ABSTRACT

Title of dissertation: INFORMATION THEORETIC GENERATION OF MULTIPLE SECRET KEYS

Chunxuan Ye, Doctor of Philosophy, 2005

Dissertation directed by: Professor Prakash Narayan
Department of Electrical and Computer Engineering
and Institute for System Research

This dissertation studies the problem of secret key generation for encrypted group communication in a network, based on an information theoretic approach. This approach, which relies on a provable form of security, also provides suggestions for key constructions.

We examine the problem of the simultaneous generation of multiple keys by different groups of terminals intended for encrypted group communication, in certain *three-terminal source models*, which capture the salient features of general multiterminal models. We characterize the rates at which two designated pairs of terminals can simultaneously generate *private* keys, each of which is effectively concealed from the remaining terminal, and the rates at which the following two types of keys can be generated simultaneously: (i) all the three terminals generate a (common) *secret* key, which is effectively concealed from an eavesdropper; and (ii) a designated pair of terminals generate a private key, which is effectively concealed from the remaining terminal as well as the eavesdropper.

Furthermore, we develop an approach for the construction of a new class of provably secure secret keys by terminals in several simple multiterminal source models, which exploits innate connections between secret key generation and multiterminal Slepian-Wolf near-lossless data compression (sans secrecy restrictions). Implementations of these con-

structions using low density parity check (LDPC) channel codes are illustrated.

INFORMATION THEORETIC GENERATION OF MULTIPLE SECRET KEYS

by

Chunxuan Ye

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
2005

Advisory Committee:

Professor Prakash Narayan, Chair/Advisor
Professor Alexander Barg
Professor Armand M. Makowski
Professor Adrian Papamarcou
Professor Steven A. Tretter
Professor Lawrence C. Washington
Professor Min Wu

This dissertation is dedicated to my parents, my wife and my daughter.

ACKNOWLEDGMENTS

My special thanks go to my advisor, Professor Prakash Narayan. His technical expertise and continual stimulation, which he communicated to me in many long meetings, proved to be helpful during this research work. Being a student with Professor Narayan has been a very rewarding experience, not only because of his profound knowledge on information theory, but also for his involvement and care for his student.

I am also grateful to all members of my dissertation advisory committee, including Dr. Alexander Barg, Dr. Armand M. Makowski, Dr. Adrian Papamarcou, Dr. Steven A. Tretter, Dr. Lawrence C. Washington and Dr. Min Wu.

I would like to acknowledge all my friends for their help and companionship. Specially, I am grateful to Dr. Damianos Karakos, Dr. Kaushik Chakraborty and Dr. Onur Kaya for many illuminating conversations in helping me to formulate my research ideas. I am also indebted to visiting scholar, Dr. Imre Csiszár for stimulating discussions on various subjects.

I express my deepest gratitude to my family, to whom I dedicate this thesis. I am especially indebted to my parents Chao Ye and Yafen Lu, who have always stood by me and guided me through my study, and have pulled me through against impossible odds at times. I devote my endless gratitude to my wife Sijia for her everlasting encouragement and support when I needed so. My never ending gratitude will also be devoted to my daughter Daisy, who has brought me a lot of laugh during my study.

I gratefully acknowledge that this research was supported by DARPA under Grant

N66001-00-C-8063 and by the National Science Foundation under Grant 010119-7136.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

1.1 Background

Encryption and Authentication

Encryption refers to the translation of data into an encoded format for the purpose of achieving data security. Reading an encrypted file requires access to a key, which enables its decryption. The two primary encryption schemes used in most existing cryptographic systems are symmetric encryption and asymmetric encryption, and often occur in combination to perform complementary functions. In a symmetric cryptosystem, a single common key (termed secret key) is used for encryption and decryption, while in an asymmetric cryptosystem, two different keys are employed: a public key for encryption and a private key for decryption. Examples of widely-used symmetric cryptosystems include the *data encryption standard* (DES), the Triple-DES, the *advanced encryption standard* (AES), RC4, etc. [47], [48]. Examples of widely-used asymmetric cryptographic algorithms are the RSA scheme, the ElGamal scheme, etc. [18], [19], [53].

One advantage of an asymmetric cryptosystem is that it provides security in a wide range of applications (e.g., digital signatures) that cannot be provided by using only symmetric techniques. However, an asymmetric cryptosystem typically executes computationally heavy and complex operations which need powerful hardware. Also, large keys, with sizes ranging from 512 to 4096 bits, are needed for an asymmetric cryptosystem to achieve sufficient, lasting security. For instance, the current RSA cryptosystem uses keys of length 1024 bits [30].

On the other hand, a symmetric cryptosystem typically performs simple, efficiently executable algorithms which require relatively inexpensive hardware. The secret keys used in a symmetric cryptosystem are of small size, usually ranging from 40 to 256 bits (e.g., 56 bits for the DES cryptosystem). In addition, a symmetric cryptosystem is well suited for networks in which communication takes the form of broadcasts, e.g., over a wireless RF medium. For instance, consider the situation in which a sensor node attempts to securely broadcast a message to all the other sensor nodes in a sensor network. If a symmetric cryptosystem is deployed in this sensor network, then the transmitting sensor node could use its secret key to encrypt the message, which could be decrypted separately by all the other sensor nodes using the same secret key. Such a simple operation is not feasible in an asymmetric cryptosystem. On the other hand, of course, even if a single sensor is compromised along with its secret key, then the security of the entire network is at risk if this secret key remains in use. (See Section 1.2 below on "Generation of Multiple Secret Keys in a Symmetric Cryptosystem.")

Message authentication is the process of using a key or key pair to verify the origin of a message and its integrity (cf. e.g., [61]). Most existing message authentication schemes are based on a digital signature which uses a key pair, or based on a *message authentication code* (MAC) which uses a single key (cf. e.g., [55]). A MAC is a short piece of information, which is attached to a message for the purpose of authenticating the message. A MAC algorithm (sometimes termed a keyed hash function) accepts as input a message as well as a secret key, and produces a MAC for the message using a suitable hash function; the authenticity of the message can be verified by using the same secret key.

Network Applications of Symmetric Cryptosystems

The symmetric encryption and authentication technologies mentioned above have a wide range of applications in architectures and protocols for network security. For example, consider IPSec, which is the security architecture for the *Internet protocol* (IP). Its security objectives include data authentication and guaranteeing confidentiality of packets in their entirety. MACs and symmetric encryption are extensively used in various protocols of IPSec, e.g., the *authentication header* (AH) protocol and the *encapsulating security payload* (ESP) protocol. Analogously, many link layer security protocols (e.g. the *point-to-point protocol* (PPP), the *Point-to-point tunneling protocol* (PPTP), the *layer 2 tunneling protocol* (L2TP), etc.) and many transport layer security protocols (e.g., the *secure socket layer* (SSL) protocol and the *secure shell* (SSH) protocol) take advantage of MACs and symmetric cryptographic algorithms for the purpose of authentication and encryption.

Wireless communication networks have additional security issues, which are not present in wired networks. Such issues arise, for instance, in handover, which entails switching a connection of a mobile phone from one base station to another and which is a common phenomenon in GSM and CDMA wireless networks (cf. e.g., [28], [46]); MACs are used in the authentication of mobile phones to base stations during handover.

1.2 Motivation

Secret Key Establishment in a Symmetric Cryptosystem

Although symmetric cryptosystems are feasible in many network settings, the main difficulty in deploying them in a network lies in secret key establishment among different communicating terminals. In an asymmetric cryptosystem, only the encryption keys, or public keys, should be dispersed among different communicating terminals. Since an encryption key does not need to be kept secret, its distribution is relatively simple. *Public-*

key infrastructure (PKI) frameworks, such as X.509 and *Pretty Good Privacy* (PGP) (cf. e.g., [8], [59]), are designed for public key distribution to avoid falsification and abuse.

In contrast, secret key establishment in a symmetric cryptosystem among different communicating terminals is fraught with difficulties, since a secret key must be protected from eavesdropping. There are two basic types of secret key establishment procedures in symmetric cryptosystems: *secret key distribution* and *secret key generation* (cf. e.g., [59]).

In a secret key distribution protocol, one communicating terminal determines a secret key and transmits it to all the other terminals. Traditional methods of secret key distribution depend on a trusted third party, or *key distribution center* (KDC). Specifically, the task of a KDC is to securely spread a secret key among communicating terminals. However, such a KDC is often burdened with extensive key management and can become a bottleneck. Additionally, a KDC itself is an attractive target for an eavesdropper.

Most existing secret key distribution protocols rely on certain asymmetric cryptographic algorithms (e.g., RSA) (cf. e.g., [55]). Specifically, a secret key is encrypted with the recipient's public key before its distribution. This hybrid use of symmetric and asymmetric cryptographic algorithms (i.e., encrypting a message by a secret key and encrypting the secret key by the recipient's public key) could overcome the inefficiency of an asymmetric cryptosystem and the difficulty in secret key distribution in a symmetric cryptosystem.

In a secret key generation protocol, on the other hand, no communicating terminal knows a secret key in advance, and a secret key is generated as a result of negotiation by the terminals. Most current secret key generation protocols are based on the Diffie-Hellman key exchange algorithm (cf. e.g., [55]), which is an asymmetric cryptographic algorithm.

Thus, asymmetric cryptographic algorithms play an important role in secret key establishment for most existing symmetric cryptosystems. However, we shall see from the discussion below that the security of such asymmetric cryptographic algorithms is based on the undesirable assumption that an eavesdropper's computational power is restricted. In this dissertation, we shall focus on the central problem of secret key generation by different communicating terminals in a symmetric cryptosystem.

Computational Complexity Theoretic Security and Information Theoretic Security

If the security of a cryptosystem relies on the difficulty in solving a computational problem, then this notion of security is called *computational complexity theoretic security.* For instance, the security of the RSA cryptosystem is based on the (unproved) difficulty in factoring large integers, and the security of many other cryptosystems is based on the (unproved) difficulty in computing discrete logarithms in certain groups [18]. (For more examples of this notion of security, see [26].)

The notion of computational complexity theoretic security relies on the assumption that an eavesdropper's computational power is restricted and that the eavesdropper lacks "efficient algorithms." However, with the development of efficient algorithms for factoring large integers and computing discrete logarithms in certain groups (e.g., quadratic sieve, elliptic curve method, etc., [8]), as well as advances in fast integer factorization using quantum computing [7], the difficulty in solving such computational problems might be significantly reduced.

On the other hand, if the security of a cryptosystem can be rigorously established without any assumption of limits on an eavesdropper's computational power, this notion of security is called *information theoretic security* or *unconditional security.* A cryptographic model based on the notion of information theoretic security guarantees that legitimate plaintext messages and secret keys are, in effect, nearly “statistically independent” of the information of the eavesdropper. This notion is clearly desirable in a cryptosystem, as it makes no assumption of limited computational power for eavesdropper. However, no practical cryptosystem based on the notion of information theoretic security has been designed. In this dissertation, we shall address information theoretic models of secret key generation in a symmetric cryptosystem.

Generation of Multiple Secret Keys in a Symmetric Cryptosystem

The use of a single secret key by all the communicating terminals in a symmetric cryptosystem may pose the following security threat: some of these communicating terminals may be compromised or become unauthorized (e.g., when they depart from the system), along with the (single) secret key, whereby the security of the cryptosystem is breached. For example, a *basic service set* (BSS) (cf. e.g., [6], [55]) in a 802.11 wireless local area network is a set of mobile units using the same radio frequency; a subset of mobile units in a BSS may cease to be reliable when they are disabled. Hence, the secret key assigned to them, in effect, is compromised. The remaining authorized mobile units should then be capable of maintaining security by switching to another secret key which is concealed from the disabled mobile units.

This leads to a situation in which *multiple secret keys must be devised in a coordinated manner by different groups of communicating terminals* (with possible overlaps of groups); such keys need protection from prespecified communicating terminals as also from the eavesdropper. In the interests of efficiency, the assignment of separate secret keys to different groups of communicating terminals must be made at the outset of operations so as to avoid the need for a fresh key generation procedure after a disablement. This dissertation will study the problem of simultaneous generation of multiple secret keys for different groups of communicating terminals.

1.3 Prior Work

Secret Key Generation over Insecure Noisy Channels

A secret key (SK) can be determined at one terminal and transmitted over a secure channel to other terminals. But in more complex ways, a SK can be generated by using insecure noisy channels. For example, in Wyner's "wiretap channel" model [64] which involves two legitimate terminals, one terminal sends information to the other terminal over a discrete memoryless channel, subject to a wiretap at the receiver. The wiretapper sees a noisy version of the receiver's signal. Wyner proved that in such a setting, a SK can be generated by the legitimate terminals. Subsequently, Csiszár and Körner [14] considered SK generation in a discrete memoryless broadcast channel in which a terminal sends information to another terminal over a discrete memoryless channel, called the legitimate channel, while a wiretapper observes the transmitted information through another discrete memoryless channel, called the wiretap channel. Unlike Wyner's wiretap channel model, in this setting, the wiretapped signal is not necessarily a degraded version of the legitimate signal.

Secret Key Generation over Noiseless Public Channels

A SK can be generated by separate terminals, in a different manner from that above, based on their observations of separate but correlated signals followed by public communication among themselves. Such a situation can arise, for instance, in a satellite broadcasting situation, which can provide for correlated signals to be received at different terminals through separate noisy channels with a common input; these terminals can then communicate over a noiseless public channel to generate a SK. Maurer [36], and Ahlswede and Csiszár [3] considered SK generation in various *source models* and *channel models*. In a source model, two or more terminals initially observe the outputs of an experiment (e.g., bits broadcast by a satellite) over separate secure noisy channels. Hence, their observations are correlated, but not necessarily identical. Based on their observations, these terminals exchange information over a noiseless public channel in order to generate a SK. In a channel model, a (central) terminal transmits information to the other terminals through a secure channel with limited capacity. Additionally, these terminals are allowed to communicate over a noiseless public channel which is observed by an eavesdropper, for the purpose of SK generation. Subsequently, much work [5], [9], [13], [16]-[17], [37]-[43], [51], [62] has been devoted to the study of SK generation at two terminals in various source and channel models.

In the recent work of Csiszár and Narayan [17], the authors consider source models consisting of an arbitrary number of terminals which respectively observe distinct correlated sources followed by unrestricted public communication among themselves; a subset of the terminals can also serve as "helpers" for the remaining terminals in generating secrecy. The notion of helpers can be interpreted in terms of a trusted third party in a key establishment protocol, which assists "user" terminals in SK generation, by providing them with additional correlated information. A SK generated by a set of user terminals with assistance – in the form of additional correlated information – from a set of helper terminals, requires concealment from an eavesdropper with access to the public communication, but not from the assisting helper terminals. A private key (PK)[1] generated by

[1] This terminology should not be confused with the decryption key in an asymmetric cryptosystem. The "private key" used hereafter will refer to a special kind of secret key.

the user terminals must be additionally protected from the assisting helper terminals. It is shown in [17] that the SK-capacity, i.e., the largest (entropy) rate at which all the user terminals can generate a SK, is obtained by subtracting from the maximum rate of shared common randomness (CR) achievable by these user terminals (i.e., information to which all the user terminals are privy with probability close to 1), the smallest sum-rate of the data-compressed interterminal communication which enables each of the terminals to acquire this maximal CR.

