(X;Y|V) - I(X;Z|V)$ in view of the Markov chain in (14.7), where the equality can be attained by setting $U = V$. Corollary 14.3 implies that unlike the degraded case, in the reversely degraded case, there might be a tension between the achievable rate and the achievable relative equivocation

originating from the choice of V, since both the achievable rate and the achievable relative equivocation depend on the choice of V. However, similar to the degraded case, in the reversely degraded case also, we need only one auxiliary random variable to attain the rate, relative equivocation and distortion region $\mathcal{R}^*$. Thus, similar to the degraded case, in the reversely degraded case also, Wyner-Ziv coding [113] is sufficient to attain the entire region $\mathcal{R}^*$. The difference between the degraded and the reversely degraded cases is that in the degraded case, we can always transmit at the minimum rate determined by the Wyner-Ziv rate distortion function in (14.24), however, in the reversely degraded case, we might need to transmit at higher rates to obtain a higher relative equivocation, since in this case, both the achievable rate and the achievable relative equivocation depend on the choice of the auxiliary random variable V. In other words, the choice of V that minimizes the rate, i.e., the minimizer for the optimization problem in (14.24), might not be the maximizer of the relative equivocation term in (14.35). The following example demonstrates this point.

Example 14.4 *In this example, we consider the reversely degraded scalar Gaussian model which is identical to the degraded scalar Gaussian model in Example 14.3 with the only exception that here, we have $\sigma_Z^2 < \sigma_Y^2$. Thus, without loss of generality, we can assume that the Markov chain*

$$X_i \to Z_i \to Y_i \tag{14.37}$$

holds, since the correlation between $N_{Y,i}$ and $N_{Z,i}$ does not change the rate, relative

equivocation and distortion region. Hence, in view of the Markov chain in (14.37), the rate, relative equivocation and distortion region of this model follows from Corollary 14.3.

Before evaluating the region in Corollary 14.3, we specify the distortion metric. Similar to Example 14.3, here also, we use the mean square error as the distortion metric, i.e., $d(x,\hat{x}) = (x-\hat{x})^2$. Hence, the optimal reconstruction function for the legitimate user is given by the conditional mean in (14.30), which implies that the distortion constraint in Corollary 14.3 can be expressed as

$$\sigma^2_{X|VY} \leq D \tag{14.38}$$

Hence, we can obtain the rate, relative equivocation and distortion region of the reversely degraded scalar Gaussian model by evaluating the region defined by (14.34)-(14.35) and (14.38), which results in the region stated in the following corollary.

Corollary 14.4 *In the reversely degraded scalar Gaussian model, $(R,\Delta) \in \mathcal{R}^*(D)$ iff*

$$R \geq \frac{1}{2}\log\frac{\sigma^2_X}{\sigma^2_{X|V}} - \frac{1}{2}\log\frac{\sigma^2_X+\sigma^2_Y}{\sigma^2_{X|V}+\sigma^2_Y} \tag{14.39}$$

$$\Delta \leq \frac{1}{2}\log\frac{\sigma^2_{X|V}+\sigma^2_Y}{\sigma^2_Y} - \frac{1}{2}\log\frac{\sigma^2_{X|V}+\sigma^2_Z}{\sigma^2_Z} \tag{14.40}$$

for some $\sigma^2_{X|V}$ satisfying

$$\sigma^2_{X|V} \leq \frac{\sigma^2_Y D}{\sigma^2_Y - D} \tag{14.41}$$

We note that both rate and relative equivocation constraints in (14.39) and (14.40), respectively, are monotonically decreasing in $\sigma^2_{X|V}$. Hence, there is a tension between the rate and the relative equivocation, i.e., there is a trade-off between the achievable rate and the relative equivocation controlled by $\sigma^2_{X|V}$, and equivalently by the choice of V.

14.5 Maximum Relative Equivocation

In the previous section, we consider the degraded and reversely degraded cases where it turned out that either $(U = \phi, V)$ or $(U = V, V)$ is optimal for the evaluation of the region given in Theorem 14.1. Here, we address the question whether one of these two choices $(U = \phi, V)$ and $(U = V, V)$ is always optimal. To this end, we consider the maximum relative equivocation that is achievable when there is no rate constraint on the transmitter. In other words, we are interested in the maximum relative equivocation that we can obtain when the legitimate user needs to reconstruct the source within a distortion D while there is no concern on the transmission rate R. We denote the maximum relative equivocation by $\Delta_{\max}(D)$ which is given in the following theorem.

Theorem 14.2 *The maximum relative equivocation $\Delta_{\max}(D)$ at the eavesdropper with respect to the legitimate user when the legitimate user needs to reconstruct the source within a distortion D while there is no concern on the transmission rate R*

is given by

$$\Delta_{\max}(D) = \max_{\substack{U \to V \to X \to Y,Z \\ E\left[d(X,\hat{X}(V,Y))\right] \leq D}} I(X;Y|U) - I(X;Z|U) \tag{14.42}$$

We note that in Theorem 14.2, there are two auxiliary random variables U and V over which optimization needs to be carried out. In the previous section, we observe that when the model is either degraded or reversely degraded, a single auxiliary random variable is sufficient. Now, we provide the following example which shows that there are models for which two auxiliary random variables are necessary, in other words, neither $(U = \phi, V)$ nor $(U = V, V)$ is sufficient to attain the maximum relative equivocation, and hence the entire rate, relative equivocation and distortion region.

Example 14.5 *Consider the parallel Gaussian source* $\mathbf{X}_i = [X_{1,i} \ X_{2,i}]^\top$ *where* $\{X_{1,i}\}_{i=1}^n$ *and* $\{X_{2,i}\}_{i=1}^n$ *are i.i.d. zero-mean Gaussian random variables with variances* $\sigma_{X,1}^2$ *and* $\sigma_{X,2}^2$*, respectively. The side information at the legitimate receiver and the eavesdropper are given by*

$$Y_{\ell,i} = X_{\ell,i} + N_{Y,\ell,i}, \quad \ell = 1, 2 \tag{14.43}$$

$$Z_{\ell,i} = X_{\ell,i} + N_{Z,\ell,i}, \quad \ell = 1, 2 \tag{14.44}$$

where $\{N_{Y,\ell,i}\}_{i=1}^n$ *and* $\{N_{Z,\ell,i}\}_{i=1}^n$ *are zero-mean Gaussian random variables with variances* $\sigma_{Y,\ell}^2$ *and* $\sigma_{Z,\ell}^2$*, respectively, which are independent of* $\{X_{\ell,i}\}_{i=1}^n$*. Moreover, we assume that* $N_{Y,1,i}$ *and* $N_{Y,2,i}$ *are independent, and also so are* $N_{Z,1,i}$ *and* $N_{Z,2,i}$*.*

We assume that noise variances satisfy

$$\sigma_{Y,1}^2 < \sigma_{Z,1}^2 \tag{14.45}$$

$$\sigma_{Z,2}^2 < \sigma_{Y,2}^2 \tag{14.46}$$

Hence, without loss of generality, we can assume the following Markov chains

$$X_1 \to Y_1 \to Z_1 \tag{14.47}$$

$$X_2 \to Z_2 \to Y_2 \tag{14.48}$$

We impose a separate distortion constraint on each component of the source as follows

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} E\left[(X_{\ell,i} - \hat{X}_{\ell,i})^2\right] \leq D_\ell, \quad \ell = 1, 2 \tag{14.49}$$

Using Theorem 14.2, the maximum relative equivocation $\Delta_{\max}(D_1, D_2)$ can be obtained as follows.