Secret Key Construction[2]

It should be noted that all of the work mentioned above is aimed at characterizing the secrecy capacities, of different varieties. In contrast to so many characterizations of the SK-capacities, few construction schemes for SK generation have yet been proposed. Two exceptions are the following.

In the recent work of Thangaraj *et al* [58], the authors propose a new approach to constructing SKs for Wyner's wiretap channel model. The authors prove that by using a channel code which achieves the capacity of the wiretap channel, a SK with rate close to SK-capacity can be constructed. The other work is due to Muramatsu [45], in which the author considers the problem of SK construction in a two-terminal source model. Specifically, it is proved that a SK can be extracted by means of a *linear* transformation of the CR shared by the terminals acquired through public discussion.

[2] The work on secret key construction refers to the explicit construction schemes for secret key generation.

1.4 Overview of Dissertation

It should be stressed that in all of the work mentioned in Section 1.3, the terminals are required to devise *only a single key*, to be used subsequently for secure encrypted communication. There are, however, situations, arising for instance in group communication, in which multiple keys must be simultaneously generated by different groups of terminals. The first main problem studied in this dissertation is the simultaneous generation of multiple keys by different groups of terminals in several source models.

The second main problem studied in this dissertation involves construction schemes for secrecy generation in several simple source models. These constructions are motivated by innate connections between secrecy generation by multiple terminals and multiterminal data compression of correlated sources not involving any secrecy constraints, recently highlighted in [17]. This suggests that techniques for multiterminal Slepian-Wolf (SW) near-lossless[3] data compression could be used for the constructions of SKs. In SW coding, the existence of linear lossless data compression codes with rates arbitrarily close to the SW bound has been long known [12]. In particular, when the sequences observed at the terminals are related to each other through virtual communication channels characterized by independent additive noises, such linear data compression codes can be obtained in terms of the cosets of linear error-correction codes for these virtual channels, a fact first illustrated in [63] for the special case of two terminals connected by a virtual binary symmetric channel. This fact, exploited by most known linear constructions of SW codes (cf. e.g. [10], [23], [32], [50]), can enable us to translate these constructions and other significant recent developments in capacity-achieving linear codes into new SK constructions.

[3] In the interests of avoiding repeated hyphenation, we shall hereafter use “lossless” in lieu of the correct “near-lossless,” which should not lead to any confusion.

This dissertation consists of three parts. In the first part (Chapters 2 and 3), we discuss the problem of simultaneous generation of multiple keys by different groups of terminals for three-terminal source models. Suppose that terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ observe, respectively, the distinct components of a discrete memoryless multiple source (DMMS), i.e., independent and identically distributed (i.i.d.) repetitions of the generic random variables (rvs) X, Y, Z with a known joint probability mass function (pmf). Unrestricted communication among the terminals is allowed over a noiseless public channel, and all the transmissions are observed by all the terminals. An eavesdropper has access to this public communication but gathers no additional side information. Furthermore, the eavesdropper is passive, i.e., unable to corrupt the transmissions[4].

In Chapter 2, we examine the problem of characterizing all the rates at which two designated pairs of terminals can simultaneously generate PKs, each of which is effectively concealed from the remaining terminal. In the three-terminal source model above, we assume that terminals $\mathcal{X}$ and $\mathcal{Y}$ (resp. $\mathcal{X}$ and $\mathcal{Z}$) generate a PK with the possible help of terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) which is concealed from the helper terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) and from an eavesdropper with access to the public communication among the terminals. Such a situation can be interpreted in terms of a "central" terminal $\mathcal{X}$ establishing individual PKs with each terminal $\mathcal{Y}$ (resp. $\mathcal{Z}$) with the remaining terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) serving as helper. The set of all rate pairs at which such PK pairs can be generated constitutes the PK-capacity region. The characterization of the PK-capacity region is given in Chapter 2.

In Chapter 3, we examine the problem of characterizing all the rates at which the

[4] Throughout this dissertation, we shall only consider cases where the communication has been authenticated, i.e., the eavesdropper is passive.

following two types of keys can be generated *simultaneously*: (i) all the three terminals generate a SK, which is effectively concealed from an eavesdropper; and (ii) a designated pair of terminals generate a PK, which is effectively concealed from the remaining terminal as well as the eavesdropper. In the three-terminal source model above, we assume that terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ generate a SK. Simultaneously, terminals $\mathcal{X}$ and $\mathcal{Y}$ generate a PK, with the possible help of terminal $\mathcal{Z}$. Such a situation can be interpreted in terms of "core" terminals $\mathcal{X}$ and $\mathcal{Y}$ establishing a PK with terminal $\mathcal{Z}$ serving as helper, and all the terminals establishing a SK. The set of all rate pairs at which such (SK, PK) pairs can be generated is called the (SK, PK)-capacity region. The characterization of the (SK, PK)-capacity region is given in Chapter 3.

In the second part (Chapter 4), we discuss the problem of SK and PK constructions by multiple terminals. We consider several simple multiterminal source models where the sources observed at different terminals are connected by virtual additive noise channels. We show how a new class of SKs and PKs can be constructed, based on the SW data compression code (i.e., a data compression code with rate close to the SW bound) from [63]. Explicit procedures for such constructions, and their substantiation, are provided. In particular, we examine the performance of low density parity check (LDPC) codes, a class of linear capacity-achieving channel codes, in the SW data compression step of the procedure, in constructing a new class of SKs with rates arbitrarily close to the SK-capacity.

In the last part (Chapter 5), we study the relationship between the CR-capacity and the SK-capacity for source models with rate constraints on the public communication. It follows from the previous discussion that if unrestricted public communication is allowed among the terminals in source models, then the CR-capacity, i.e., the largest rate of

CR that is achieved by the terminals, can be decomposed into the smallest sum-rate of the communication needed to achieve the CR-capacity, and the SK-capacity. In Chapter 5, we consider several two-terminal source models with rate constraints on the public communication between these terminals. We study the relationship between the SK-capacity and the CR-capacity for these models. Specifically, we examine whether the CR-capacity is equal to the sum of the smallest sum-rate of communication needed to achieve the CR-capacity and the SK-capacity.

Finally, Chapter 6 summarizes the dissertation and discusses future work.

1.5 Contributions

The main contributions of this dissertation are as follows.

(i). Single-letter inner and outer bounds for the PK-capacity region are derived for a model with three terminals which observe separate correlated sources, when two pairs of terminals simultaneously generate PKs after public communication among themselves. We further prove that under certain special conditions, these bounds coincide to yield the (exact) PK-capacity region. This is the first work on the simultaneous generation of multiple PKs. It constitutes a generalization of the work on the generation of a single PK [3], [16], [17].

(ii). Single-letter inner and outer bounds for the (SK, PK)-capacity region are derived for a model with three terminals which observe separate correlated sources, when all the terminals generate a SK, and a designated pair of terminals generate a PK, all in a simultaneous manner. We further prove that under a certain condition, these bounds coincide to yield the (exact) (SK, PK)-capacity region. This is the first work on the simultaneous generation of a SK and a PK. It constitutes a generalization of the work on the generation of a single SK or PK [3], [16], [17].

(iii). A new approach is proposed for constructing SKs and PKs by terminals in several simple multiterminal source models where the sources are connected by virtual additive noise channels. We prove that the generated SKs and PKs satisfy the requisite secrecy conditions, and the rates of the generated SKs and PKs approach the corresponding SK-capacities or PK-capacities. Furthermore, implementations of these constructions schemes using LDPC codes are illustrated.

(iv). For several two-terminal source models with rate constraints on the public communication between these terminals, it is proved that the CR-capacity equals the sum of the smallest sum-rate of the communication needed to achieve the CR-capacity, and the SK-capacity. These initial results suggest that the decomposition of the CR-capacity into the SK-capacity, and the smallest sum-rate of the communication needed to achieve the CR-capacity, could hold for a larger class of source models consisting of multiple terminals with rate constraints on their public communication.

Chapter 2

The Private Key Capacity Region for Three Terminals

2.1 Introduction

The problem of secret key generation by separate terminals, based on their observations of distinct correlated sources followed by public communication among themselves, has been investigated by several authors ([36], [3], [5], [9], [13], [16]–[17], [37]–[43], [51], [62], among others). It is shown that these terminals can generate common randomness which is kept secret from an eavesdropper that is privy to the public interterminal communication and sometimes also to a wiretapped source which is correlated with the previous sources.

In the wake of [36], models for secrecy generation by two terminals have been widely studied. Of particular interest to us is the recent work in [17], which considers models consisting of an arbitrary number of terminals which respectively observe the distinct components of a discrete memoryless multiple source, followed by unrestricted public communication among themselves; a subset of the terminals can also serve as "helpers" for the remaining terminals in generating secrecy. Three varieties of secrecy capacity – the largest rate of secrecy generation – are considered according to the extent of an eavesdropper's knowledge: *secret key, private key* and *wiretap secret key* capacity. A secret key (SK) generated by a set of "user" terminals with assistance – in the form of additional correlated information – from a set of helper terminals (e.g., centralized or trusted servers in a key establishment protocol), requires concealment from an eavesdropper with access to the public interterminal communication. A private key (PK) generated by the user terminals must be additionally protected from the assisting helper terminals. A wiretap secret key[1] (WSK) must satisfy the even more stringent requirement of being protected from a resourceful eavesdropper's access to a wiretapped correlated source. It should be stressed that in all of the work mentioned above, the user terminals are required to devise *only a single key*, of any variety, to be used subsequently for secure encrypted communication.

There are, however, situations, arising for instance in "group communication," in which *multiple keys must be simultaneously devised in a coordinated manner by different groups of terminals* (with possible overlaps of groups); such keys need protection from prespecified terminals as also from an eavesdropper. Such a situation can occur when certain disabled terminals cease to be authorized or reliable so that the keys assigned to them, in effect, are compromised; the remaining authorized terminals must then be capable of maintaining security by switching to another set of keys which are concealed from the disabled terminals. In the interests of efficiency, all such keys must be devised at the outset of operations so as to avoid the need for a fresh key generation procedure after a disablement. These situations produce a rich vein of secrecy generation problems, the information-theoretic underpinnings of which are substantial enough for investigation already in the case of just three terminals. Various types of secrecy generation (as in [17]) can then be studied for different subsets of the three terminals.

Considering a model with three terminals, our emphasis in this chapter is on the problem of characterizing all the rates at which two pairs of terminals can simultaneously generate PKs, each of which is effectively concealed from the remaining terminal. The general problem of PK generation for all three pairs of terminals is briefly addressed towards

[1] The capacity problem associated with a wiretap secret key is not fully resolved even in the case of two user terminals, and we do not consider it here.

the end. Suppose that terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ observe, respectively, the distinct components of a discrete memoryless multiple source (DMMS), i.e., independent and identically distributed (i.i.d.) repetitions of the (generic) random variables (rvs) X, Y, Z, respectively. For the purposes of secrecy generation, the terminals are permitted unrestricted communication among themselves over a public channel, and all the transmissions are observed by all the terminals. An eavesdropper has access to this public communication but gathers no additional side information; also, the eavesdropper is passive, i.e., unable to corrupt the transmissions. Terminals $\mathcal{X}$ and $\mathcal{Y}$ (resp. $\mathcal{X}$ and $\mathcal{Z}$) generate a PK with the possible help of terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) which is concealed from the helper terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) and from an eavesdropper with access to the public communication among the terminals. Our main technical results are single-letter inner and outer bounds for the PK-capacity region, i.e., the set of all rate pairs at which such PK pairs can be generated. Further, under certain special conditions on the joint probability mass function (pmf) of X, Y, Z, these bounds are shown to coincide to yield the (exact) PK-capacity region.

All our results for the PK-capacity region hold in a strong sense; specifically, achievability results are established under a "strong" requirement and converse results under a "weak" requirement. While the weak and strong definitions of secrecy capacity have been shown to yield identical results for various models [37], [13], [16], [40], [17], it is worth mentioning that our technique leads directly to strong achievability.

This chapter is organized as follows. Section 2.2 contains the preliminaries. Our main results – inner and outer bounds for the PK-capacity region – are provided in Section 2.3. Furthermore, under certain special conditions, these bounds coincide to yield the (exact) PK-capacity region. Section 2.3 also contains several examples of the PK-capacity region. The proofs are given in Section 2.4. In Section 2.5, we examine the general problem of characterizing all the rates at which all pairs of terminals can simultaneously generate PKs.

2.2 Preliminaries

Consider a DMMS with three components corresponding to generic rvs X, Y, Z with finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$. Let $X^n = (X_1, \cdots, X_n)$, $Y^n = (Y_1, \cdots, Y_n)$, $Z^n = (Z_1, \cdots, Z_n)$ be n i.i.d. repetitions of the rvs X, Y, Z. The terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ [2] respectively observe the components X^n, Y^n, Z^n of the DMMS (X^n, Y^n, Z^n), where n denotes the observation length. The terminals can communicate with each other through broadcasts over a noiseless public channel, possibly interactively in many rounds. Following [17], we assume without any loss of generality that these transmissions occur in consecutive time slots in r rounds; the communication is depicted by $3r$ rvs $F_1, \cdots, F_{3r}$, where F_t denotes the transmission in time slot t, $1 \leq t \leq 3r$, by a terminal assigned an index $i = t \bmod 3$, $1 \leq i \leq 3$, with terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ corresponding to indices 1, 2, 3, respectively. In general, F_t is allowed to be any function, defined in terms of a mapping f_t, of the observations at the terminal with index i and of the previous transmissions $F_{[1,t-1]} = (F_1, \cdots, F_{t-1})$; thus, for instance, $F_1 = f_1(X^n)$, $F_2 = f_2(Y^n, F_1)$, $F_3 = f_3(Z^n, F_1, F_2)$, and so on. We do not permit any randomization at the terminals; in particular, $f_1, \cdots, f_{3r}$ are deterministic mappings. Let $\mathbf{F} = (F_1, \cdots, F_{3r})$ denote collectively all the transmissions in the $3r$ time slots.

Given $\varepsilon > 0$ and the rvs U, V, we say that U is *ε-recoverable* from V if $\Pr\{U \neq f(V)\} \leq \varepsilon$ for some function $f(V)$ of V (cf. [17]).

[2] The use of the same symbol for a terminal as well as for the alphabet of its observations should not lead to any confusion.

The rvs $K_{\mathcal{X}\mathcal{Y}}$ and $K_{\mathcal{X}\mathcal{Z}}$, which are functions of (X^n, Y^n, Z^n), with finite ranges $\mathcal{K}_{\mathcal{X}\mathcal{Y}}$ and $\mathcal{K}_{\mathcal{X}\mathcal{Z}}$, respectively, represent an *ε-private key* (ε*-PK*) pair, where $K_{\mathcal{X}\mathcal{Y}}$ (resp. $K_{\mathcal{X}\mathcal{Z}}$) is the PK for terminals $\mathcal{X}$, $\mathcal{Y}$ (resp. $\mathcal{X}$, $\mathcal{Z}$) with privacy from the terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$), achievable with communication $\mathbf{F}$, if:

- $K_{\mathcal{X}\mathcal{Y}}$ is ε-recoverable from each of $(\mathbf{F}, X^n)$, $(\mathbf{F}, Y^n)$;
- $K_{\mathcal{X}\mathcal{Z}}$ is ε-recoverable from each of $(\mathbf{F}, X^n)$, $(\mathbf{F}, Z^n)$;
- $K_{\mathcal{X}\mathcal{Y}}$ satisfies the secrecy condition and the uniformity condition

$$\frac{1}{n} I(K_{\mathcal{X}\mathcal{Y}} \wedge \mathbf{F}, Z^n) \leq \varepsilon; \tag{2.1}$$

$$\frac{1}{n} H(K_{\mathcal{X}\mathcal{Y}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}}| - \varepsilon;$$

and

- $K_{\mathcal{X}\mathcal{Z}}$ satisfies the secrecy condition and the uniformity condition

$$\frac{1}{n} I(K_{\mathcal{X}\mathcal{Z}} \wedge \mathbf{F}, Y^n) \leq \varepsilon; \tag{2.2}$$

$$\frac{1}{n} H(K_{\mathcal{X}\mathcal{Z}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{X}\mathcal{Z}}| - \varepsilon.$$

The conditions above thus mean that terminals $\mathcal{X}$ and $\mathcal{Y}$ generate a PK $K_{\mathcal{X}\mathcal{Y}}$ with the terminal $\mathcal{Z}$ acting as helper (e.g., a “third-party” in a key establishment protocol) by providing $\mathcal{X}$, $\mathcal{Y}$ with additional correlated information; this PK is nearly uniformly distributed, and is concealed from an eavesdropper that observes the public communication $\mathbf{F}$ as well as from the helper $\mathcal{Z}$ (and, hence, “private”). Simultaneously, *with the same public communication*, terminals $\mathcal{X}$ and $\mathcal{Z}$ generate a PK $K_{\mathcal{X}\mathcal{Z}}$ with the terminal $\mathcal{Y}$ acting as helper; this PK is nearly uniformly distributed, and is concealed from an eavesdropper as well as from the helper $\mathcal{Y}$. Note that the previous conditions readily imply that $K_{\mathcal{X}\mathcal{Y}}$ and $K_{\mathcal{X}\mathcal{Z}}$ are “nearly” statistically independent.

We remark that this model can be interpreted in terms of a "central" terminal $\mathcal{X}$ establishing individual PKs with each terminal $\mathcal{Y}$ (resp. $\mathcal{Z}$) with the remaining terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$) serving as helper. We are interested in the *simultaneous generation* of individual PK pairs ($K_{\mathcal{XY}}$, $K_{\mathcal{XZ}}$) as above.

Definition 2.1 *A pair of nonnegative numbers ($R_{\mathcal{XY}}$, $R_{\mathcal{XZ}}$) is an achievable PK-rate pair if ε_n-PK pairs $\left(K_{\mathcal{XY}}^{(n)}, K_{\mathcal{XZ}}^{(n)}\right)$ are achievable with suitable communication (with the number of rounds possibly depending on n), such that $\varepsilon_n \to 0$, $\frac{1}{n}H\left(K_{\mathcal{XY}}^{(n)}\right) \to R_{\mathcal{XY}}$, $\frac{1}{n}H\left(K_{\mathcal{XZ}}^{(n)}\right) \to R_{\mathcal{XZ}}$. The set of all achievable PK-rate pairs is the PK-capacity region C_{PK}. An achievable PK-rate pair will be called strongly achievable if ε_n above can be taken to vanish exponentially in n. A PK-capacity region will be termed strong if all rate pairs in that region are strongly achievable.*

Remarks:

1. Maurer [37] pointed out that the secrecy conditions (2.1), (2.2) were inadequate for cryptographic purposes, and should be strengthened by omission of the factor $\frac{1}{n}$. Note that the concept of strong achievability above, which is adopted from [16], [17], demands even more. All our achievability results will be proved as strong achievability results.

2. The (strong) PK-capacity region is a closed convex set. Closedness is obvious from the definition. Convexity follows from a standard time-sharing argument (cf. [15, p. 242]).

3. If $K_{\mathcal{XZ}}^{(n)}$ is set equal to a constant in the definition above, i.e., only a single ε_n-PK is generated by terminals $\mathcal{X}$ and $\mathcal{Y}$ with terminal $\mathcal{Z}$ serving as a helper terminal, then the entropy rate of such a PK is called *achievable PK-rate*, and the largest achievable PK-rate is the *PK-capacity*. An achievable PK-rate is called *strongly achievable PK-rate* if ε_n vanishes exponentially in n. A PK-capacity is termed *strong* if all smaller rates are

strongly achievable. It is known (cf. [3], [16]) that the (strong) PK-capacity is equal to $I(X \wedge Y|Z)$.

2.3 Statement of Results

Theorem 2.1 *(Outer bound for C_{PK}): Let $(R_{\mathcal{XY}}, R_{\mathcal{XZ}})$ be an achievable PK-rate pair. Then*

$$R_{\mathcal{XY}} \leq I(X \wedge Y|Z), \qquad R_{\mathcal{XZ}} \leq I(X \wedge Z|Y), \tag{2.3}$$

$$R_{\mathcal{XY}} + R_{\mathcal{XZ}} \leq \min_{U} I(X \wedge Y, Z|U), \tag{2.4}$$

where the minimum is over all rvs U that satisfy the Markov conditions

$$U -\circ- Y -\circ- XZ, \quad U -\circ- Z -\circ- XY. \tag{2.5}$$

Remarks:

1. The bounds in (2.3) on the individual largest achievable PK-rates are already known from the *single* PK results in [3], [16].

2. The minimum in (2.4) is attainable, since by a direct application of the Support Lemma [15, p. 310], the rv U in (2.4) can be assumed, without restricting generality, to take values in a set $\mathcal{U}$ of cardinality $|\mathcal{U}| \leq |\mathcal{Y}| \cdot |\mathcal{Z}| + 1$.

Definition 2.2 *A common function of Y and Z is any rv which equals both a function of Y and a function of Z; a maximal common function $U_{mcf(Y,Z)}$ of Y and Z is such that every other common function of Y and Z is a function of $U_{mcf(Y,Z)}$ (cf. e.g.,* [16], [22]*). The rvs Y and Z are deterministically correlated if there exists a common function of Y and Z which renders them conditionally independent (cf.* [15, p. 405]*).*

Proposition 2.1 *If there exists a common function of Y and Z which renders them conditionally independent, then that common function is a maximal common function of Y and Z.*

Proof of Proposition 2.1: Let U be a common function of Y and Z such that

$$I(Y \wedge Z|U) = 0. \tag{2.6}$$

Let U' be an arbitrary common function of Y and Z. Then

$$I(Y \wedge Z|U) \geq I(U' \wedge Z|U) = H(U'|U) - H(U'|U, Z) = H(U'|U). \tag{2.7}$$

It follows from (2.6) and (2.7) that U' is a function of U, which implies that U is a maximal common function of Y and Z. ■

An example of a maximal common function is given below.

Example 2.1: Let Y and Z be $\{0, 1, 2\}$-valued rvs with joint pmf

$$P_{YZ}(0, 0) = P_{YZ}(0, 1) = a,$$

$$P_{YZ}(1, 2) = P_{YZ}(2, 2) = \frac{1}{2} - a,$$

for some $0 < a < \frac{1}{2}$.

A rv U, as a function of Y, is defined as follows:

$$U = \begin{cases} 0, & \text{if } Y = 0, \\ 1, & \text{if } Y \in \{1, 2\}. \end{cases}$$

Equivalently, U can also be defined as:

$$U = \begin{cases} 0, & \text{if } Z \in \{0, 1\}, \\ 1, & \text{if } Z = 2. \end{cases}$$

Hence, U is a common function of Y and Z. It is easily seen that $Y -\!\!\circ\!\!- U -\!\!\circ\!\!- Z$. Therefore, Y and Z are deterministically correlated. Furthermore, by Proposition 2.1, U is a maximal common function of Y and Z. ■

Since $U_{mcf(Y,Z)}$ satisfies the two Markov conditions in (2.5), we have the following corollary of Theorem 2.1.

Corollary 2.1 *(Outer bound for C_{PK}): Any achievable PK-rate pair $(R_{\mathcal{X}\mathcal{Y}}, R_{\mathcal{X}\mathcal{Z}})$ satisfies (2.3) and*

$$R_{\mathcal{X}\mathcal{Y}} + R_{\mathcal{X}\mathcal{Z}} \leq I(X \wedge Y, Z | U_{mcf(Y,Z)}).$$

Theorem 2.2 *(Inner bound for C_{PK}): The (strong) PK-capacity region C_{PK} is inner-bounded by the convex hull of the union of the regions*

$$\left\{ \begin{array}{ll} (R_{\mathcal{X}\mathcal{Y}}, R_{\mathcal{X}\mathcal{Z}}): & R_{\mathcal{X}\mathcal{Y}} \leq \max_{U:\ U -\!\circ\!- Y -\!\circ\!- XZ} [I(X \wedge Y|U) - I(Y \wedge Z|U)], \\ & R_{\mathcal{X}\mathcal{Z}} \leq I(X \wedge Z|Y) \end{array} \right\} \tag{2.8}$$

and

$$\left\{ \begin{array}{ll} (R_{\mathcal{X}\mathcal{Y}}, R_{\mathcal{X}\mathcal{Z}}): & R_{\mathcal{X}\mathcal{Y}} \leq I(X \wedge Y|Z), \\ & R_{\mathcal{X}\mathcal{Z}} \leq \max_{V:\ V -\!\circ\!- Z -\!\circ\!- XY} [I(X \wedge Z|V) - I(Y \wedge Z|V)] \end{array} \right\}. \tag{2.9}$$

Remarks:

1. The maxima in (2.8) and (2.9) are attainable, since by a direct application of the Support Lemma [15, p. 310], the rvs U, V in (2.8) and (2.9) can be assumed, without restricting generality, to take values in sets $\mathcal{U}$, $\mathcal{V}$ of cardinalities $|\mathcal{U}| \leq |\mathcal{Y}| + 1$ and $|\mathcal{V}| \leq |\mathcal{Z}| + 1$.

2. Although interterminal communication between $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ is permitted, the regions in (2.8) and (2.9) are shown to be achieved by a single autonomous transmission from each terminal based on its own local observation of its component of the DMMS.

Note that $U = V = U_{mcf(Y,Z)}$ are permissible choices in (2.8) and (2.9). Hence, it follows from (2.8) and (2.9) that

$$\Big(I(X \wedge Y|U_{mcf(Y,Z)}) - I(Y \wedge Z|U_{mcf(Y,Z)}),\ I(X \wedge Z|Y)\Big) \tag{2.10}$$

and

$$\Big(I(X \wedge Y|Z),\ I(X \wedge Z|U_{mcf(Y,Z)}) - I(Y \wedge Z|U_{mcf(Y,Z)})\Big) \tag{2.11}$$

are two strongly achievable rate pairs. Since the sum of the two coordinates in (2.10) as well as in (2.11) equals $I(X \wedge Y, Z|U_{mcf(Y,Z)}) - I(Y \wedge Z|U_{mcf(Y,Z)})$, the following corollary is obtained from the strong achievability of rate pairs (2.10), (2.11), and the convexity of the (strong) PK-capacity region.

Corollary 2.2 *(Inner bound for C_{PK}): The (strong) PK-capacity region C_{PK} is inner-bounded by the region*

$$\left\{ \begin{array}{ll} (R_{\mathcal{XY}}, R_{\mathcal{XZ}}): & R_{\mathcal{XY}} \leq I(X \wedge Y|Z), \quad R_{\mathcal{XZ}} \leq I(X \wedge Z|Y), \\ & R_{\mathcal{XY}} + R_{\mathcal{XZ}} \leq I(X \wedge Y, Z|U_{mcf(Y,Z)}) - I(Y \wedge Z|U_{mcf(Y,Z)}) \end{array} \right\}.$$

The gap between the inner bound in Corollary 2.2 and the outer bound in Corollary 2.1 is $I(Y \wedge Z|U_{mcf(Y,Z)})$ for the sum of two individual PK-rates in a PK-rate pair. Figure 2.1 shows both these inner and outer bounds.

The following notion will be used in describing another inner bound for the PK-capacity region.

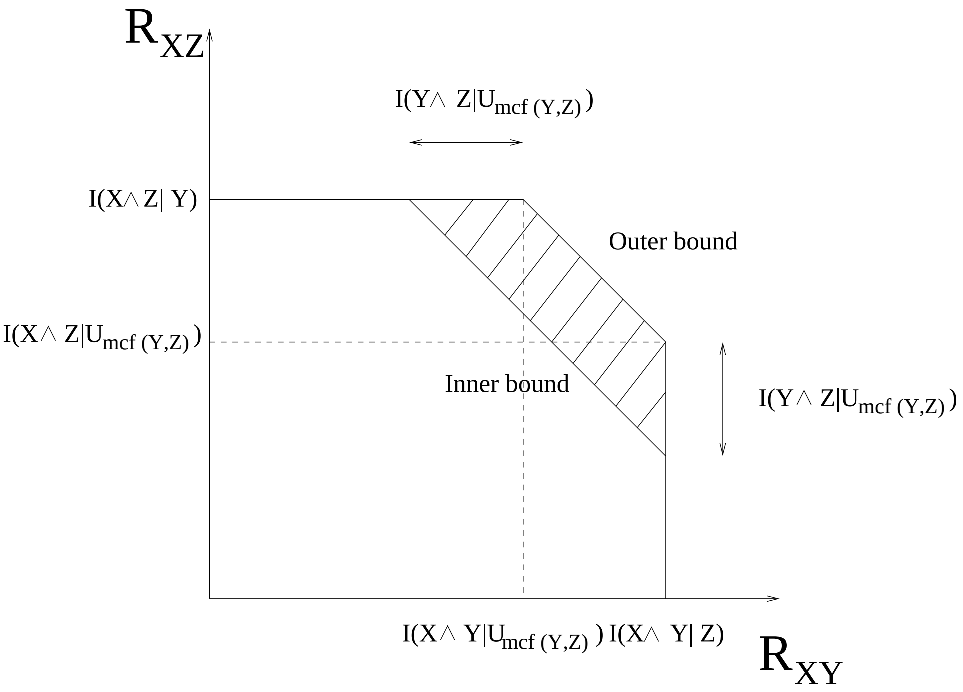


Figure 2.1: Inner and outer bounds for the PK-capacity region.

Definition 2.3 (cf. [11])*: A function of Y is a sufficient statistic for Y with respect to (w.r.t.) Z if it renders Y and Z conditionally independent; such a sufficient statistic is a minimal sufficient statistic $U_{mss(Y)}$ for Y w.r.t. Z if it is a function of every other sufficient statistic for Y w.r.t. Z.*

Theorem 2.3 *(Inner bound for C_{PK}): The (strong) PK-capacity region C_{PK} is inner-bounded by the convex hull of the union of the regions*

$$\left\{ \begin{array}{c} (R_{\mathcal{XY}}, R_{\mathcal{XZ}}): \quad 0 \le R_{\mathcal{XY}} \le I(X \wedge Y|U_{mss(Y)}, Z), \quad 0 \le R_{\mathcal{XZ}} \le I(X \wedge Z|Y), \\ R_{\mathcal{XY}} + R_{\mathcal{XZ}} \le I(X \wedge Y, Z|U_{mss(Y)}) \end{array} \right\} \tag{2.12}$$

and

$$\left\{ \begin{array}{c} (R_{\mathcal{XY}}, R_{\mathcal{XZ}}): \quad 0 \le R_{\mathcal{XY}} \le I(X \wedge Y|Z), \quad 0 \le R_{\mathcal{XZ}} \le I(X \wedge Z|V_{mss(Z)}, Y), \\ R_{\mathcal{XY}} + R_{\mathcal{XZ}} \le I(X \wedge Y, Z|V_{mss(Z)}) \end{array} \right\}, \tag{2.13}$$

where $U_{mss(Y)}$ (resp. $V_{mss(Z)}$) is the minimal sufficient statistic for Y (resp. Z) w.r.t. Z (resp. Y).