Corollary 14.5

$$\Delta_{\max}(D_1, D_2) = I(X_1; Y_1) - I(X_1; Z_1) \tag{14.50}$$

if there exists V_1 satisfying $V_1 \to X_1 \to Y_1 \to Z_1$ and $\sigma_{X_1|V_1Y_1}^2 \leq D_1$.

We note that the maximum relative equivocation given in (14.50) corresponds

to the choice $U = (\phi, X_2), V = (V_1, X_2)$ *with independent* V_1 *and* X_2 *for the relative equivocation bound given in Theorem 14.2. It is clear that this optimal choice does not correspond to either* $(U = \phi, V)$ *or* $(U = V, V)$.

Next, we obtain the maximum relative equivocation arising from the choices $(U = \phi, V)$ *and* $(U = V, V)$. *When* $(U = \phi, V)$, *the corresponding maximum relative equivocation* $\Delta^{\phi}_{\max}(D_1, D_2)$ *is stated in the following lemma.*

Lemma 14.2

$$\Delta^{\phi}_{\max}(D_1, D_2) = \sum_{i=1}^{2} I(X_i; Y_i) - I(X_i; Z_i) \tag{14.51}$$

if there exist (V_1, V_2) *satisfying* $V_i \to X_i \to Y_i, Z_i$ *and* $\sigma^2_{X_i|V_iY_i} \leq D_i$.

Next, we obtain the maximum relative equivocation arising from the choice $U = V$, *denoted by* $\Delta^{\mathrm{S}}_{\max}(D_1, D_2)$, *as stated in the following lemma.*

Lemma 14.3

$$\Delta^{\mathrm{S}}_{\max}(D_1, D_2) = \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(X_1; Y_1|V_1) - I(X_1; Z_1|V_1) \tag{14.52}$$

We note that (14.52) corresponds to the choice $U = V = (V_1, X_2)$ *where* V_1 *and* X_2 *are independent.*

Now, we compare the maximum relative equivocation with the ones arising from the choices $(U = \phi, V)$ *and* $U = V$. *First, we compare* $\Delta_{\max}(D_1, D_2)$ *and*

$\Delta^{\phi}_{\max}(D_1, D_2)$ *as follows*

$$\Delta^{\phi}_{\max}(D_1, D_2) - \Delta_{\max}(D_1, D_2) = I(X_2; Y_2) - I(X_2; Z_2) \tag{14.53}$$

$$= -I(X_2; Z_2|Y_2) \tag{14.54}$$

$$< 0 \tag{14.55}$$

which implies that $(U = \phi, V)$ *is, in general, a sub-optimal choice for the non-degraded parallel Gaussian model.*

Next, we compare $\Delta_{\max}(D_1, D_2)$ *and* $\Delta^{\mathrm{S}}_{\max}(D_1, D_2)$*. To this end, we introduce the following lemma which will be used in the sequel.*

Lemma 14.4 **([Chapter 13, Lemma 13.1])** *For jointly Gaussian* (X, Y, Z) *satisfying the Markov chain* $X \to Y \to Z$ *and* $\Pr[Y = Z] \neq 1$*, if* $D < \sigma^2_{X|Y}$*, we have*

$$\min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(V; Y|Z) > 0 \tag{14.56}$$

Now, we are ready to compare $\Delta_{\max}(D_1, D_2)$ *and* $\Delta^{\mathrm{S}}_{\max}(D_1, D_2)$ *as follows*

$$\Delta^{\mathrm{S}}_{\max}(D_1, D_2) - \Delta_{\max}(D_1, D_2) = \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(X_1; Y_1|V_1) - I(X_1; Z_1|V_1)$$

$$- [I(X_1; Y_1) - I(X_1; Z_1)] \tag{14.57}$$

$$= \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1; Z_1) - I(V_1; Y_1) \tag{14.58}$$

$$= \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} -I(V_1; Y_1|Z_1) \tag{14.59}$$

$$= - \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1; Y_1|Z_1) \tag{14.60}$$

$$< 0 \tag{14.61}$$

where (14.59) is due to the Markov chain $V_1 \to X_1 \to Y_1 \to Z_1$ and (14.61) comes from Lemma 14.4. Hence, (14.61) implies that $U = V$ is, in general, a sub-optimal choice for the non-degraded parallel Gaussian model.

This example shows that in general, we might need two different auxiliary random variables to evaluate the region $\mathcal{R}^*$ in Theorem 14.1 for non-degraded models. Hence, we conclude that, in general, the Wyner-Ziv coding scheme [113] is not sufficient to attain the region $\mathcal{R}^*$ for general non-degraded models.

14.6 Uncoded Transmission

We note that in Theorem 14.2, there is no concern about the transmission rate R. Hence, the encoder can use any uncoded scheme that requires an infinite rate. We would like to understand whether the maximum relative equivocation $\Delta_{\max}(D)$ can be attained by an uncoded scheme. To this end, we consider a slightly more general scenario, where the encoder is allowed to use any *instantaneous* encoding function in the form of $g_i(X_i)$ where $g_i(\cdot)$ can be a deterministic or a stochastic mapping. When $g_i(\cdot)$ is chosen to be a stochastic function, we assume that it is independent across time. We note that since any uncoded scheme can be obtained

from an instantaneous encoding scheme by choosing $g_i(\cdot)$ to be a linear function, the instantaneous encoding scheme encompasses any uncoded scheme. Moreover, uncoded transmission with artificial noise can also be obtained from an instantaneous encoding scheme by selecting $g_i(x) = \alpha x + N$, where N denotes the noise. When the encoder uses an instantaneous encoding scheme, the transmitted signal is given by $M = [g_1(X_1), \ldots, g_n(X_n)]$. We denote the maximum relative equivocation when the encoder uses an instantaneous scheme by $\Delta_{\text{ins}}(D)$, where, as usual, D denotes the distortion level within which the legitimate user needs to reconstruct the source. The following example shows that, in general, $\Delta_{\max}(D)$ cannot be achieved by an instantaneous encoding scheme, i.e., there are models where the maximum relative equivocation $\Delta_{\max}(D)$ is strictly larger than $\Delta_{\text{ins}}(D)$, i.e., $\Delta_{\max}(D) > \Delta_{\text{ins}}(D)$.

Example 14.6 *In this example, we consider the degraded scalar Gaussian source and side information model which is defined in Example 14.3. Consequently, here, we have the Markov chain*

$$X_i \to Y_i \to Z_i, \quad i = 1, \ldots, n \tag{14.62}$$

Using Theorem 14.2 and Corollary 14.1, the maximum relative equivocation $\Delta_{\max}(D)$ *for the degraded scalar Gaussian model can be written as*

$$\Delta_{\max}(D) = I(X;Y) - I(X;Z) \tag{14.63}$$

as long as there is a V *satisfying* $\sigma^2_{X|VY} \leq D$.

Next, we obtain $\Delta_{\text{ins}}(D)$ for the degraded scalar Gaussian source and side information model.