Remark: Although interterminal communication between $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ is permitted, the regions in (2.12) and (2.13) are shown to be achieved by a single autonomous transmission from each terminal based on its own local observation of its component of the DMMS.

Next, under a special (sufficient) condition below, the outer bound in Theorem 2.1 coincides with the inner bound in Theorem 2.2, thereby giving a complete characterization of the PK-capacity region under this condition.

Theorem 2.4 *If there exists a rv U such that*

$$U -\!\!\circ\!\!- Y -\!\!\circ\!\!- XZ, \qquad U -\!\!\circ\!\!- Z -\!\!\circ\!\!- XY, \qquad Y -\!\!\circ\!\!- U -\!\!\circ\!\!- Z, \tag{2.14}$$

the (strong) PK-capacity region equals the set of pairs ($R_{\mathcal{XY}}$, $R_{\mathcal{XZ}}$) which satisfy (2.3) and

$$R_{\mathcal{XY}} + R_{\mathcal{XZ}} \leq \min_{U} I(X \wedge Y, Z|U), \tag{2.15}$$

where the minimum is w.r.t. U satisfying (2.14).

Remarks:

1. As in Theorem 2.1, the minimum in (2.15) is shown to be attained (cf. Remark 2 following Theorem 2.1).

2. The rv U satisfying all three Markov conditions in (2.14) simultaneously need not always exist, as shown in Example 2.2 below.

Definition 2.4 (cf. [15, p. 350])*: Let (Y, Z) be $\mathcal{Y} \times \mathcal{Z}$-valued rvs with a given joint pmf. The joint pmf of (Y, Z) is called indecomposable if there are no functions f and g with respective domains $\mathcal{Y}$ and $\mathcal{Z}$ such that* $\Pr\{f(Y) = g(Z)\} = 1$ *and $f(Y)$ takes at least two values with nonzero probability.*

Remark: It should be noted that if $\Pr\{Y = y, Z = z\} > 0$ for all $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$, then the joint pmf of (Y, Z) is indecomposable (cf. [2]).

Example 2.2: Let Y and Z be $\{0, 1\}$-valued rvs with joint pmf

$$P_{YZ}(0,0) = P_{YZ}(1,1) = \frac{1-p}{2},$$

$$P_{YZ}(0,1) = P_{YZ}(1,0) = \frac{p}{2},$$

for some $0 < p < 1$, $p \neq \frac{1}{2}$.

Suppose that U is an arbitrary rv satisfying the first two Markov conditions in (2.14), whereby

$$U \multimap\!\!- Y \multimap\!\!- Z, \quad U \multimap\!\!- Z \multimap\!\!- Y.$$

Since $P_{YZ}(y, z) > 0$, $y, z \in \{0, 1\}$, the joint pmf of (Y, Z) is indecomposable. Then by [15, p. 402], U is independent of (Y, Z). Consequently,

$$I(Y \wedge Z|U) = I(Y \wedge Z) = 1 - h_b(p) > 0,$$

where $h_b(p) = -p \log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function. Thus, the last Markov condition in (2.14) does not hold. Therefore, in this example, no rv U can satisfy all three Markov conditions in (2.14). ■

The special case in which Y and Z are deterministically correlated is of particular interest as then the bounds for the PK-capacity region in Theorem 2.1, Corollary 2.1, Theorem 2.2, Corollary 2.2, Theorem 2.3, as well as the characterization in Theorem 2.4, all coincide to yield a complete characterization, as argued next. By Proposition 2.1, $I(Y \wedge Z|U_{mcf(Y,Z)}) = 0$, so that the gap disappears between the inner bound in Corollary 2.2 and the outer bound in Corollary 2.1. Hence, all the bounds in Theorem 2.1, Corollary 2.1, Theorem 2.2 and Corollary 2.2 coincide to yield the PK-capacity region. Furthermore, in this special case, the inner bound in Theorem 2.3 also gives the PK-capacity region since

$$U_{mss(Y)} = V_{mss(Z)} = U_{mcf(Y,Z)}, \tag{2.16}$$

which is easily seen as follows. On the one hand,

$$0 = I(Y \wedge Z | U_{mss(Y)}) \geq I(U_{mcf(Y,Z)} \wedge Z | U_{mss(Y)}) = H(U_{mcf(Y,Z)} | U_{mss(Y)}),$$

and

$$0 = I(Y \wedge Z | V_{mss(Z)}) \geq I(U_{mcf(Y,Z)} \wedge Z | V_{mss(Z)}) = H(U_{mcf(Y,Z)} | V_{mss(Z)}),$$

i.e., $U_{mcf(Y,Z)}$ is a common function of $U_{mss(Y)}$ and $V_{mss(Z)}$. On the other hand, $I(Y \wedge Z | U_{mcf(Y,Z)}) = 0$ gives that $U_{mcf(Y,Z)}$ is a sufficient statistic for Y w.r.t. Z as well as for Z w.r.t. Y, thereby implying that both $U_{mss(Y)}$ and $V_{mss(Z)}$ are functions of $U_{mcf(Y,Z)}$. Thus, (2.16) follows. Lastly, since $U = U_{mcf(Y,Z)}$ satisfies (2.14) and can be easily seen to achieve the minimum in (2.15), the PK-capacity region of Theorem 2.4 is the same as that alluded to above. These observations lead to the following summary result.

Theorem 2.5 *If the rvs Y and Z are deterministically correlated, the (strong) PK-capacity region C_{PK} equals the set of pairs ($R_{\mathcal{XY}}$, $R_{\mathcal{XZ}}$) which satisfy (2.3) and*

$$R_{\mathcal{XY}} + R_{\mathcal{XZ}} \leq I(X \wedge Y, Z | U_{mcf(Y,Z)}),$$

where $U_{mcf(Y,Z)}$ is the maximal common function of Y and Z.

Example 2.3: Let Y and Z be independent rvs, each uniformly distributed on $\{0, 1\}$, and let $X = Y \oplus Z$, where $\oplus$ denotes addition modulo 2. Since Y and Z are independent, $U_{mcf(Y,Z)}$ is a constant. Further, Y and Z are deterministically correlated. It follows from Theorem 2.5 that the PK-capacity region is the set of pairs $(R_{\mathcal{XY}}, R_{\mathcal{XZ}})$ satisfying

$$R_{\mathcal{XY}} + R_{\mathcal{XZ}} \leq I(X \wedge Y, Z | U_{mcf(Y,Z)}) = 1.$$

This PK-capacity region is triangular. The two corner points, $(0, 1)$ and $(1, 0)$, can be perfectly achieved (i.e., with $\varepsilon_n = 0$), which implies, from a time-sharing argument, that all PK-rate pairs in this region could be perfectly achieved. To achieve the corner point $(1, 0)$, terminal $\mathcal{Z}$ transmits $\mathbf{F} = Z^n = z^n$. Upon receiving z^n, terminal $\mathcal{X}$ recovers y^n perfectly, which is set to be $K_{\mathcal{X}\mathcal{Y}}$. It is clear that

$$I(K_{\mathcal{X}\mathcal{Y}} \wedge \mathbf{F}, Z^n) = I(Y^n \wedge Z^n) = 0,$$

and

$$\frac{1}{n} H(K_{\mathcal{X}\mathcal{Y}}) = \frac{1}{n} H(Y^n) = 1.$$

Therefore, a perfect PK, of rate 1 bit/symbol, is generated by terminals $\mathcal{X}$ and $\mathcal{Y}$. By symmetry, the other corner point $(0, 1)$ can also be perfectly achieved. ■

Example 2.4: Let $Y = (Y_1, N)$ and $Z = (Z_1, N)$, where Y_1, Z_1, and N are mutually independent. Let the joint pmf of (X, Y_1, Z_1, N) satisfy

$$I(Y_1 \wedge Z_1 | X, N) > 0, \tag{2.17}$$

and

$$\max\{I(X \wedge Z_1 | N), I(X \wedge Y_1 | N)\} > 0. \tag{2.18}$$

Since

$$I(Y \wedge Z | N) = I(Y_1 \wedge Z_1 | N) = I(Y_1 \wedge Z_1) = 0,$$

Y and Z are deterministically correlated and N is a maximal common function of Y and Z. It follows from Theorem 2.5 that the PK-capacity region is the set of pairs $(R_{\mathcal{X}\mathcal{Y}}, R_{\mathcal{X}\mathcal{Z}})$ satisfying

$$R_{\mathcal{X}\mathcal{Y}} \leq I(X \wedge Y_1 | Z_1, N),$$

$$\begin{aligned} R_{\mathcal{XZ}} &\leq I(X \wedge Z_1|Y_1, N), \\ R_{\mathcal{XY}} + R_{\mathcal{XZ}} &\leq I(X \wedge Y_1, Z_1|N). \end{aligned}$$

Then from (2.17) and (2.18),

$$\begin{aligned} I(X \wedge Y_1, Z_1|N) &= I(X \wedge Y_1|N) + I(X \wedge Z_1|Y_1, N) \\ &= H(Y_1|Z_1, N) - H(Y_1|X, N) + I(X \wedge Z_1|Y_1, N) \\ &< H(Y_1|Z_1, N) - H(Y_1|X, Z_1, N) + I(X \wedge Z_1|Y_1, N) \\ &= I(X \wedge Y_1|Z_1, N) + I(X \wedge Z_1|Y_1, N), \end{aligned}$$

and

$$I(X \wedge Y_1, Z_1|N) > \max\{I(X \wedge Y_1|Z_1, N), I(X \wedge Z_1|Y_1, N)\}.$$

Hence, this PK-capacity region is pentagonal. ■

2.4 Proofs

The technical tool used to prove Theorem 2.1 is supplied by Lemma 2.1 below.

Lemma 2.1 *Let $(K_{\mathcal{XY}}, K_{\mathcal{XZ}})$ be an ε-PK pair, with values in finite sets $\mathcal{K}_{\mathcal{XY}}$ and $\mathcal{K}_{\mathcal{XZ}}$, respectively, achieved with communication $\mathbf{F} = (F_1, \cdots, F_{3r})$. Let U be an arbitrary rv satisfying the Markov conditions in (2.5). Let $U^n = (U_1, \cdots, U_n)$ be n i.i.d. repetitions of the rv U such that each (U_i, X_i, Y_i, Z_i), $1 \leq i \leq n$, has identical joint pmf, and (U_i, X_i, Y_i, Z_i) is independent of (U_j, X_j, Y_j, Z_j), $1 \leq j \neq i \leq n$. Then*

$$\frac{1}{n}H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}|\mathbf{F}, U^n) = H(X, Y, Z|U) - (R_X + R_Y + R_Z) + \frac{3 + 3\varepsilon \log |\mathcal{K}_{\mathcal{XY}}||\mathcal{K}_{\mathcal{XZ}}|}{n} \quad (2.19)$$

for some (R_X, R_Y, R_Z) satisfying

$$R_X \geq H(X|Y, Z), \qquad R_Y + R_Z \geq H(Y, Z|U, X), \quad (2.20)$$

$$R_Y \geq H(Y|X,Z), \qquad R_X + R_Z \geq H(X,Z|Y) - \frac{1}{n}H(K_{\mathcal{XZ}}), \tag{2.21}$$

$$R_Z \geq H(Z|X,Y), \qquad R_X + R_Y \geq H(X,Y|Z) - \frac{1}{n}H(K_{\mathcal{XY}}). \tag{2.22}$$

The proof of Lemma 2.1 is analogous to that of Lemma 2 in [17]. Still, for completeness, a proof is provided below.

Proof of Lemma 2.1: Since $\mathbf{F}$, $K_{\mathcal{XY}}$ and $K_{\mathcal{XZ}}$ are functions of (X^n, Y^n, Z^n),

$$H(X^n, Y^n, Z^n|U^n) = H(\mathbf{F}|U^n) + H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}|\mathbf{F}, U^n) + H(X^n, Y^n, Z^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n).$$

Setting

$$\begin{aligned}
R_X &= \frac{1}{n}\sum_{t:t\ mod\ 3\equiv 1} H(F_t|U^n, F_{[1,t-1]}) + \frac{1}{n}H(X^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n)\\
&\quad + \frac{1+\varepsilon\log|\mathcal{K}_{\mathcal{XY}}||\mathcal{K}_{\mathcal{XZ}}|}{n},\\
R_Y &= \frac{1}{n}\sum_{t:t\ mod\ 3\equiv 2} H(F_t|U^n, F_{[1,t-1]}) + \frac{1}{n}H(Y^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n, X^n),\\
&\quad + \frac{1+\varepsilon\log|\mathcal{K}_{\mathcal{XY}}||\mathcal{K}_{\mathcal{XZ}}|}{n},\\
R_Z &= \frac{1}{n}\sum_{t:t\ mod\ 3\equiv 3} H(F_t|U^n, F_{[1,t-1]}) + \frac{1}{n}H(Z^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n, X^n, Y^n),\\
&\quad + \frac{1+\varepsilon\log|\mathcal{K}_{\mathcal{XY}}||\mathcal{K}_{\mathcal{XZ}}|}{n},
\end{aligned}$$

the previous equality gives

$$\frac{1}{n}H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}|\mathbf{F}, U^n) = H(X,Y,Z|U) - (R_X + R_Y + R_Z) + \frac{3+3\varepsilon\log|\mathcal{K}_{\mathcal{XY}}||\mathcal{K}_{\mathcal{XZ}}|}{n}.$$

It remains to show that (R_X, R_Y, R_Z) as defined above satisfy (2.20) – (2.22).

Since $U^n -\!\circ\!- Y^nZ^n -\!\circ\!- X^n$,

$$\begin{aligned}
H(X^n|Y^n, Z^n) &= H(\mathbf{F}, X^n|U^n, Y^n, Z^n)\\
&= \sum_{t=1}^{3r} H(F_t|U^n, Y^n, Z^n, F_{[1,t-1]}) + H(X^n|\mathbf{F}, U^n, Y^n, Z^n).
\end{aligned} \tag{2.23}$$

Since for t mod $3 \neq\ 1$, F_t is a function of $(Y^n, Z^n, F_{[1,t-1]})$,

$$\begin{aligned}\sum_{t=1}^{3r} H(F_t|U^n, Y^n, Z^n, F_{[1,t-1]}) &= \sum_{t:t\ mod\ 3\equiv 1} H(F_t|U^n, Y^n, Z^n, F_{[1,t-1]}) \\ &\leq \sum_{t:t\ mod\ 3\equiv 1} H(F_t|U^n, F_{[1,t-1]}).\end{aligned}$$

Further,

$$\begin{aligned}H(X^n|\mathbf{F}, U^n, Y^n, Z^n) &\leq H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}, X^n|\mathbf{F}, U^n, Y^n, Z^n) \\ &\leq H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}|\mathbf{F}, U^n, Y^n, Z^n) + H(X^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n) \\ &\leq 1 + \varepsilon \log|\mathcal{K}_{\mathcal{XY}}||\mathcal{K}_{\mathcal{XZ}}| + H(X^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n),\end{aligned}$$

where the last inequality follows from Fano's inequality.