Lemma 14.5

$$\Delta_{\text{ins}}(D) = \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(X;Y|V) - I(X;Z|V) \tag{14.64}$$

We now compare $\Delta_{\max}(D)$ and $\Delta_{\text{ins}}(D)$ as follows

$$\Delta_{\text{ins}}(D) - \Delta_{\max}(D) = \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(X;Y|V) - I(X;Z|V) - [I(X;Y) - I(X;Z)] \tag{14.65}$$

$$= \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(V;Z) - I(V;Y) \tag{14.66}$$

$$= \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} - I(V;Y|Z) \tag{14.67}$$

$$= - \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(V;Y|Z) \tag{14.68}$$

$$< 0 \tag{14.69}$$

where (14.67) follows from the Markov chain $V \to Y \to Z$ and (14.69) is due to Lemma 14.4. Hence, (14.69) implies that for the degraded scalar Gaussian source and side information model, the maximum relative equivocation cannot be achieved by an uncoded scheme, i.e., $\Delta_{\max}(D) > \Delta_{\text{ins}}(D)$.

Example 14.6 shows that in general, the maximum relative equivocation cannot be achieved by an uncoded scheme. In other words, even when there is no concern

on the transmission rate R that encoder uses, we still need to use a coded scheme to achieve the maximum relative equivocation at the eavesdropper.

14.7 Conclusions

In this chapter, we study the problem of secure lossy source coding with side information. Unlike the earlier works in [14, 112], and also our work in Chapter 13, which use the equivocation of the source at the eavesdropper as the secrecy measure, we formulate this problem under a new secrecy measure, namely the relative equivocation of the source at the eavesdropper with respect to the legitimate user. We argue that this new secrecy measure corresponds to the natural generalization of the equivocation in a wiretap channel to the context of secure lossy source coding. We obtain a single-letter description of the rate, relative equivocation and distortion region for the problem of secure lossy source coding with side information under this new secrecy measure. We specialize this single-letter expression to the degraded and reversely degraded cases. We also discuss the relationships between the optimal scheme attaining this region and the Wyner-Ziv scheme.

14.8 Appendix

14.8.1 Proof of Lemma 14.1

Let d_Y^n and d_Z^n denote the minimum achievable distortion by the legitimate user and the eavesdropper, respectively, for block-length n. First, we identify d_Y^n and d_Z^n. To

this end, we note that

$$E\left[d^n(X^n, \hat{X}^n(M, Y^n))\right] = \frac{1}{n}\sum_{i=1}^{n} E\left[d(X_i, \hat{X}_i(M, Y^n))\right] \tag{14.70}$$

$$= \frac{1}{n}\sum_{i=1}^{n}\sum_{x_i,m,y^n} p(x_i, m, y^n) d(x_i, \hat{x}_i(m, y^n)) \tag{14.71}$$

from which d_Y^n can be identified as

$$d_Y^n = \frac{1}{n}\sum_{i=1}^{n}\sum_{m,y^n}\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i} p(x_i, m, y^n) d(x_i, \hat{x}_i)\right] \tag{14.72}$$

Similarly, d_Z^n is given by

$$d_Z^n = \frac{1}{n}\sum_{i=1}^{n}\sum_{m,z^n}\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i} p(x_i, m, z^n) d(x_i, \hat{x}_i)\right] \tag{14.73}$$

Next, we show that if $X_i \to Y_i \to Z_i$, $d_Y^n \le d_Z^n$ which implies that $d_Y \le d_Z$. Using (14.73), we have

$$d_Z^n = \frac{1}{n}\sum_{i=1}^{n}\sum_{m,z^n}\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i} p(x_i, m, z^n) d(x_i, \hat{x}_i)\right] \tag{14.74}$$

$$= \frac{1}{n}\sum_{i=1}^{n}\sum_{m,z^n}\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i,y^n} p(x_i, m, y^n, z^n) d(x_i, \hat{x}_i)\right] \tag{14.75}$$

$$= \frac{1}{n}\sum_{i=1}^{n}\sum_{m,z^n}\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i,y^n} p(x_i, m, y^n) p(z^n|y^n) d(x_i, \hat{x}_i)\right] \tag{14.76}$$

$$\ge \frac{1}{n}\sum_{i=1}^{n}\sum_{m,z^n}\sum_{y^n}\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i} p(x_i, m, y^n) p(z^n|y^n) d(x_i, \hat{x}_i)\right] \tag{14.77}$$

$$= \frac{1}{n}\sum_{i=1}^{n}\sum_{m,z^n}\sum_{y^n} p(z^n|y^n)\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i} p(x_i, m, y^n) d(x_i, \hat{x}_i)\right] \tag{14.78}$$

$$= \frac{1}{n}\sum_{i=1}^{n}\sum_{m,y^n}\left[\min_{\hat{x}_i\in\hat{\mathcal{X}}}\sum_{x_i} p(x_i,m,y^n)d(x_i,\hat{x}_i)\right] \tag{14.79}$$

$$= d_Y^n \tag{14.80}$$

where (14.76) comes from the Markov chain $X_i \to Y_i \to Z_i$. The second statement of the lemma follows from the symmetry; completing the proof of Lemma 14.1.

14.8.2 Proof of Theorem 14.1

Here, we prove Theorem 14.1 in two steps. First, in the next section, we prove the achievability of the region $\mathcal{R}^*$ in Theorem 14.1 and in Section 14.8.2.2, we provide the converse proof.

14.8.2.1 Achievability

To show the achievability of the region $\mathcal{R}^*$ in Theorem 14.1, we use the coding scheme proposed in [14]. We fix the joint distribution $p(u,v|x) = p(v|x)p(u|v)$ and the reconstruction function $\hat{x}(v,y)$ such that $E\big[d(X,\hat{X}(V,Y))\big] \leq D/(1+\epsilon)$.

Codebook generation:

- Generate $2^{n(R_u+\tilde{R}_u)}$ u^n sequences through $p(u^n) = \prod_{i=1}^{n} p(u_i)$, and index them as $u^n(w_u,\tilde{w}_u)$, where $w_u \in \{1,\ldots,2^{nR_u}\}$ and $\tilde{w}_u \in \{1,\ldots,2^{n\tilde{R}_u}\}$.

- For each $u^n(w_u,\tilde{w}_u)$, generate $2^{n(R_v+\tilde{R}_v)}$ v^n sequences through $p(v^n|u^n) = \prod_{i=1}^{n} p(v_i|u_i)$, and index them as $v^n(w_u,\tilde{w}_u,w_v,\tilde{w}_v)$, where $w_v \in \{1,\ldots,2^{nR_v}\}$ and $\tilde{w}_v \in \{1,\ldots,2^{n\tilde{R}_v}\}$.

Encoding:

If x^n is the source sequence to be transmitted, find a u^n sequence such that (u^n, x^n) is jointly typical[3]. Due to the mutual covering lemma [118], if we have

$$R_u + \tilde{R}_u > I(U;X) \tag{14.81}$$

then there exists at least one such u^n sequence. Once such a u^n sequence is found, we find a v^n sequence such that (v^n, u^n, x^n) is jointly typical. Again, due to the mutual covering lemma [118], if we have

$$R_v + \tilde{R}_v > I(V;X|U) \tag{14.82}$$

then there exists at least one such v^n sequence. After finding these typical u^n, v^n sequences, the transmitter sends their first indices, i.e., w_u, w_v. Hence, the total transmission rate R is given by $R = R_u + R_v$.

Decoding and distortion:

After receiving w_u, w_v, the legitimate user decodes $\tilde{w}_u, \tilde{w}_v$ by using its side information. In particular, the legitimate user looks for the unique $\tilde{w}_u, \tilde{w}_v$ such that (u^n, v^n, y^n) is jointy typical. If the following constraints are satisfied

$$\tilde{R}_u < I(U;Y) \tag{14.83}$$

$$\tilde{R}_v < I(V;Y|U) \tag{14.84}$$

[3]Throughout the proof, we use the strong typicality as defined in [118].

the legitimate user can identify the (u^n, v^n) sequences with vanishingly small probability of error.

Once the legitimate user decodes the v^n sequence, it computes the reconstruction of the source x^n via $\hat{x}^n(v^n, y^n)$. The corresponding distortion can be computed as follows

$$E\left[d^n(X^n, \hat{X}^n)\right] \leq \Pr[\mathcal{E}]d_{max} + \Pr[\mathcal{E}^c]E\left[d^n(X^n, \hat{X}^n)|\mathcal{E}^c\right] \tag{14.85}$$

$$= \Pr[\mathcal{E}]d_{max} + \Pr[\mathcal{E}^c]\left(\frac{1}{n}\sum_{i=1}^{n} E\left[d(X_i, \hat{X}_i)|\mathcal{E}^c\right]\right) \tag{14.86}$$

$$\leq \Pr[\mathcal{E}]d_{max} + \Pr[\mathcal{E}^c](1+\epsilon)E\left[d(X, \hat{X})\right] \tag{14.87}$$

$$\leq \Pr[\mathcal{E}]d_{max} + \Pr[\mathcal{E}^c]D \tag{14.88}$$

where $d_{max} = \max_{(x^n, \hat{x}^n)\in\mathcal{X}^n\times\mathcal{X}^n} d^n(x^n, \hat{x}^n)$, $\mathcal{E}$ denotes the event that there is an error in either encoding or decoding. Equation (14.87) follows from the typical average lemma [118] in conjunction with the fact that if there is no error in encoding or decoding, then $(x^n, \hat{x}^n)$ is jointly typical, and (14.88) follows from the assumption that $E\big[d(X, \hat{X})\big] \leq D/(1+\epsilon)$. Equation (14.88) implies that if there is no error in encoding or decoding, then the reconstruction of the source within the distortion level D is possible.

Equivocation computation:

Finally, we consider the relative equivocation of this coding scheme. We first

obtain a lower bound for the equivocation of the eavesdropper as follows.

$$
\begin{aligned}
H(X^n|M,Z^n) &= H(X^n|W_u,W_v,Z^n) && (14.89)\\
&\geq H(X^n|W_u,W_v,Z^n,U^n) && (14.90)\\
&= H(X^n|W_v,Z^n,U^n) && (14.91)\\
&= H(X^n|U^n) - I(X^n;W_v,Z^n|U^n) && (14.92)\\
&= H(X^n|U^n) - I(X^n;Z^n|U^n) - I(X^n;W_v|U^n,Z^n) && (14.93)\\
&\geq H(X^n|U^n) - I(X^n;Z^n|U^n) - H(W_v) && (14.94)\\
&= H(X^n|U^n) - I(X^n;Z^n|U^n) - nR_v && (14.95)
\end{aligned}
$$

where (14.91) comes from the Markov chain $W_u \rightarrow U^n \rightarrow X^n, Z^n, W_v$. Next, we consider the equivocation at the legitimate user as follows.

$$
\begin{aligned}
H(X^n|M,Y^n) &= H(X^n|W_u,W_v,Y^n) && (14.96)\\
&\leq H(X^n,U^n,V^n|W_u,W_v,Y^n) && (14.97)\\
&= H(U^n,V^n|W_u,W_v,Y^n) + H(X^n|W_u,W_v,Y^n,U^n,V^n) && (14.98)\\
&\leq n\epsilon_{1n} + H(X^n|W_u,W_v,Y^n,U^n,V^n) && (14.99)\\
&= n\epsilon_{1n} + H(X^n|Y^n,U^n,V^n) && (14.100)\\
&= n\epsilon_{1n} + H(X^n|U^n) - I(X^n;Y^n,V^n|U^n) && (14.101)
\end{aligned}
$$

where $\epsilon_{1n} \rightarrow 0$ as $n \rightarrow \infty$, (14.99) comes from Fano's lemma by noting the fact that the legitimate user can decode (U^n, V^n) using the transmitted message W_u, W_v and

its side information Y^n, and (14.100) follows from the Markov chain $(W_u, W_v) \to (U^n, V^n) \to X^n, Y^n$. Combining (14.95) and (14.101) yields

$$\begin{aligned}
&H(X^n|M, Z^n) - H(X^n|M, Y^n) \\
&\geq I(X^n; Y^n, V^n|U^n) - I(X^n; Z^n|U^n) - nR_v - n\epsilon_{1n} && (14.102) \\
&= I(X^n; Y^n|U^n) + I(X^n; V^n|U^n, Y^n) - I(X^n; Z^n|U^n) - nR_v - n\epsilon_{1n} && (14.103) \\
&= I(X^n; Y^n|U^n) + I(X^n; V^n|U^n) - I(Y^n; V^n|U^n) - I(X^n; Z^n|U^n) - nR_v \\
&\quad - n\epsilon_{1n} && (14.104)
\end{aligned}$$

where (14.104) comes from the Markov chain $U^n \to V^n \to X^n \to Y^n$. Next, we introduce the following lemma.

Lemma 14.6 ([64, Lemma 3]) *Let T_1^n, T_2^n, T_3^n be length-n sequences satisfying $T_1^n \to T_2^n \to T_3^n$, and $\{(T_{1i}, T_{2i}, T_{3i})\}_{i=1}^n$ be i.i.d. tuples. We have*

$$\left| \frac{1}{n} I(T_1^n; T_2^n|T_3^n) - I(T_1; T_2|T_3) \right| \leq \gamma_n \tag{14.105}$$

where $\gamma_n \to 0$ as $n \to \infty$.

While [64] shows only the upper bound, following similar steps the lower bound in Lemma 14.6 can be established as well. Using Lemma 14.6 in (14.104), we get

$$\begin{aligned}
H(X^n|M, Z^n) - H(X^n|M, Y^n) \geq\ & nI(X; Y|U) + nI(X; V|U) - nI(Y; V|U) \\
& - nI(X; Z|U) - n\gamma_n - nR_v - n\epsilon_{1n} && (14.106)
\end{aligned}$$

Finally, we set the rate R_v as follows

$$R_v = I(X;V|U) - I(Y;V|U) + \beta \tag{14.107}$$

which, in view of (14.106), implies

$$H(X^n|M,Z^n) - H(X^n|M,Y^n) \geq nI(X;Y|U) - nI(X;Z|U) - n\beta - n\gamma_n - n\epsilon_{1n} \tag{14.108}$$

which completes the equivocation computation.

Thus, we have shown that if the following constraints are satisfied,

$$R_u + \tilde{R}_u > I(U;X) \tag{14.109}$$

$$R_v + \tilde{R}_v > I(V;X|U) \tag{14.110}$$

$$\tilde{R}_u < I(U;Y) \tag{14.111}$$

$$\tilde{R}_v < I(V;Y|U) \tag{14.112}$$

$$R_v = I(X;V|U) - I(Y;V|U) + \beta \tag{14.113}$$

this coding scheme enables the reconstruction of the source at the legitimate user within the distortion level D while achieving the relative equivocation rate of

$$I(X;Y|U) - I(X;Z|U) - \beta \tag{14.114}$$

at the eavesdropper. Eliminating $\tilde{R}_u, \tilde{R}_v$ from (14.109)-(14.113) in conjunction with

the fact that $R = R_u + R_v$ leads to $R > I(V;X) - I(V;Y) + \beta$; completing the proof.