Upon bounding the terms on the right side of (2.23) from above, we obtain that

$$H(X^n|Y^n, Z^n) \leq nR_X.$$

Since

$$\begin{aligned}H(Y^n, Z^n|U^n, X^n) &\leq H(\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, Y^n, Z^n|U^n, X^n) \\ &= H(\mathbf{F}|U^n, X^n) + H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}|\mathbf{F}, U^n, X^n) \\ &\quad + H(Y^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n, X^n) + H(Z^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n, X^n, Y^n) \\ &= \sum_{t:t\ mod\ 3\equiv 2,3} H(F_t|U^n, X^n, F_{[1,t-1]}) + H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}|\mathbf{F}, U^n, X^n) \\ &\quad + H(Y^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n, X^n) + H(Z^n|\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, U^n, X^n, Y^n) \\ &\leq n(R_Y + R_Z),\end{aligned}$$

(R_X, R_Y, R_Z) satisfy (2.20). Since

$$\begin{aligned}H(Y^n|X^n, Z^n) &\leq H(\mathbf{F}, K_{\mathcal{XY}}, K_{\mathcal{XZ}}, Y^n|U^n, X^n, Z^n) \\ &= \sum_{t:t\ mod\ 3\equiv 2} H(F_t|U^n, X^n, Z^n, F_{[1,t-1]}) + H(K_{\mathcal{XY}}, K_{\mathcal{XZ}}|\mathbf{F}, U^n, X^n, Z^n)\end{aligned}$$

$$\begin{aligned} & H(Y^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}}, K_{\mathcal{X}\mathcal{Z}}, U^n, X^n, Z^n) \\ \leq\ & nR_Y, \end{aligned}$$

and

$$\begin{aligned} H(X^n, Z^n|Y^n) &\leq H(\mathbf{F}, K_{\mathcal{X}\mathcal{Y}}, K_{\mathcal{X}\mathcal{Z}}, X^n, Z^n|U^n, Y^n) \\ &\leq H(\mathbf{F}|U^n, Y^n) + H(K_{\mathcal{X}\mathcal{Y}}|\mathbf{F}, U^n, Y^n) + H(K_{\mathcal{X}\mathcal{Z}}|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}}, U^n, Y^n) \\ &\quad + H(X^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}}, K_{\mathcal{X}\mathcal{Z}}, U^n) + H(Z^n|\mathbf{F}, U^n, X^n, Y^n) \\ &\leq n(R_X + R_Z) + H(K_{\mathcal{X}\mathcal{Z}}), \end{aligned}$$

(R_X, R_Y, R_Z) also satisfy (2.21). Similarly, it can be shown that (R_X, R_Y, R_Z) satisfy (2.22), completing the proof. ■

Proof of Theorem 2.1: We only show (2.4), as (2.3) is from [17]. Suppose that $\left(K_{\mathcal{X}\mathcal{Y}}^{(n)}, K_{\mathcal{X}\mathcal{Z}}^{(n)}\right)$ represent an ε_n-PK pair, with values in finite sets $\mathcal{K}_{\mathcal{X}\mathcal{Y}}^{(n)}$ and $\mathcal{K}_{\mathcal{X}\mathcal{Z}}^{(n)}$, respectively, achieved with communication $\mathbf{F} = (F_1, \cdots, F_{3r})$, where $\varepsilon_n \to 0$ (see Definition 2.1). Let U be an arbitrary rv satisfying the Markov conditions in (2.5). Let $U^n = (U_1, \cdots, U_n)$ be n i.i.d. repetitions of the rv U such that each (U_i, X_i, Y_i, Z_i), $1 \leq i \leq n$, has identical joint pmf, and (U_i, X_i, Y_i, Z_i) is independent of (U_j, X_j, Y_j, Z_j), $1 \leq j \neq i \leq n$. Then

$$U^n -\!\circ\!- Y^n -\!\circ\!- X^n Z^n, \qquad U^n -\!\circ\!- Z^n -\!\circ\!- X^n Y^n,$$

which implies that

$$U^n -\!\circ\!- \mathbf{F}Y^n -\!\circ\!- X^n Z^n, \qquad U^n -\!\circ\!- \mathbf{F}Z^n -\!\circ\!- X^n Y^n.$$

Hence,

$$\begin{aligned} I\left(K_{\mathcal{X}\mathcal{Z}}^{(n)} \wedge \mathbf{F}, U^n\right) &\leq I\left(K_{\mathcal{X}\mathcal{Z}}^{(n)} \wedge \mathbf{F}, U^n, Y^n\right) \\ &= I\left(K_{\mathcal{X}\mathcal{Z}}^{(n)} \wedge \mathbf{F}, Y^n\right) + I\left(K_{\mathcal{X}\mathcal{Z}}^{(n)} \wedge U^n|\mathbf{F}, Y^n\right) \end{aligned}$$

$$
\begin{aligned}
&\leq n\varepsilon_n + I\left(K^{(n)}_{\mathcal{XZ}}, X^n \wedge U^n | \mathbf{F}, Y^n\right) \\
&\leq n\varepsilon_n + H\left(K^{(n)}_{\mathcal{XZ}} | \mathbf{F}, X^n\right) \\
&\leq n\varepsilon_n + 1 + \varepsilon_n \log \left|\mathcal{K}^{(n)}_{\mathcal{XY}}\right| \left|\mathcal{K}^{(n)}_{\mathcal{XZ}}\right|. \qquad (2.24)
\end{aligned}
$$

Similarly, we have

$$
I\left(K^{(n)}_{\mathcal{XY}} \wedge \mathbf{F}, K^{(n)}_{\mathcal{XZ}}, U^n\right) \leq n\varepsilon_n + 2 + 2\varepsilon_n \log \left|\mathcal{K}^{(n)}_{\mathcal{XY}}\right| \left|\mathcal{K}^{(n)}_{\mathcal{XZ}}\right|. \qquad (2.25)
$$

On the other hand, it follows from (2.19) and (2.20) that

$$
\begin{aligned}
\frac{1}{n} H\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}} | \mathbf{F}, U^n\right) &\leq H(X, Y, Z|U) - [H(X|Y, Z) + H(Y, Z|U, X)] \\
&\quad + \frac{3 + 3\varepsilon_n \log \left|\mathcal{K}^{(n)}_{\mathcal{XY}}\right| \left|\mathcal{K}^{(n)}_{\mathcal{XZ}}\right|}{n} \\
&= I(X \wedge Y, Z|U) + \frac{3 + 3\varepsilon_n \log \left|\mathcal{K}^{(n)}_{\mathcal{XY}}\right| \left|\mathcal{K}^{(n)}_{\mathcal{XZ}}\right|}{n}. \qquad (2.26)
\end{aligned}
$$

Finally, it follows from (2.24) – (2.26) that

$$
\begin{aligned}
&\frac{1}{n} H\left(K^{(n)}_{\mathcal{XY}}\right) + \frac{1}{n} H\left(K^{(n)}_{\mathcal{XZ}}\right) \\
= \; &\frac{1}{n} H\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}\right) + \frac{1}{n} I\left(K^{(n)}_{\mathcal{XY}} \wedge K^{(n)}_{\mathcal{XZ}}\right) \\
= \; &\frac{1}{n} H\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}} | \mathbf{F}, U^n\right) + \frac{1}{n} I\left(K^{(n)}_{\mathcal{XZ}} \wedge \mathbf{F}, U^n\right) + \frac{1}{n} I\left(K^{(n)}_{\mathcal{XY}} \wedge \mathbf{F}, K^{(n)}_{\mathcal{XZ}}, U^n\right) \\
\leq \; &I(X \wedge Y, Z|U) + 2\varepsilon_n + \frac{6 + 6\varepsilon_n \log \left|\mathcal{K}^{(n)}_{\mathcal{XY}}\right| \left|\mathcal{K}^{(n)}_{\mathcal{XZ}}\right|}{n}.
\end{aligned}
$$

This completes the proof. ■

The proof of Theorem 2.2 is based on Lemma 2.2 below, which is implied by [16] (Theorem 2.6). Since the models considered in [16] involve rate constraints on the public communication **F** between user terminals, the full force of the results in [16] is not needed here. We provide below a version of the model and the corresponding lemma of direct use here.

Consider a DMMS with three components corresponding to generic rvs X, Y, Z with finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$. Let $X^n = (X_1, \cdots, X_n)$, $Y^n = (Y_1, \cdots, Y_n)$, $Z^n = (Z_1, \cdots, Z_n)$ be n i.i.d. repetitions of the rvs X, Y, Z. Terminals $\mathcal{X}$ and $\mathcal{Y}$ respectively observe the components X^n and Y^n of the DMMS, where n denotes the observation length. Here, terminals $\mathcal{X}$ and $\mathcal{Y}$ represent the two users who wish to generate a wiretap secret key (WSK), which should be concealed from a wiretapper $\mathcal{Z}$ that observes the component Z^n of the DMMS. The user terminals can communicate with each other through broadcasts over a noiseless public channel, possibly interactively in many rounds. Again, we assume without any loss of generality that these transmissions occur in consecutive time slots in r rounds; the communication is depicted by $2r$ rvs $F_1, \cdots, F_{2r}$, where F_t denotes the transmission in time slot t, $1 \leq t \leq 2r$, by terminal $\mathcal{X}$ (resp. $\mathcal{Y}$) if t is odd (resp. even). In general, F_t is allowed to be any function, defined in terms of a mapping f_t, of the local observations at the user terminal and of the previous transmissions $F_{[1,t-1]} = (F_1, \cdots, F_{t-1})$. No randomization is permitted at the user terminals; in particular, $f_1, \cdots, f_{2r}$ are deterministic mappings. Let $\mathbf{F} = (F_1, \cdots, F_{2r})$ denote collectively all the transmissions in the $2r$ time slots.

The rv $K_{\mathcal{X}\mathcal{Y}}$, which is a function of (X^n, Y^n), with finite range $\mathcal{K}_{\mathcal{X}\mathcal{Y}}$, represents an *$\varepsilon$-wiretap secret key* (*$\varepsilon$-WSK*) for terminals $\mathcal{X}$ and $\mathcal{Y}$ and concealed from the wiretapper $\mathcal{Z}$, achievable with communication $\mathbf{F}$, if:

- $K_{\mathcal{X}\mathcal{Y}}$ is ε-recoverable from each of $(\mathbf{F}, X^n)$, $(\mathbf{F}, Y^n)$;
- $K_{\mathcal{X}\mathcal{Y}}$ satisfies the wiretap secrecy condition

$$\frac{1}{n} I(K_{\mathcal{X}\mathcal{Y}} \wedge \mathbf{F}, Z^n) \leq \varepsilon;$$

and

- $K_{\mathcal{X}\mathcal{Y}}$ satisfies the uniformity condition

$$\frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}}) \geq \frac{1}{n}\log|\mathcal{K}_{\mathcal{X}\mathcal{Y}}| - \varepsilon.$$

Definition 2.5 *A nonnegative number $R_{\mathcal{X}\mathcal{Y}}$ is an achievable WSK-rate if an ε_n-WSK $K^{(n)}_{\mathcal{X}\mathcal{Y}}$ is achievable with suitable communication (with the number of rounds possibly depending on n), such that $\varepsilon_n \to 0$ and $\frac{1}{n}H\left(K^{(n)}_{\mathcal{X}\mathcal{Y}}\right) \to R_{\mathcal{X}\mathcal{Y}}$. The largest achievable WSK-rate is the WSK-capacity C_{WSK}. An achievable WSK-rate will be said to be strongly achievable if ε_n above can be taken to vanish exponentially in n. A WSK-capacity will be termed strong if all smaller rates are strongly achievable.*

Lemma 2.2 [16] *The (strong) WSK-capacity is bounded below according to*

$$C_{WSK} \geq \max_U \left[I(X \wedge Y|U) - I(X \wedge Z|U)\right], \tag{2.27}$$

where the maximum is over all rvs U that satisfy the Markov condition $U -\!\!\circ\!\!- X -\!\!\circ\!\!- YZ$. Furthermore, the right side of (2.27) is a WSK-rate that can be achieved by a single transmission from terminal $\mathcal{X}$. ■

Remarks:

1. The right side of (2.27) was first proved to be a lower bound for the "weak" WSK-capacity in [3]. If randomization is allowed at terminals $\mathcal{X}$ and $\mathcal{Y}$, the right side of (2.27) was also proved to be a lower bound for the strong WSK-capacity in [13].

2. It follows from the proof of Lemma 2.2 that upon receiving the transmission from terminal $\mathcal{X}$, terminal $\mathcal{Y}$ recovers the observation $X^n = x^n$ at terminal $\mathcal{X}$, with error probability decaying to 0 exponentially with n.

Proof of Theorem 2.2: We prove here only the strong achievability of the region (2.8). The strong achievability of the region (2.9) follows by symmetry. Thanks to a time-sharing argument, to finish the proof of this theorem, it suffices to show the strong achievability of the rate pair

$$\left(\max_{U:\ U -\!\!\circ\!\!- Y -\!\!\circ\!\!- XZ} \left[I(X \wedge Y|U) - I(Y \wedge Z|U) \right], I(X \wedge Z|Y) \right).$$

The scheme to achieve a PK pair with the rates as above is as follows. Let $X^n = x^n$, $Y^n = y^n$, $Z^n = z^n$ be the respective observations at the terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$. Terminal $\mathcal{X}$ does not transmit in the first time slot. In the second time slot, terminal $\mathcal{Y}$ transmits $f_2(y^n)$, in order to establish a WSK with terminal $\mathcal{X}$ by regarding terminal $\mathcal{Z}$ as a wiretapper. By Lemma 2.2, after this transmission, terminals $\mathcal{X}$ and $\mathcal{Y}$ generate an ε_n-WSK $K^{(n)}_{\mathcal{X}\mathcal{Y}}$, with ε_n decaying to 0 exponentially, and

$$\frac{1}{n} H\left(K^{(n)}_{\mathcal{X}\mathcal{Y}}\right) \geq \max_{U:\ U -\!\!\circ\!\!- Y -\!\!\circ\!\!- XZ} \left[I(X \wedge Y|U) - I(Y \wedge Z|U) \right].$$

Furthermore, upon receiving the transmission $f_2(y^n)$, terminal $\mathcal{X}$ recovers y^n with error probability decaying exponentially 0 with n.