14.8.2.2 Converse

Let (R, Δ, D) be an achievable tuple. Then, there exists an $(n, R + \epsilon)$ code such that

$$\lim_{n\to\infty} \frac{1}{n}\big[H(X^n|M, Z^n) - H(X^n|M, Y^n)\big] \geq \Delta - \epsilon \tag{14.115}$$

$$\lim_{n\to\infty} E[d^n(X^n, \hat{X}^n)] \leq D + \epsilon \tag{14.116}$$

We note that the joint distribution of (M, X^n, Y^n, Z^n) is given by

$$p(m, x^n, y^n, z^n) = p(m, x^n) \prod_{i=1}^{n} p(y_i, z_i|x_i) \tag{14.117}$$

Next, we define the following auxiliary random variables

$$U_i = MY^{i-1}Z_{i+1}^n \tag{14.118}$$

$$V_i = X_{i+1}^n Y_{i+1}^n U_i \tag{14.119}$$

which, due to the probability distribution in (14.117), satisfy the following Markov chain

$$U_i \to V_i \to X_i \to Y_i, Z_i, \quad i = 1, \ldots, n \tag{14.120}$$

A lower bound for the rate $(R+\epsilon)$ can be found as follows

$$n(R+\epsilon) \geq H(M) \geq \sum_{i=1}^{n} I(V_i;X_i) - I(V_i;Y_i) \tag{14.121}$$

by using the analysis in Section IV.B of [14].

The distortion level can be bounded as follows

$$\begin{aligned} E[d^n(X^n,\hat{X}^n)] &= E[d^n(X^n,\hat{X}^n(M,Y^n))] && (14.122)\\ &= \frac{1}{n}\sum_{i=1}^{n} E[d(X_i,\hat{X}_i(M,Y^n))] && (14.123)\\ &\geq \frac{1}{n}\sum_{i=1}^{n} E[d(X_i,\hat{X}_i(M,Y^n,Z_{i+1}^n,X_{i+1}^n))] && (14.124)\\ &= \frac{1}{n}\sum_{i=1}^{n} E[d(X_i,\hat{X}_i(V_i,Y_i))] && (14.125) \end{aligned}$$

where (14.122) comes from the fact that $\hat{X}^n$ is a function of M, Y^n, (14.124) is due to the fact that providing extra information for the reconstruction of the source cannot increase the distortion of the reconstructed sequence, and (14.125) comes from the definition of V_i in (14.119).

Finally, we consider the relative equivocation term as follows

$$\begin{aligned} H(X^n|M,Z^n) - H(X^n|M,Y^n) &= I(X^n;Y^n|M) - I(X^n;Z^n|M) && (14.126)\\ &= \sum_{i=1}^{n} I(X^n;Y_i|M,Y^{i-1}) - I(X^n;Z_i|M,Z_{i+1}^n) && (14.127) \end{aligned}$$

$$= \sum_{i=1}^{n} I(X^n; Y_i|M, Y^{i-1}) - I(X^n; Z_i|M, Z_{i+1}^n) + I(Z_{i+1}; Y_i|M, X^n, Y^{i-1})$$

$$- I(Y^{i-1}; Z_i|M, X^n, Z_{i+1}^n) \tag{14.128}$$

$$= \sum_{i=1}^{n} I(X^n, Z_{i+1}^n; Y_i|M, Y^{i-1}) - I(X^n, Y^{i-1}; Z_i|M, Z_{i+1}^n) \tag{14.129}$$

$$= \sum_{i=1}^{n} I(X^n; Y_i|M, Y^{i-1}, Z_{i+1}^n) + I(Z_{i+1}^n; Y_i|M, Y^{i-1}) - I(X^n; Z_i|M, Z_{i+1}^n, Y^{i-1})$$

$$- I(Y^{i-1}; Z_i|M, Z_{i+1}^n) \tag{14.130}$$

$$= \sum_{i=1}^{n} I(X^n; Y_i|M, Y^{i-1}, Z_{i+1}^n) - I(X^n; Z_i|M, Z_{i+1}^n, Y^{i-1}) \tag{14.131}$$

$$= \sum_{i=1}^{n} I(X^n; Y_i|U_i) - I(X^n; Z_i|U_i) \tag{14.132}$$

where (14.128) and (14.131) come from the Csiszar-Korner sum identity [3, Lemma 7].

Next, we note the following

$$I(X^n; Y_i|M, Y^{i-1}, Z_{i+1}^n) = H(Y_i|M, Y^{i-1}, Z_{i+1}^n) - H(Y_i|M, Y^{i-1}, Z_{i+1}^n, X^n) \tag{14.133}$$

$$= H(Y_i|M, Y^{i-1}, Z_{i+1}^n) - H(Y_i|M, Y^{i-1}, Z_{i+1}^n, X_i) \tag{14.134}$$

$$= I(X_i; Y_i|M, Y^{i-1}, Z_{i+1}^n) \tag{14.135}$$

where (14.134) comes from the following Markov chain

$$Y_i \to X_i \to MY^{i-1}Z_{i+1}^n X^{i-1} X_{i+1}^n \tag{14.136}$$

which follows from the probability distribution in (14.117). Similarly, we can get

$$I(X^n; Z_i|M, Y^{i-1}, Z_{i+1}^n) = I(X_i; Z_i|M, Y^{i-1}, Z_{i+1}^n) \tag{14.137}$$

Using (14.135) and (14.137) in (14.132), we get

$$H(X^n|M, Z^n) - H(X^n|M, Y^n) = \sum_{i=1}^{n} I(X_i; Y_i|U_i) - I(X_i; Z_i|U_i) \tag{14.138}$$

Finally, we define the uniformly distributed random variable $Q \in \{1, \ldots, n\}$ which is independent of all other random varaibles, and $U = (U_Q, Q), V = (V_Q, Q)$. Using these random variables in (14.121), (14.125), and (14.138), we can get the desired bounds given in Theorem 14.1.

Chapter 15

Conclusions

In this dissertation, we address whether wireless communications can be secured at the physical layer of communication by exploiting the unique characteristics of the wireless medium, without any recourse to higher-layer security protocols. Towards addressing this question, we study several fundamental multi-user channel models, inspired by wireless communication applications, by using information-theoretic techniques.

In Chapter 2, we study the Gaussian MIMO wiretap channel in which a common message is sent to both the legitimate user and the eavesdropper in addition to the private message sent only to the legitimate user. In this model, there is a secrecy concern on the private message, in that it needs to be kept hidden as much as possible from the eavesdropper. A single-letter description for the capacity-equivocation region of this channel model exists due to [3]. In Chapter 2, we show that it is sufficient to consider jointly Gaussian auxiliary random variables and channel input to evaluate this single-letter description of the capacity-equivocation region. Our result provides the most comprehensive description for the capacity-equivocation region of the Gaussian MIMO wiretap channel and generalizes all of the previous partial results.

In Chapter 3, we study the secure broadcasting problem, where a transmitter

wants to have secure communication with multiple legitimate users in the presence of an external eavesdropper. Characterizing the secrecy capacity region of this channel in its most general form seems to be intractable for now, since the version of this problem without any secrecy constraints, is the broadcast channel with an arbitrary number of receivers, whose capacity region is unknown. Consequently, we take the approach of considering special classes of channels. In particular, in Chapter 3, we consider degraded multi-receiver wiretap channels, parallel multi-receiver wiretap channels with a more noisy eavesdropper, parallel multi-receiver wiretap channels with less noisiness orderings in each sub-channel, and parallel degraded multi-receiver wiretap channels. For each channel model, we obtain either partial characterizations of the secrecy capacity region or the entire region.