In the third time slot, terminal $\mathcal{Z}$ transmits $f_3(z^n)$, in order to establish a WSK with terminal $\mathcal{X}$ by regarding terminal $\mathcal{Y}$ as a wiretapper. Again, by Lemma 2.2, after this transmission, terminals $\mathcal{X}$ and $\mathcal{Z}$ generate an ε_n-WSK $K^{(n)}_{\mathcal{X}\mathcal{Z}}$, with ε_n decaying to 0 exponentially, and

$$\begin{aligned} \frac{1}{n} H\left(K^{(n)}_{\mathcal{X}\mathcal{Z}}\right) &\geq \max_{V:\ V -\!\!\circ\!\!- Z -\!\!\circ\!\!- XY} \left[I(Z \wedge X, Y|V) - I(Z \wedge Y|V) \right] \\ &\geq I(X \wedge Z|Y). \end{aligned}$$

The last inequality follows by choosing V to be a constant. In this scheme, $\mathbf{F} = (F_2, F_3)$, where $F_2 = f_2(Y^n)$ and $F_3 = f_3(Z^n)$. Now,

$$\frac{1}{n} I\left(K^{(n)}_{\mathcal{X}\mathcal{Z}} \wedge \mathbf{F}, Y^n\right) = \frac{1}{n} I\left(K^{(n)}_{\mathcal{X}\mathcal{Z}} \wedge F_3, Y^n\right) \leq \varepsilon_n,$$

where the inequality follows since $K_{\mathcal{XZ}}^{(n)}$ is an ε_n-WSK. Similarly,

$$\frac{1}{n} I\left(K_{\mathcal{XY}}^{(n)} \wedge \mathbf{F}, Z^n\right) \leq \varepsilon_n.$$

Therefore, the two ε_n-WSK $K_{\mathcal{XY}}^{(n)}$, $K_{\mathcal{XZ}}^{(n)}$, with individual rates no less than

$$\max_{U:\ U - \circ - Y - \circ - XZ} \left[I(X \wedge Y|U) - I(Y \wedge Z|U)\right]$$

and

$$I(X \wedge Z|Y),$$

respectively, constitute an ε_n-PK pair. This completes the proof. ∎

In the proof of Theorem 2.3, we shall use the notations and properties of typical sequences, which are given in Appendix A.2, as well as the following lemma, which is proved in [17].

Lemma 2.3 [17] *Given the finite sets $\mathcal{U}$, $\mathcal{V}$, a function $f : \mathcal{U}^n \rightarrow \{1, \cdots, 2^{nR}\}$, and a positive number H, there exists a mapping $g : \mathcal{U}^n \rightarrow \{1, \cdots, 2^{nH}\}$ such that for i.i.d. repetitions of any rvs (U, V) with*

$$H(U|V) > R + H + \delta,$$

where $\delta > 0$ is arbitrarily small but fixed, the probabilities that $g(U^n)$ is uniformly distributed and $g(U^n)$ is independent of $(f(U^n), V^n)$ go exponentially to 0. ∎

Proof of Theorem 2.3: We prove here only the strong achievability of the region (2.12). The strong achievability of the region (2.13) follows by symmetry.

Denote by $U_{mss(Y_i)}$ the minimal sufficient statistic for Y_i w.r.t. Z_i, $1 \leq i \leq n$. Let $U_{mss(Y)}^n = \left(U_{mss(Y_1)}, \cdots, U_{mss(Y_2)}\right)$. Terminal $\mathcal{Y}$ obtains the sequence $U_{mss(Y)}^n = u^n$ from its local observation y^n, and transmits the sequence u^n.

Consider random partitions of $\mathcal{Y}^n$ and $\mathcal{Z}^n$ into b_1 and b_2 bins, respectively, where $b_1 = b_1(n)$ and $b_2 = b_2(n)$ are two integers to be specified later. For each $y^n \in \mathcal{Y}^n$ (resp. $z^n \in \mathcal{Z}^n$), let $F_{\mathcal{Y}}(y^n)$ (resp. $F_{\mathcal{Z}}(z^n)$) be the random index of the bin containing y^n (resp. z^n), where $F_{\mathcal{Y}}(y^n)$ (resp. $F_{\mathcal{Z}}(z^n)$) is uniformly distributed on the set of integers $\{1, \cdots, b_1\}$ (resp. $\{1, \cdots, b_2\}$). Then, clearly $F_{\mathcal{Y}}(y^n)$, $y^n \in \mathcal{Y}^n$ are mutually independent, as are $F_{\mathcal{Z}}(z^n)$, $z^n \in \mathcal{Z}^n$. Furthermore, assume that $(F_{\mathcal{Y}}(y^n), y^n \in \mathcal{Y}^n)$, $(F_{\mathcal{Z}}(z^n), z^n \in \mathcal{Z}^n)$ and (X^n, Y^n, Z^n) are mutually independent.

Terminals $\mathcal{Y}$ and $\mathcal{Z}$, with respective observations y^n and z^n, transmit random indices $F_{\mathcal{Y}}(y^n) = J_{\mathcal{Y}}$ and $F_{\mathcal{Z}}(z^n) = J_{\mathcal{Z}}$, where $J_{\mathcal{Y}}$ and $J_{\mathcal{Z}}$ are uniformly distributed on $\{1, \cdots, b_1\}$ and $\{1, \cdots, b_2\}$, respectively.

The decoding at terminal $\mathcal{X}$ is performed as follows. Fix $\xi > 0$. Terminal $\mathcal{X}$, upon observing $x^n \in \mathcal{X}^n$ as well as receiving the sequence u^n and the integers $j_{\mathcal{Y}}$, $j_{\mathcal{Z}}$, decodes according to the decoding rule ϕ, defined by

$$\phi(u^n, x^n, j_{\mathcal{Y}}, j_{\mathcal{Z}}) = (\hat{y}^n, \hat{z}^n),$$

iff $(\hat{y}^n, \hat{z}^n)$ is the unique element in $\mathcal{Y}^n \times \mathcal{Z}^n$ such that

- $(u^n, x^n, \hat{y}^n, \hat{z}^n) \in T^n_{U_{mss(Y)}XYZ,\xi}$ and
- $F_{\mathcal{Y}}(\hat{y}^n) = j_{\mathcal{Y}}$, $F_{\mathcal{Z}}(\hat{z}^n) = j_{\mathcal{Z}}$.

If no such $(\hat{y}^n, \hat{z}^n)$ exists, an error is declared. The probability of decoding error at terminal $\mathcal{X}$ is then

$$P_e^{(n)} = \Pr\left\{\phi(U^n_{mss(Y)}, X^n, F_{\mathcal{Y}}(Y^n), F_{\mathcal{Z}}(Z^n)) \neq (Y^n, Z^n)\right\}.$$

Define the events

$$E_0 = \left\{(U^n_{mss(Y)}, X^n, Y^n, Z^n) \notin T^n_{U_{mss(Y)}XYZ,\xi}\right\},$$

$$E_1 = \left\{\exists \tilde{y}^n \in \mathcal{Y}^n : Y^n \neq \tilde{y}^n; F_{\mathcal{Y}}(Y^n) = F_{\mathcal{Y}}(\tilde{y}^n); (U^n_{mss(Y)}, X^n, \tilde{y}^n, Z^n) \in T^n_{U_{mss(Y)}XYZ,\xi}\right\},$$

$$E_2 = \left\{\exists \tilde{z}^n \in \mathcal{Z}^n : Z^n \neq \tilde{z}^n; F_{\mathcal{Z}}(Z^n) = F_{\mathcal{Z}}(\tilde{z}^n); (U^n_{mss(Y)}, X^n, Y^n, \tilde{z}^n) \in T^n_{U_{mss(Y)}XYZ,\xi}\right\},$$

$$E_3 = \{\exists (\tilde{y}^n, \tilde{z}^n) \in \mathcal{Y}^n \times \mathcal{Z}^n : Y^n \neq \tilde{y}^n; Z^n \neq \tilde{z}^n; F_{\mathcal{Y}}(Y^n) = F_{\mathcal{Y}}(\tilde{y}^n); F_{\mathcal{Z}}(Z^n) = F_{\mathcal{Z}}(\tilde{z}^n);$$
$$(U^n_{mss(Y)}, X^n, \tilde{y}^n, \tilde{z}^n) \in T^n_{U_{mss(Y)}XYZ,\xi}\},$$

Clearly,

$$P_e^{(n)} = \Pr\left\{\bigcup_{i=0}^{3} E_i\right\} \leq \sum_{i=0}^{3} \Pr\{E_i\}. \tag{2.28}$$

It follows from Proposition A.1 in Appendix A.2 that for some $\varepsilon = \varepsilon(\xi) > 0$, and all sufficiently large n,

$$\Pr\{E_0\} < 2^{-n\varepsilon} \tag{2.29}$$

To bound $\Pr\{E_1\}$, we have

$$\begin{aligned}
& \Pr\{E_1\} \\
= & \sum_{(u^n,x^n,y^n,z^n)\in T^n_{U_{mss(Y)}XYZ,\xi}} \Pr\left\{(U^n_{mss(Y)}, X^n, Y^n, Z^n) = (u^n, x^n, y^n, z^n)\right\} \\
& \cdot \sum_{\tilde{y}^n \neq y^n : (u^n,x^n,\tilde{y}^n,z^n)\in T^n_{U_{mss(Y)}XYZ,\xi}} \Pr\left\{F_{\mathcal{Y}}(\tilde{y}^n) = F_{\mathcal{Y}}(y^n) | (U^n_{mss(Y)}, X^n, Y^n, Z^n) = (u^n, x^n, y^n, z^n)\right\} \\
= & \sum_{(u^n,x^n,y^n,z^n)\in T^n_{U_{mss(Y)}XYZ,\xi}} \Pr\left\{(U^n_{mss(Y)}, X^n, Y^n, Z^n) = (u^n, x^n, y^n, z^n)\right\} \\
& \sum_{\tilde{y}^n \neq y^n : (u^n,x^n,\tilde{y}^n,z^n)\in T^n_{U_{mss(Y)}XYZ,\xi}} b_1^{-1} \\
\leq & \sum_{(u^n,x^n,y^n,z^n)\in T^n_{U_{mss(Y)}XYZ,\xi}} \Pr\left\{(U^n_{mss(Y)}, X^n, Y^n, Z^n) = (u^n, x^n, y^n, z^n)\right\} \\
& \cdot b_1^{-1} \cdot 2^{n[H(Y|U_{mss(Y)},X,Z)+2\xi]} \\
\leq & \ 2^{-n\left[\frac{1}{n}\log b_1 - H(Y|U_{mss(Y)},X,Z) - 2\xi\right]}.
\end{aligned} \tag{2.30}$$

Similarly, we have

$$\Pr\{E_2\} \leq 2^{-n\left[\frac{1}{n}\log b_2 - H(Z|U_{mss(Y)},X,Y) - 2\xi\right]}, \tag{2.31}$$

and

$$\Pr\{E_3\} \leq 2^{-n\left[\frac{1}{n}\log b_1 b_2 - H(Y,Z|U_{mss(Y)},X) - 2\xi\right]}. \tag{2.32}$$

Upon picking the integers b_1, b_2 so as to satisfy

$$\frac{1}{n}\log b_1 \geq H(Y|U_{mss(Y)}, X, Z) + 3\xi, \tag{2.33}$$

$$\frac{1}{n}\log b_2 \geq H(Z|U_{mss(Y)}, X, Y) + 3\xi, \tag{2.34}$$

and

$$\frac{1}{n}\log b_1 b_2 \geq H(Y, Z|U_{mss(Y)}, X) + 3\xi, \tag{2.35}$$

it follows from (2.28) – (2.32) that for some $\eta = \eta(\varepsilon, \xi) > 0$ and all sufficiently large n,

$$P_e^{(n)} \leq 2^{-n\eta}.$$

It then follows that there exists a pair of (deterministic) mappings $f_{\mathcal{Y}} = f_{\mathcal{Y}}(Y^n)$ and $f_{\mathcal{Z}} = f_{\mathcal{Z}}(Z^n)$ satisfying

$$\Pr\left\{\phi\left(U^n_{mss(Y)}, X^n, f_{\mathcal{Y}}(Y^n), f_{\mathcal{Z}}(Z^n)\right) \neq (Y^n, Z^n)\right\} \leq 2^{-n\eta}.$$

Next, apply Lemma 2.3 with Y, $(U_{mss(Y)}, Z)$ and $f_{\mathcal{Y}}$ in the roles of U, V and f, with $R = \frac{1}{n}\log b_1$ and $H = H(Y|U_{mss(Y)}, Z) - \frac{1}{n}\log b_1 - \xi = H(Y|U_{mss(Y)}) - \frac{1}{n}\log b_1 - \xi$, respectively. The following holds with probability exponentially tending to 1 in n: there exists a mapping $g_{\mathcal{Y}} : \mathcal{Y}^n \to \{1, \cdots, 2^{n[H(Y|U_{mss(Y)}) - \frac{1}{n}\log b_1 - \xi]}\}$ such that $g_{\mathcal{Y}}(Y^n)$ is uniformly distributed and $g_{\mathcal{Y}}(Y^n)$ is independent of $(f_{\mathcal{Y}}(Y^n), U^n_{mss(Y)}, Z^n)$.

Apply Lemma 2.3 again with Z, Y and $f_{\mathcal{Z}}$ in the roles of U, V and f, with $R = \frac{1}{n}\log b_2$ and $H = H(Z|Y) - \frac{1}{n}\log b_2 - \xi$, respectively. The following holds with probability exponentially tending to 1: there exists a mapping $g_{\mathcal{Z}} : \mathcal{Z}^n \to \{1, \cdots, 2^{n[H(Z|Y) - \frac{1}{n}\log b_2 - \xi]}\}$ such that $g_{\mathcal{Z}}(Z^n)$ is uniformly distributed and $g_{\mathcal{Z}}(Z^n)$ is independent of $(f_{\mathcal{Z}}(Z^n), Y^n)$

If no error is declared by terminal $\mathcal{X}$, the PK $K^{(n)}_{\mathcal{XY}}$ is set as $g_{\mathcal{Y}}(Y^n)$, and the PK $K^{(n)}_{\mathcal{XZ}}$ is set as $g_{\mathcal{Z}}(Z^n)$. Otherwise, $K^{(n)}_{\mathcal{XY}}$ and $K^{(n)}_{\mathcal{XZ}}$ are respectively set to be uniformly distributed on

$$\left\{1, \cdots, 2^{n[H(Y|U_{mss(Y)}) - \frac{1}{n}\log b_1 - \xi]}\right\},$$

and

$$\left\{1, \cdots, 2^{n[H(Z|Y) - \frac{1}{n}\log b_2 - \xi]}\right\},$$

independent of (X^n, Y^n, Z^n).

Clearly, $K_{\mathcal{XY}}^{(n)}$ and $K_{\mathcal{XZ}}^{(n)}$ are ε_n-recoverable at terminal $\mathcal{X}$, with ε_n exponentially decaying to 0.