In Chapter 4, we study the Gaussian MIMO broadcast channel with common and confidential messages where the transmitter sends a confidential message to each user that needs to be kept hidden from the other user, in addition a common message directed to both users. We obtain the entire capacity region of this channel model. In particular, we show that a combination of superposition coding and the S-DPC scheme proposed in [8] can attain the entire capacity region. In the converse proof of this capacity result, the channel enhancement technique [4] and an extremal inequality from [5] play important roles. In addition to this capacity result, in Chapter 4, we also establish a connection between the Gaussian MIMO broadcast channel with common and confidential messages and its non-confidential counterpart, i.e., the Gaussian MIMO broadcast channel with common and private messages, where there is no secrecy concern on the private messages. This connection

explains why while the capacity region of the Gaussian MIMO broadcast channel with common and private messages is not completely known, we are able to obtain the entire capacity region for its confidential counterpart.

In Chapter 5, we study the Gaussian MIMO multi-receiver wiretap channel where the transmitter sends a confidential message to each legitimate user in the presence of an external eavesdropper. We obtain the secrecy capacity region of this channel model. In particular, we show that the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel can be attained by a combination of dirty-paper coding with Gaussian signals and stochastic encoding. We prove this result in two main steps. In the first step, we consider the degraded Gaussian MIMO multi-receiver wiretap channel, for which there is a single-letter description of the secrecy capacity region. We propose a new technique to evaluate the single-letter description for the vector Gaussian model, using which, we obtain the secrecy capacity region of the degraded channel. In the second step, we consider arbitrary, not necessarily degraded, MIMO channels for which there is no single-letter description of the secrecy capacity region. Despite that, we obtain the secrecy capacity region of arbitrary, not necessarily degraded, MIMO channels by using the channel enhancement technique and some limiting arguments [4, 21]. We also demonstrate that our new technique to evaluate single-letter expressions for vector Gaussian models can be useful in other problems as well, by providing an alternative proof for the capacity region of the degraded Gaussian MIMO broadcast channel and an outer bound for the vector Gaussian CEO problem.

In Chapter 6, we study the multi-receiver wiretap channel with public and

confidential messages, which generalizes the channel model we consider in Chapters 3 and 5 by incorporating public messages without any secrecy constraints on them. We first consider the degraded discrete memoryless channel, and provide inner and outer bounds for its capacity region. We show that there are cases where these bounds match providing the capacity region. Second, we provide an inner bound for the capacity region of the general multi-receiver wiretap channel by using superposition coding, rate-splitting, binning and Marton's coding. Third, we consider the degraded Gaussian MIMO multi-receiver wiretap channel, and show that, to evaluate the proposed inner and outer bounds for the Gaussian MIMO case, it is sufficient to consider jointly Gaussian auxiliary random variables and channel input. Similar to the discrete degraded case, for the degraded Gaussian MIMO case also, these bounds match for certain cases. Finally, we consider the general Gaussian MIMO multi-receiver wiretap channel and propose an inner bound for its capacity region.

In Chapter 7, we study the *weak eavesdropper* MAC-WT. First, we develop an n-letter outer bound for the secrecy capacity region of this class of channels. This n-letter outer bound matches the achievable region partially. Although this partial matching gives us a limited characterization of the capacity region, since it is in an n-letter form, evaluation of this outer bound seems intractable. On the other hand, focusing on Gaussian channels, we evaluate a looser version of our bound which determines the secrecy capacity region along individual rates axes to within half bit per channel use irrespective of the channel parameters. Moreover, if the users' links to the legitimate user are orthogonal, we are able to determine the entire secrecy

capacity region to within half bit per channel use. We also demonstrate that our outer bounding technique can be applied to the IC-WT with strong interference.

In Chapters 8 and 9, we study the effects of cooperation on secrecy. In particular, in Chapter 8, we study the CRBC and propose an achievable secrecy rate region by using CAF. Evaluation of this achievable secrecy rate region for the Gaussian CRBC demonstrates that by means of cooperation, both users can have secure communication in a Gaussian CRBC although this is not possible in the underlying Gaussian broadcast channel, i.e., when we remove the cooperation links between the receivers. Hence, this example shows that cooperation can improve secrecy for the broadcast setting. In Chapter 9, we study the MAC-GF and propose an achievable scheme by using CAF. We evaluate this achievable scheme for the Gaussian MAC-GF, and show that both users can have secure communication with the receiver, although this is not possible without cooperation among the users.

The common theme in Chapters 8 and 9 is that user cooperation can increase secrecy, and, even an untrusted party can help. However, this improvement depends on the cooperative strategy. For instance, even though a decode-and-forward (DAF) based cooperation scheme can increase the rate, it cannot improve the secrecy, because in this case the cooperating party, which is also the eavesdropper, needs to decode the message it forwards. However, in CAF, we do not require the cooperating party to decode the message. In fact, in CAF, the cooperating party helps increase the rate of the main transmitter to levels which it itself cannot decode, hence improving the secrecy of the main transmitter-receiver pair against itself.

In Chapter 10, we study the two-user one-eavesdropper compound wiretap

channel. First, focusing on the discrete memoryless case, we provide a lower bound for the secrecy capacity, which is the best known lower bound. Next, we study the Gaussian MIMO instance of the aforementioned compound wiretap channel. For the Gaussian MIMO case, we propose an achievable secrecy rate by using DPC in the achievable scheme we provided for the discrete channel. We show that the resulting secrecy rate achieves at least half of the secrecy capacity. Finally, we consider a special class of two-user one-eavesdropper Gaussian MIMO compound wiretap channels and obtain its secrecy capacity.

In Chapter 11, we generalize the compound wiretap channel we study in Chapter 10 to a multi-user setting by studying the DCMRWC for two different communication scenarios. In the first scenario, the transmitter wants to send a confidential message to each group of users, where both messages are to be kept confidential from an eavesdropper. In the second scenario, the transmitter sends a confidential message to the users in the first group which is wiretapped by both the users in the second group and the eavesdroppers, and a different confidential message to the second group of users which is wiretapped by only the eavesdroppers. For both scenarios, we establish the secrecy capacity region for the general discrete memoryless channel model, the parallel channel model, and the Gaussian parallel channel model. For the Gaussian MIMO channel model, we obtain the secrecy capacity region when there is only one user in the second group, i.e., when there is only one weak user.

In Chapter 12, we study the two-user fading broadcast channel with confidential messages, where the transmitter sends a confidential message to each user that needs to be kept hidden from the other user. We obtain the ergodic secrecy capac-

ity region of the fading broadcast channel. Our result shows that fading enhances secrecy by enabling both users to have simultaneous secure communication with the transmitter, although this is not possible in the scalar non-fading broadcast channel, where only one of the two users can have secrecy. This simultaneous secrecy of both users is achieved by an opportunistic communication scheme, in which, at each time instant, the transmitter talks to the user having a better channel gain.

In Chapter 13, we study the secure lossy transmission of a vector Gaussian source to a legitimate user with some side information in the presence of an eavesdropper who also has some side information. By using the single-letter description of the rate-equivocation region, we obtain an outer bound for the rate-equivocation region of the vector Gaussian model at hand. We obtain this outer bound by optimizing the rate and equivocation constraints involved in the single-letter description individually. As a result of these individual optimizations, we obtain the maximum equivocation at the eavesdropper when there is no rate constraint on the transmitter to describe the source to the legitimate user. We show that, even in this case, where there is no rate constraint on the transmitter, an uncoded scheme cannot attain the maximum equivocation. Moreover, by using our maximum equivocation result, we show that, in general, Wyner-Ziv coding, which is optimal in the absence of an eavesdropper, is sub-optimal for the secure lossy source coding problem.

In Chapter 14, we revisit the secure lossy source coding problem, and propose a new secrecy measure, namely the relative equivocation of the source at the eavesdropper with respect to the legitimate user. We argue that this new secrecy measure partially overcomes the shortcomings of the previous ones (the equivocation of the

source at the eavesdropper used in [14, 112], and also in our work in Chapter 13, and the equivocation of the reconstructed source at the eavesdropper used in [117]) when one wants to quantify the relative confusion of the eavesdropper with respect to the legitimate user. We obtain the rate, relative equivocation and distortion region resulting from the use of this new secrecy measure in a single-letter form. We specialize this single-letter expression to the degraded and reversely degraded cases. We show that Wyner-Ziv scheme is not optimal in general, although, it is optimal for the degraded and reversely degraded cases as well as in the absence of an eavesdropper.

Bibliography

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.

[2] A. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[4] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Transactions on Information Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[5] H. Weingarten, T. Liu, , S. Shamai (Shitz), Y. Steinberg, and P. Viswanath, "The capacity region of the degraded multiple-input multiple-output compound broadcast channel," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.

[6] I. Csiszar and J. Korner, *Information theory: Coding theorems for discrete memoryless systems*. Cambridge University Press, 2011, 2nd Edition.

[7] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "The capacity-equivocation region of the MIMO Gaussian wiretap channel," in *IEEE International Symposium on Information Theory*, Jun. 2010.

[8] ——, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2011.

[9] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "On the capacity region of the multi-antenna broadcast channel with common messages," in *IEEE International Symposium on Information Theory*, Jul. 2006.

[10] H. Weingarten, "Multiple-input multiple-output broadcast systems," Ph.D. dissertation, Technion, Haifa, Israel, 2007.

[11] K. Marton, "A coding theorem for the discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 25, no. 1, pp. 306–311, May 1979.

[12] W. Yu and J. Cioffi, "Sum capacity of Gaussian vector broadcast channels," *IEEE Transactions on Information Theory*, vol. 50, no. 9, pp. 1875–1892, Sep. 2004.

[13] C. Nair and A. El Gamal, "The capacity region of a class of 3-receiver broadcast channels with degraded message sets," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.

[14] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," in *Allerton Conference on Communication, Control, and Computing*, Sep. 2010, also available at [arXiv: 1009.3891v1].

[15] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap chan-

nel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[16] A. Khisti and G. Wornell, "Secure transmission with multiple antennas-Part II: The MIMOME channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[17] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[18] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[19] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[20] J. Korner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Transactions on Information Theory*, vol. 23, no. 1, pp. 60–64, Jan. 1977.

[21] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[22] T. Cover and J. Thomas, *Elements of Information Theory.* Wiley & Sons, 2006, 2nd Edition.

[23] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "The secrecy rate region of the broadcast channel," in *Allerton Conference on Communication, Control, and Computing*, Sep. 2008, also available at [arXiv:0806.4200].

[24] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[25] E. Ekrem and S. Ulukus, "On secure broadcasting," in *Asilomar Conference on Signals, Systems, and Computers*, Oct. 2008.

[26] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470 – 2492, Jun. 2008.

[27] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Allerton Conference on Communication, Control, and Computing*, Sep. 2006, pp. 841–848.

[28] G. S. Poltyrev, "Capacity for a sum of certain broadcast channels," *Problemy Peredachi Informatsii*, vol. 15, no. 2, pp. 40–44, Apr.-Jun. 1979.

[29] A. El Gamal, "Capacity of the product and sum of two unmatched broadcast channels," *Problems of Information Transmission*, vol. 16, no. 1, pp. 3–23, Jan. 1980.

[30] A. J. Goldsmith and M. Effros, "The capacity region of broadcast channels with intersymbol interference and colored Gaussian noise," *IEEE Transactions on Information Theory*, vol. 47, no. 1, pp. 219–240, Jan. 2001.

[31] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential and common messages," in *IEEE International Symposium on Information Theory*, Jun. 2010, pp. 2578–2582.

[32] ——, "New results on multiple-input multiple-output broadcast channels with confidential messages," submitted to *IEEE Transactions on Information Theory*, Jan. 2009. Also available at [arXiv:1101.2007].

[33] E. Ekrem and S. Ulukus, "Gaussian MIMO broadcast channels with common and confidential messages," in *IEEE International Symposium on Information Theory*, Jun. 2010.

[34] N. Jindal and A. Goldsmith, "Optimal power allocation for parallel broadcast channels with independent and common information," in *IEEE International Symposium on Information Theory*, Jun. 2004, p. 215.

[35] J. Xu, Y. Cao, and B. Chen, "Capacity bounds for broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.

[36] S. H. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 3072–3081, Nov. 2001.

[37] S. Ihara, "On the capacity of channels with additive non-Gaussian noise," *Information and Control*, vol. 37, no. 1, pp. 34–39, Apr. 1978.

[38] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, vol. 2009, no. 142374, 2009.

[39] P. Bergmans, "A simple converse for broadcast channels with additive white Gaussian noise," *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 279–280, Mar. 1974.

[40] A. El Gamal, "EE478 Multiple user information theory," Lecture notes.

[41] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 623–656, Oct. 1948.

[42] A. J. Stam, "Some inequalities satisfied by the quantities of information of Fisher and Shannon," *Information and Control*, vol. 2, pp. 101–112, Jun. 1959.

[43] N. M. Blachman, "The convolution inequality for entropy powers," *IEEE Transactions on Information Theory*, vol. IT-11, no. 2, pp. 267–271, Apr. 1965.

[44] M. H. M. Costa, "A new entropy power inequality," *IEEE Transactions on Information Theory*, vol. 31, no. 6, pp. 751–760, Nov. 1985.

[45] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "A vector generalization of

Costa's entropy-power inequality with applications," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1865–1879, Apr. 2010.

[46] D. Guo, S. Shamai (Shitz), and S. Verdu, "Mutual information and minimum mean-square error in Gaussian channels," *IEEE Transactions on Information Theory*, vol. 51, no. 4, pp. 1261–1283, Apr. 2005.

[47] ——, "Estimation of non-Gaussian random variables in Gaussian noise: Properties of the MMSE," in *IEEE International Symposium on Information Theory*, Jul. 2008.

[48] O. Rioul, "Information theoretic proofs of entropy power inequalities," *IEEE Transactions on Information Theory*, vol. 57, no. 1, pp. 33–55, Jan. 2011.

[49] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[50] O. Johnson, *Information theory and the central limit theorem.* Imperial College Press, 2004.

[51] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information theoretic problems," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1839–1851, May 2007.

[52] D. P. Palomar and S. Verdu, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 141–154, Jan. 2006.

[53] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1985.

[54] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security*, vol. 2009(824235), 2009.

[55] ——, "An alternative proof for the capacity region of the degraded Gassign MIMO broadcast channel," *IEEE Transactions on Information Theory*, vol. 58, no. 4, pp. 2427–2433, Apr. 2012.

[56] A. Dembo, "Information inequalities and uncertainty principles," Technical Report, Department of Statistics, Stanford University, Stanford, CA., 1990.

[57] A. Dembo, T. M. Cover, and J. A. Thomas, "Information theoretic inequalities," *IEEE Transactions on Information Theory*, vol. 37, no. 6, pp. 1501–1518, Nov. 1991.