The uniformity of $g_{\mathcal{Y}}(Y^n)$ and $g_{\mathcal{Z}}(Z^n)$ gives that

$$\begin{aligned}\frac{1}{n}H\left(K_{\mathcal{XY}}^{(n)}\right) &= H(Y|U_{mss(Y)}) - \frac{1}{n}\log b_1 - \xi,\\ \frac{1}{n}H\left(K_{\mathcal{XZ}}^{(n)}\right) &= H(Z|Y) - \frac{1}{n}\log b_2 - \xi.\end{aligned}$$

The lower bounds (2.33) – (2.35) on $\frac{1}{n}\log b_1$, $\frac{1}{n}\log b_2$ and $\frac{1}{n}\log b_1 b_2$ imply that

$$\frac{1}{n}H\left(K_{\mathcal{XY}}^{(n)}\right) \leq H(Y|U_{mss(Y)}) - H(Y|U_{mss(Y)}, X, Z) - 4\xi = I(X \wedge Y|U_{mss(Y)}, Z) - 4\xi,$$

$$\frac{1}{n}H\left(K_{\mathcal{XZ}}^{(n)}\right) \leq H(Z|Y) - H(Z|X,Y) - 4\xi = I(X \wedge Z|Y) - 4\xi,$$

$$\begin{aligned}\frac{1}{n}H\left(K_{\mathcal{XY}}^{(n)}\right) + \frac{1}{n}H\left(K_{\mathcal{XZ}}^{(n)}\right) &\leq H(Y|U_{mss(Y)}) + H(Z|Y) - H(Y,Z|U_{mss(Y)}, X) - 5\xi\\ &= I(X \wedge Y, Z|U_{mss(Y)}) - 5\xi.\end{aligned}$$

Note that

$$I\left(K_{\mathcal{XY}}^{(n)} \wedge \mathbf{F}, Z^n\right) = I(g_{\mathcal{Y}}(Y^n) \wedge f_{\mathcal{Y}}(Y^n), U_{mss(Y)}^n, Z^n)$$

and

$$I\left(K_{\mathcal{XZ}}^{(n)} \wedge \mathbf{F}, Y^n\right) = I(g_{\mathcal{Z}}(Z^n) \wedge f_{\mathcal{Z}}(Z^n), Y^n).$$

It follows from the independence of $g_{\mathcal{Y}}(Y^n)$ and $(f_{\mathcal{Y}}(Y^n), U_{mss(Y)}^n, Z^n)$, as well as of $g_{\mathcal{Z}}(Z^n)$ and $(f_{\mathcal{Z}}(Z^n), Y^n)$, that $\left(K_{\mathcal{XY}}^{(n)}, K_{\mathcal{XZ}}^{(n)}\right)$ constitutes a (strongly) achievable PK pair. This completes the proof. ■

Proof of Theorem 2.4: The converse part follows from Theorem 2.1. The achievability part is seen as follows. Let U be an arbitrary rv satisfying all three Markov conditions in (2.14). Theorem 2.2 implies that

$$(I(X \wedge Y|U), I(X \wedge Z|Y))$$

and

$$(I(X \wedge Y|Z), I(X \wedge Z|U))$$

are two strongly achievable PK-rate pairs. Note that

$$\begin{aligned} I(X \wedge Y|U) + I(X \wedge Z|Y) &= I(X \wedge Y|Z) + I(X \wedge Z|U) \\ &= I(X \wedge Y, Z|U). \end{aligned}$$

Hence, the strong PK-capacity region is inner bounded by the region

$$\left\{ \begin{array}{ll} (R_{\mathcal{X}\mathcal{Y}}, R_{\mathcal{X}\mathcal{Z}}) : & R_{\mathcal{X}\mathcal{Y}} \leq I(X \wedge Y|Z) \quad R_{\mathcal{X}\mathcal{Z}} \leq I(X \wedge Z|Y), \\ & R_{\mathcal{X}\mathcal{Y}} + R_{\mathcal{X}\mathcal{Z}} \leq \max_U I(X \wedge Y, Z|U) \end{array} \right\},$$

where the maximum is w.r.t. U satisfying (2.14). This completes the proof. ∎

2.5 Generalizations

The model considered in this section is an obvious generalization of the previous model, in that after r rounds of communication, a PK must be generated by each of the three pairs of terminals (i.e., terminals $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{X}$ and $\mathcal{Z}$, $\mathcal{Y}$ and $\mathcal{Z}$). We shall define the PK-capacity region for this model and derive an outer bound for the PK-capacity region. Also, we shall provide an example in which this outer bound for the PK-capacity region is tight.

Consider a DMMS with three components corresponding to generic rvs X, Y, Z with finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$. Let $X^n = (X_1, \cdots, X_n)$, $Y^n = (Y_1, \cdots, Y_n)$, $Z^n = (Z_1, \cdots, Z_n)$

be n i.i.d. repetitions of the rvs X, Y, Z. The terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ respectively observe the components X^n, Y^n, Z^n of the DMMS (X^n, Y^n, Z^n), where n denotes the observation length. The terminals can communicate with each other through broadcasts over a noiseless public channel, possibly interactively in many rounds. We assume without any loss of generality that these transmissions occur in consecutive time slots in r rounds; the communication is depicted by $3r$ rvs $F_1, \cdots, F_{3r}$, where F_t denotes the transmission in time slot t, $1 \leq t \leq 3r$, by a terminal assigned an index $i = t \bmod 3$, $1 \leq i \leq 3$, with terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ corresponding to indices 1, 2, 3, respectively. In general, F_t is allowed to be any function, defined in terms of a mapping f_t, of the observations at the terminal with index i and of the previous transmissions $F_{[1,t-1]} = (F_1, \cdots, F_{t-1})$; thus, for instance, $F_1 = f_1(X^n)$, $F_2 = f_2(Y^n, F_1)$, $F_3 = f_3(Z^n, F_1, F_2)$, and so on. We do not permit any randomization at the terminals; in particular, $f_1, \cdots, f_{3r}$ are deterministic mappings. Let $\mathbf{F} = (F_1, \cdots, F_{3r})$ denote collectively all the transmissions in the $3r$ time slots.

The rvs $K_{\mathcal{X}\mathcal{Y}}$, $K_{\mathcal{X}\mathcal{Z}}$ and $K_{\mathcal{Y}\mathcal{Z}}$, which are functions of (X^n, Y^n, Z^n), with finite ranges $\mathcal{K}_{\mathcal{X}\mathcal{Y}}$, $\mathcal{K}_{\mathcal{X}\mathcal{Z}}$ and $\mathcal{K}_{\mathcal{Y}\mathcal{Z}}$, respectively, represent an *ε-private key* (*ε-PK*) triple, where $K_{\mathcal{X}\mathcal{Y}}$ (resp. $K_{\mathcal{X}\mathcal{Z}}$; $K_{\mathcal{Y}\mathcal{Z}}$) is the PK for terminals $\mathcal{X}$, $\mathcal{Y}$ (resp. $\mathcal{X}$, $\mathcal{Z}$; $\mathcal{Y}$, $\mathcal{X}$) with privacy from the terminal $\mathcal{Z}$ (resp. $\mathcal{Y}$; $\mathcal{Z}$), achievable with communication $\mathbf{F}$, if:

- $K_{\mathcal{X}\mathcal{Y}}$ is ε-recoverable from each of $(\mathbf{F}, X^n)$, $(\mathbf{F}, Y^n)$;
- $K_{\mathcal{X}\mathcal{Z}}$ is ε-recoverable from each of $(\mathbf{F}, X^n)$, $(\mathbf{F}, Z^n)$;
- $K_{\mathcal{Y}\mathcal{Z}}$ is ε-recoverable from each of $(\mathbf{F}, Y^n)$, $(\mathbf{F}, Z^n)$;
- $K_{\mathcal{X}\mathcal{Y}}$ satisfies the secrecy condition and the uniformity condition

$$\frac{1}{n} I(K_{\mathcal{X}\mathcal{Y}} \wedge \mathbf{F}, Z^n) \leq \varepsilon;$$

$$\frac{1}{n} H(K_{\mathcal{X}\mathcal{Y}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}}| - \varepsilon;$$

- $K_{\mathcal{XZ}}$ satisfies the secrecy condition and the uniformity condition

$$\frac{1}{n} I(K_{\mathcal{XZ}} \wedge \mathbf{F}, Y^n) \leq \varepsilon;$$

$$\frac{1}{n} H(K_{\mathcal{XZ}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{XZ}}| - \varepsilon.$$

and

- $K_{\mathcal{YZ}}$ satisfies the secrecy condition and the uniformity condition

$$\frac{1}{n} I(K_{\mathcal{YZ}} \wedge \mathbf{F}, X^n) \leq \varepsilon;$$

$$\frac{1}{n} H(K_{\mathcal{YZ}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{YZ}}| - \varepsilon.$$

Definition 2.6 *A triple of nonnegative numbers $(R_{\mathcal{XY}}, R_{\mathcal{XZ}}, R_{\mathcal{YZ}})$ is an achievable PK-rate triple if an ε_n-PK triple $\left(K_{\mathcal{XY}}^{(n)}, K_{\mathcal{XZ}}^{(n)}, K_{\mathcal{YZ}}^{(n)}\right)$ is achievable with suitable communication, such that $\varepsilon_n \to 0$, $\frac{1}{n} H\left(K_{\mathcal{XY}}^{(n)}\right) \to R_{\mathcal{XY}}$, $\frac{1}{n} H\left(K_{\mathcal{XZ}}^{(n)}\right) \to R_{\mathcal{XZ}}$, $\frac{1}{n} H\left(K_{\mathcal{YZ}}^{(n)}\right) \to R_{\mathcal{YZ}}$. The set of all achievable PK-rate triples is the PK-capacity region C_{PK}. An achievable PK-rate triple will be called strongly achievable if ε_n above can be taken to vanish exponentially in n. A PK-capacity region will be termed strong if all rate triples in that region are strongly achievable.*

Remark: The (strong) PK-capacity region is also a closed convex set.

Theorem 2.6 *(Outer bound for C_{PK}): Let ($R_{\mathcal{XY}}$, $R_{\mathcal{XZ}}$, $R_{\mathcal{YZ}}$) be an achievable PK-rate triple. Then*

$$R_{\mathcal{XY}} \leq I(X \wedge Y|Z), \qquad R_{\mathcal{XZ}} + R_{\mathcal{YZ}} \leq I(Z \wedge X, Y|U_{mcf(X,Y)}), \tag{2.36}$$

$$R_{\mathcal{XZ}} \leq I(X \wedge Z|Y), \qquad R_{\mathcal{XY}} + R_{\mathcal{YZ}} \leq I(Y \wedge X, Z|U_{mcf(X,Z)}), \tag{2.37}$$

$$R_{\mathcal{YZ}} \leq I(Y \wedge Z|X), \qquad R_{\mathcal{XY}} + R_{\mathcal{XZ}} \leq I(X \wedge Y, Z|U_{mcf(Y,Z)}), \tag{2.38}$$

$$R_{\mathcal{X}\mathcal{Y}} + R_{\mathcal{X}\mathcal{Z}} + R_{\mathcal{Y}\mathcal{Z}} \leq 2H(X,Y,Z|U_{mcf(X,Y,Z)}) - H(X,Y|Z) - H(X,Z|Y) - H(Y,Z|X), \tag{2.39}$$

where $U_{mcf(X,Y)}$ (resp. $U_{mcf(X,Z)}$, $U_{mcf(Y,Z)}$) is a maximal common function of X and Y (resp. X and Z, Y and Z), and $U_{mcf(X,Y,Z)}$ is a maximal common function of X, Y and Z.

The technical tool used to prove Theorem 2.6 is supplied by Lemma 2.4 below.

Lemma 2.4 *Let $(K_{\mathcal{X}\mathcal{Y}}, K_{\mathcal{X}\mathcal{Z}}, K_{\mathcal{Y}\mathcal{Z}})$ be an ε-PK triple, with values in finite sets $\mathcal{K}_{\mathcal{X}\mathcal{Y}}$, $\mathcal{K}_{\mathcal{X}\mathcal{Z}}$, $\mathcal{K}_{\mathcal{Y}\mathcal{Z}}$, respectively, achieved with communication $\mathbf{F} = (F_1, \cdots, F_{3r})$. Then*

$$\begin{aligned} \frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}}, K_{\mathcal{X}\mathcal{Z}}, K_{\mathcal{Y}\mathcal{Z}}|\mathbf{F}, U^n_{mcf(X,Y,Z)}) &= H(X,Y,Z|U_{mcf(X,Y,Z)}) - (R_X + R_Y + R_Z) \\ &\quad + \frac{3 + 3\varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}}||\mathcal{K}_{\mathcal{X}\mathcal{Z}}||\mathcal{K}_{\mathcal{X}\mathcal{Y}}|}{n} \end{aligned} \tag{2.40}$$

for some (R_X, R_Y, R_Z) satisfying

$$\begin{aligned} R_X &\geq H(X|Y,Z), & R_Y + R_Z &\geq H(Y,Z|X) - \frac{1}{n}H(K_{\mathcal{Y}\mathcal{Z}}), \\ R_Y &\geq H(Y|X,Z), & R_X + R_Z &\geq H(X,Z|Y) - \frac{1}{n}H(K_{\mathcal{X}\mathcal{Z}}), \\ R_Z &\geq H(Z|X,Y), & R_X + R_Y &\geq H(X,Y|Z) - \frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}}). \end{aligned}$$

Proof of Lemma 2.4: Set

$$\begin{aligned} R_X &= \frac{1}{n}\sum_{t:t\ mod\ 3\equiv 1} H(F_t|U^n_{mcf(X,Y,Z)}, F_{[1,t-1]}) + \frac{1}{n}H(X^n|\mathbf{F}, U^n_{mcf(X,Y,Z)}, K_{\mathcal{X}\mathcal{Y}}, K_{\mathcal{X}\mathcal{Z}}) \\ &\quad + \frac{1 + \varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}}||\mathcal{K}_{\mathcal{X}\mathcal{Z}}||\mathcal{K}_{\mathcal{Y}\mathcal{Z}}|}{n}, \\ R_Y &= \frac{1}{n}\sum_{t:t\ mod\ 3\equiv 2} H(F_t|U^n_{mcf(X,Y,Z)}, F_{[1,t-1]}) + \frac{1}{n}H(Y^n|\mathbf{F}, X^n), \\ &\quad + \frac{1 + \varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}}||\mathcal{K}_{\mathcal{X}\mathcal{Z}}||\mathcal{K}_{\mathcal{Y}\mathcal{Z}}|}{n}, \end{aligned}$$

$$\begin{aligned} R_Z &= \frac{1}{n}\sum_{t:t \ mod \ 3\equiv 3} H(F_t|U^n_{mcf(X,Y,Z)}, F_{[1,t-1]}) + \frac{1}{n}H(Z^n|\mathbf{F}, X^n, Y^n), \\ &+\frac{1+\varepsilon\log|\mathcal{K}_{\mathcal{XY}}||\mathcal{K}_{\mathcal{XZ}}||\mathcal{K}_{\mathcal{YZ}}|}{n}. \end{aligned}$$

The remaining proof is analogous to that of Lemma 2.1, and omitted here. ■

Proof of Theorem 2.6: We only show (2.39), as the bounds in (2.36) – (2.38) are already known from Theorem 2.1.