[58] E. Ekrem and S. Ulukus, "An outer bound for the vector Gassign CEO problem," submitted to *IEEE Transactions on Information Theory*, Jan. 2012. Also available at [arXiv:1202.0536].

[59] Y. Oohama, "Rate-distortion theory for Gaussian multiterminal source coding systems with several side informations at the decoder," *IEEE Transactions on Information Theory*, vol. 51, no. 7, pp. 2577–2593, Jul. 2005.

[60] V. Prabhakaran, D. Tse, and K. Ramchandran, "Rate region of the quadratic Gaussian CEO problem," in *IEEE International Symposium on Information Theory*, Jun. 2004, p. 119.

[61] A. B. Wagner and V. Anantharam, "An improved outer bound for multiterminal source coding," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 1919–1937, May 2008.

[62] S.-Y. Tung, "Multiterminal source coding," Ph.D. dissertation, Cornell University, Ithaca, NY, 1978.

[63] A. El Gamal and E. C. van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless channels," *IEEE Transactions on Information Theory*, vol. 27, no. 1, pp. 120–122, Jul. 1980.

[64] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[65] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5747–5755, Dec. 2008.

[66] ——, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[67] M. H. M. Costa and A. El Gamal, "The capacity region of the discrete memoryless interference channel with strong interefence," *IEEE Transactions on Information Theory*, vol. IT-33, no. 5, pp. 710–711, Sep. 1987.

[68] A. Carleial, "A case where interference does not reduce capacity," *IEEE Transactions on Information Theory*, vol. IT-21, no. 5, pp. 569–570, Sep. 1975.

[69] X. He and A. Yener, "Secure degrees of freedom for Gaussian channels with interference: Structured codes outperform Gaussian signalling," in *IEEE Global Communications Conference*, Dec. 2009.

[70] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "On the secure degrees of freedom of the multiple access wiretap channel," in *IEEE International Symposium on Information Theory*, Jun. 2010.

[71] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Allerton Conference on Communications, Control and Computing*, Sep. 2008.

[72] M. Madiman and A. Barron, "Generalized entropy power inequalities and monotonicity properties of information," *IEEE Transactions on Information Theory*, vol. 53, no. 7, pp. 2317–2329, Jul. 2007.

[73] Y. Oohama, "Relay channels with confidential messages," submitted to *IEEE Transactions on Information Theory,* Mar. 2007. Also available at [arXiv:0611125].

[74] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," in *Asilomar Conference on Signals, Systems, and Computers*, Nov. 2007.

[75] ——, "The role of an untrusted relay in secret communication," in *IEEE International Symposium on Information Theory*, Jul. 2008.

[76] ——, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[77] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[78] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Conference on Information Sciences and Systems*, Mar. 2007.

[79] M. Bloch and A. Thangaraj, "Confidential messages to a cooperative relay," in *IEEE Information Theory Workshop*, May 2008.

[80] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. IT-25, no. 5, pp. 572–584, Sep. 1979.

[81] M. H. M. Costa, "Writing on dirty paper," *IEEE Transactions on Information Theory*, vol. IT-29, no. 3, pp. 439–441, May 1983.

[82] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parametres," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[83] R. Tanniuos and A. Nosratinia, "Relay channels with private messages," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3777–3785, Oct. 2007.

[84] H. Sato, "An outer bound to the capacity region of broadcast channels," *IEEE Transactions on Information Theory*, vol. IT-24, no. 3, pp. 374–377, May 1978.

[85] Y. Liang and G. Kramer, "Rate regions for relay broadcast channel," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3517–3535, Oct. 2007.

[86] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[87] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *IEEE International Symposium on Information Theory*, Jul. 2006.

[88] L. Ong and M. Motani, "Coding strategies for multiple-access channels with feedback and correlated sources," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3476–3497, Oct. 2007.

[89] M. A. Khojastepour, A. Sabharwal, and B. Aazhang, "Improved achievable rates for user cooperation and relay channels," in *IEEE International Symposium on Information Theory*, Jun. 2004.

[90] H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," *IEEE Transactions on Information Theory*, vol. 35, no. 3, pp. 572–578, May 1989.

[91] ——, "A coding theorem for secret sharing communication systems with two Gaussian wiretap channels," *IEEE Transactions on Information Theory*, vol. 37, no. 3, pp. 634–638, May 1991.

[92] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *IEEE International Symposium on Information Theory*, Jun. 2007, pp. 1301–1305.

[93] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 28, no. 5, pp. 2748–2765, May 2012.

[94] T. Liu, V. Prabhakaran, and S. Viswanath, "The secrecy capacity of a class of parallel Gaussian compound wiretap channels," in *IEEE International Symposium on Information Theory*, Jul. 2008, pp. 116–120.

[95] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[96] Z. Li, R. Yates, and W. Trappe, "Secret communication with a fading eavesdropper channel," in *IEEE International Symposium on Information Theory*, Jun. 2007, pp. 1296 – 1300.

[97] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[98] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *IEEE International Symposium on Information Theory*, Sep. 2005, pp. 2152–2155.

[99] G. Caire, G. Taricco, and E. Biglieri, "Optimal power control over fading channels," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1468–1489, Jul. 1999.

[100] D. Gunduz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *IEEE Information Theory Workshop*, May 2008.

[101] ——, "Lossless compression with security constraints," in *IEEE International Symposium on Information Theory*, Jul. 2008.

[102] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *IEEE Information Theory Workshop*, Sep. 2007.

[103] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," in *Allerton Conference on Communication, Control, and Computing*, Oct. 2009.

[104] ——, "Secure source coding with a helper," submitted to *IEEE Transactions on Information Theory*, Oct. 2009.

[105] W. Luh and D. Kundur, "Distributed keyless secret sharing over noiseless channels," in *IEEE Global Communications Conference*, 2007.

[106] L. Grokop, A. Sahai, and M. Gastpar, "Discriminatory source coding for a noiseless broadcast channel," in *IEEE International Symposium on Information Theory*, 2005.

[107] P. Cuff, "A framework for partial secrecy," in *IEEE Global Communications Conference*, Dec. 2010.

[108] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Transactions on Information Theory*, vol. 29, no. 6, pp. 918–923, Nov. 1983.

[109] ——, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Transactions on Information Theory*, vol. 34, no. 4, pp. 835–842, Jul. 1988.

[110] ——, "Rate-distortion theory for the Shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[111] N. Merhav, "On the Shannon cipher system with a capacity-limited key-distribution channel," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1269–1273, Mar. 2006.

[112] ——, "Shannon's secrecy system with informed receivers and its applications to systematic coding for wiretapped channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2723–2734, Jun. 2008.

[113] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.

[114] H. V. Poor, *An Introduction to Signal Detection and Estimation*. Springer, 1994, 2nd Edition.

[115] K. B. Petersen and M. S. Petersen, *The Matrix Cookbook*, 2008, available at http://matrixcookbook.com.

[116] R. W. Newcomb, "On the simultaneous diagonalization of two semi-definite matrices," *Quarterly of Applied Mathematics*, vol. 19, pp. 144–146, 1961.

[117] N. Merhav, "On joint coding for watermarking and encryption," *IEEE Transactions on Information Theory*, vol. 52, no. 1, pp. 190–205, Jan. 2006.

[118] A. El Gamal and Y. H. Kim, *Network Information Theory*. Cambridge University Press, 2012.