Suppose that $\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}, K^{(n)}_{\mathcal{YZ}}\right)$ represent an ε_n-PK triple, with values in finite sets $\mathcal{K}^{(n)}_{\mathcal{XY}}$, $\mathcal{K}^{(n)}_{\mathcal{XZ}}$, $\mathcal{K}^{(n)}_{\mathcal{YZ}}$, respectively, achieved with communication $\mathbf{F} = (F_1, \cdots, F_{3r})$, where $\varepsilon_n \to 0$ (see Definition 2.6). Then

$$\begin{aligned} &\frac{1}{n}H\left(K^{(n)}_{\mathcal{XY}}\right) + \frac{1}{n}H\left(K^{(n)}_{\mathcal{XZ}}\right) + \frac{1}{n}H\left(K^{(n)}_{\mathcal{YZ}}\right) \\ =\ & \frac{1}{n}H\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}, K^{(n)}_{\mathcal{YZ}}\right) + \frac{1}{n}I\left(K^{(n)}_{\mathcal{XY}} \wedge K^{(n)}_{\mathcal{XZ}}\right) + \frac{1}{n}I\left(K^{(n)}_{\mathcal{YZ}} \wedge K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}\right) \\ =\ & \frac{1}{n}H\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}, K^{(n)}_{\mathcal{YZ}}|\mathbf{F}, U^n_{mcf(X,Y,Z)}\right) + \frac{1}{n}I\left(K^{(n)}_{\mathcal{XY}} \wedge \mathbf{F}, U^n_{mcf(X,Y,Z)}\right) \\ & +\frac{1}{n}I\left(K^{(n)}_{\mathcal{XZ}} \wedge \mathbf{F}, U^n_{mcf(X,Y,Z)}, K^{(n)}_{\mathcal{XY}}\right) + \frac{1}{n}I\left(K^{(n)}_{\mathcal{YZ}} \wedge \mathbf{F}, U^n_{mcf(X,Y,Z)}, K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}\right) \\ \leq\ & \frac{1}{n}H\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}, K^{(n)}_{\mathcal{YZ}}|\mathbf{F}, U^n_{mcf(X,Y,Z)}\right) + 3\varepsilon_n, \end{aligned} \tag{2.41}$$

where the inequality follows since $\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}, K^{(n)}_{\mathcal{YZ}}\right)$ represent an ε_n-PK triple. Now, (2.40) and the latter inequalities in (2.37) – (2.39) imply that

$$\begin{aligned} &\frac{1}{n}H\left(K^{(n)}_{\mathcal{XY}}, K^{(n)}_{\mathcal{XZ}}, K^{(n)}_{\mathcal{YZ}}|\mathbf{F}, U^n_{mcf(X,Y,Z)}\right) \\ \leq\ & H(X,Y,Z|U_{mcf(X,Y,Z)}) - \frac{1}{2}\left[H(X,Y|Z) + H(X,Z|Y) + H(Y,Z|X)\right] \\ & +\frac{1}{2n}\left[H\left(K^{(n)}_{\mathcal{XY}}\right) + H\left(K^{(n)}_{\mathcal{XZ}}\right) + H\left(K^{(n)}_{\mathcal{YZ}}\right)\right] + \frac{3+3\varepsilon_n\log\left|\mathcal{K}^{(n)}_{\mathcal{XY}}\right|\left|\mathcal{K}^{(n)}_{\mathcal{XZ}}\right|\left|\mathcal{K}^{(n)}_{\mathcal{YZ}}\right|}{n}. \end{aligned} \tag{2.42}$$

Putting (2.42) into (2.41), we finish the proof of the theorem. ■

Example 2.5: Let X and Y be $\{0,1\}$-valued rvs with joint pmf

$$P_{XY}(0,0) = P_{XY}(1,1) = \frac{1-p}{2},$$

$$P_{XY}(0,1) = P_{XY}(1,0) = \frac{p}{2},$$

for some $0 < p < 1$. Let $Z = X \oplus Y$. As in Example 2.2, the joint pmf of (X, Y) is indecomposable, and $U_{mcf(X,Y)}$ is independent of (X, Y), which implies that $U_{mcf(X,Y)}$ is a constant. Consequently, $U_{mcf(X,Y,Z)}$ is a constant. Since $I(X \wedge Y | U_{mcf(X,Y)}) = 1 - h_b(p)$, X and Y are deterministically correlated iff $p = \frac{1}{2}$.

It is easily seen that Z is independent of X (resp. Y), which implies that $U_{mcf(X,Z)}$ (resp. $U_{mcf(Y,Z)}$) is a constant. Thus,

$$I(X \wedge Y|Z) = 1, \qquad I(X \wedge Z|Y) = I(Y \wedge Z|X) = h_b(p),$$

$$I(X \wedge Y, Z|U_{mcf(Y,Z)}) = I(Y \wedge X, Z|U_{mcf(X,Z)}) = 1,$$

$$I(Z \wedge X, Y|U_{mcf(X,Y)}) = h_b(p),$$

and

$$2H(X, Y, Z|U_{mcf(X,Y,Z)}) - H(X, Y|Z) - H(X, Z|Y) - H(Y, Z|X) = 1.$$

The outer bound for C_{PK} is, hence, given by (2.36) – (2.39). Figure 2.2 shows this outer bound for C_{PK}.

Next, the tightness of this outer bound is easily seen. It is clear that $(1, 0, 0)$, $(0, h_b(p), 0)$ and $(0, 0, h_b(p))$ are perfectly achievable PK-rate triples (i.e., with $\varepsilon_n = 0$). From Theorem 2.5 and the fact that Y and Z are deterministically correlated, $(1 - h_b(p), h_b(p), 0)$ is also a perfectly achievable PK-rate triple. Similarly, $(1 - h_b(p), 0, h_b(p))$ is another perfectly achievable PK-rate triple. Therefore, by means of a time-sharing argument, every PK-rate triple in the region of Figure 2.2 is also perfectly achievable. ∎

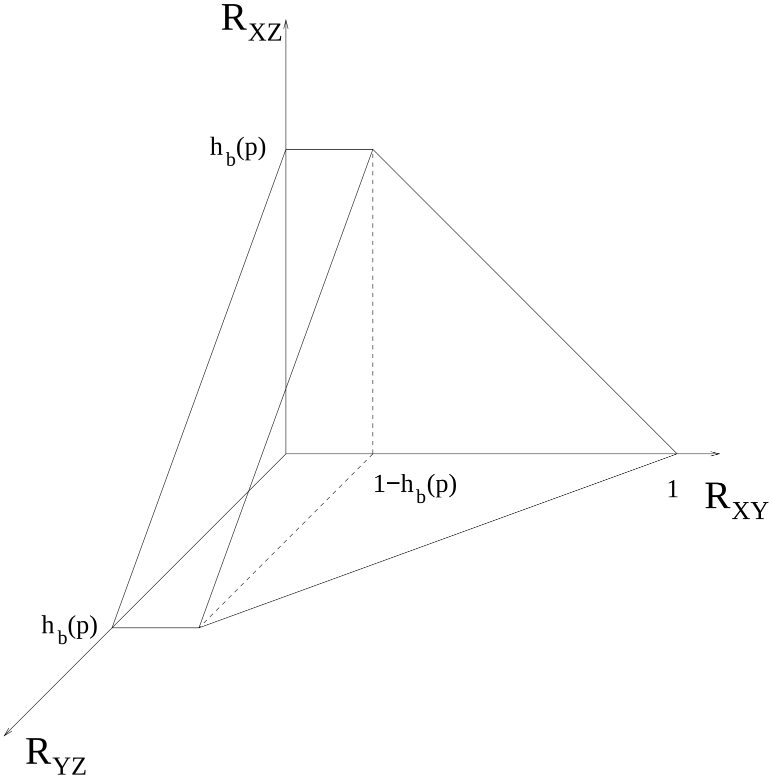


Figure 2.2: The PK-capacity region for Example 2.5.

Chapter 3

The Secret Key–Private Key Capacity Region for Three Terminals

3.1 Introduction

As has already been mentioned in Chapter 2 that there are situations, arising for instance in "group communication," in which multiple keys must be simultaneously devised in a coordinated manner by different groups of terminals (with possible overlaps of groups); such keys need protection from prespecified terminals as also from an eavesdropper. For instance, in group communication, different groups of terminals (with possible overlaps of groups) must generate different keys for encrypted communication within those groups. A key devised for a group must be concealed from terminals outside that group as well as from an eavesdropper. Such "group-wide" keys can be simultaneously devised in a coordinated manner by different groups of terminals. Separate keys for different groups are also needed when certain disabled terminals become unauthorized or unreliable so that the keys assigned to them, in effect, are compromised; to maintain security, the remaining authorized terminals must then switch to another set of keys which are concealed from the disabled terminals. In the interests of efficiency, all such keys must be devised at the outset of operations so as to avoid the need for a fresh key generation procedure after a disablement.

In general, in a network with m terminals, we could have one (common) secret key (SK) for all the terminals, and private keys (PK) for every proper subset of the m terminals. These situations produce a rich vein of secrecy generation problems, the information-theoretic underpinnings of which are substantial enough for investigation already in the case of just three terminals.

In this chapter, we consider a simple model with three terminals and examine the problem of characterizing all the rates at which the following two types of keys can be generated *simultaneously*: (i) all the three terminals generate a SK, which is effectively concealed from an eavesdropper; and (ii) a designated pair of terminals generate a PK, which is effectively concealed from the remaining terminal as well as the eavesdropper. Suppose that terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ observe, respectively, the distinct components of a discrete memoryless multiple source (DMMS), i.e., independent and identically distributed (i.i.d.) repetitions of the generic random variables (rvs) X, Y, Z, respectively. The terminals are permitted unrestricted communication among themselves over a public channel, and all the transmissions are observed by all the terminals. An eavesdropper has access to this public communication too, but gathers no additional (wiretapped) side-information; also, the eavesdropper is passive, i.e., unable to corrupt the transmissions. Terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ generate a SK, which is concealed from the eavesdropper with access to the public communication among the terminals. Also, terminals $\mathcal{X}$ and $\mathcal{Y}$ generate a PK, with the possible help of terminal $\mathcal{Z}$, which is concealed from the helper terminal $\mathcal{Z}$ and from the eavesdropper. The set of all rate pairs at which such (SK, PK) pairs can be generated is called the (SK, PK)-capacity region. Our main technical results are single-letter inner and outer bounds for the (SK, PK)-capacity region. Further, under a certain special condition, these bounds are shown to coincide to yield the (exact) (SK, PK)-capacity region.

This chapter is organized as follows. Section 3.2 contains the preliminaries. Our main results – an outer bound and an inner bound for the (SK, PK)-capacity region – are provided in Section 3.3. Furthermore, under a certain condition, these bounds coincide to yield the (exact) (SK, PK)-capacity region. The proofs are given in Section 3.4. In

Section 3.5, we discuss the tightness of the outer bound.

3.2 Preliminaries

Consider a DMMS with three components, and with corresponding generic rvs X, Y, Z taking values in finite alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, respectively. Let $X^n = (X_1, \cdots, X_n)$, $Y^n = (Y_1, \cdots, Y_n)$, $Z^n = (Z_1, \cdots, Z_n)$ be n i.i.d. repetitions of the rvs X, Y, Z. The terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ respectively observe the components X^n, Y^n, Z^n of the DMMS (X^n, Y^n, Z^n), where n denotes the observation length. The terminals can communicate with each other through broadcasts over a noiseless public channel, possibly interactively in many rounds. We assume, without any loss of generality, that these transmissions occur in consecutive time slots in r rounds; the communication is depicted by $3r$ rvs $F_1, \cdots, F_{3r}$, where F_t denotes the transmission in time slot t, $1 \leq t \leq 3r$, by a terminal assigned an index $i = t \bmod 3$, $1 \leq i \leq 3$, with terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ corresponding to indices 1, 2, 3, respectively. In general, F_t is allowed to be any function, defined in terms of a mapping f_t, of the observations at the terminal with index i, $i = t \bmod 3$, and of the previous transmissions $F_{[1,t-1]} = (F_1, \cdots, F_{t-1})$. We do not permit any randomization at the terminals; in particular, $f_1, \cdots, f_{3r}$ are deterministic mappings. Let $\mathbf{F} = (F_1, \cdots, F_{3r})$ denote collectively all the transmissions in the $3r$ time slots.

The rvs $K_{\mathcal{XYZ}}$ and $K_{\mathcal{XY}}$, which are functions of (X^n, Y^n, Z^n), with finite ranges $\mathcal{K}_{\mathcal{XYZ}}$ and $\mathcal{K}_{\mathcal{XY}}$, respectively, represent an *ε-secret key-private key (ε-(SK, PK))* pair, where the SK $K_{\mathcal{XYZ}}$ is for all the terminals and the PK $K_{\mathcal{XY}}$ is for terminals $\mathcal{X}$, $\mathcal{Y}$ with privacy from the terminal $\mathcal{Z}$, achievable with communication $\mathbf{F}$, if:

- $K_{\mathcal{XYZ}}$ is ε-recoverable from each of $(\mathbf{F}, X^n)$, $(\mathbf{F}, Y^n)$, $(\mathbf{F}, Z^n)$;
- $K_{\mathcal{XY}}$ is ε-recoverable from each of $(\mathbf{F}, X^n)$, $(\mathbf{F}, Y^n)$;

- $K_{\mathcal{XYZ}}$ satisfies the secrecy condition and the uniformity condition

$$\frac{1}{n} I(K_{\mathcal{XYZ}} \wedge \mathbf{F}) \leq \varepsilon; \tag{3.1}$$

$$\frac{1}{n} H(K_{\mathcal{XYZ}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{XYZ}}| - \varepsilon; \tag{3.2}$$

and

- $K_{\mathcal{XY}}$ satisfies the secrecy condition and the uniformity condition

$$\frac{1}{n} I(K_{\mathcal{XY}} \wedge \mathbf{F}, Z^n) \leq \varepsilon; \tag{3.3}$$

$$\frac{1}{n} H(K_{\mathcal{XY}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{XY}}| - \varepsilon. \tag{3.4}$$

The conditions above thus mean that terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ generate a nearly uniformly distributed SK $K_{\mathcal{XYZ}}$ which is concealed from an eavesdropper that observes the public communication $\mathbf{F}$. Simultaneously, *based on the same public communication*, terminals $\mathcal{X}$ and $\mathcal{Y}$ generate a PK $K_{\mathcal{XY}}$ with the terminal $\mathcal{Z}$ acting as helper (e.g., a "third-party" in a key establishment protocol) by providing $\mathcal{X}$, $\mathcal{Y}$ with additional correlated information; this private key is nearly uniformly distributed, and is concealed from an eavesdropper that observes the public communication $\mathbf{F}$ as well as from the helper $\mathcal{Z}$ (hence, "private"). Note that the previous conditions readily imply that $K_{\mathcal{XYZ}}$ and $K_{\mathcal{XY}}$ are "nearly" statistically independent.

Definition 3.1 *A pair of nonnegative numbers ($R_{\mathcal{XYZ}}$, $R_{\mathcal{XY}}$) constitute an achievable (SK, PK)-rate pair if for every $\varepsilon > 0$ and all sufficiently large n, ε-(SK, PK) pairs $(K_{\mathcal{XYZ}}, K_{\mathcal{XY}})$ are achievable with suitable communication (with the number of rounds possibly depending on n), such that $\frac{1}{n} H\left(K_{\mathcal{XYZ}}\right) \geq R_{\mathcal{XYZ}} - \varepsilon$, $\frac{1}{n} H\left(K_{\mathcal{XY}}\right) \geq R_{\mathcal{XY}} - \varepsilon$. The set of all achievable (SK, PK)-rate pairs is the (SK, PK)-capacity region, denoted by $\mathcal{C}_{SP}$.*

Remarks:

1. Maurer [37] pointed out that the secrecy conditions (3.1) and (3.3) were inadequate for cryptographic purposes, and should be strengthened by omission of the factor $\frac{1}{n}$. While all our achievability results below are presented in the "weak sense," they can be established in the stronger sense of [37] by using the techniques developed in [40].

2. The (SK, PK)-capacity region $\mathcal{C}_{SP}$ is a closed convex set. Closedness is obvious from the definition, while convexity follows from a time-sharing argument (cf. [15, p. 242]).

3. If $K_{\mathcal{X}\mathcal{Y}}$ is set equal to a constant in the definition above, i.e., only a (single) ε-SK is generated by terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, then the entropy rate of such a secret key is called an *achievable SK-rate*, and the largest achievable SK-rate is the *SK-capacity.* It is known [17] that the SK-capacity is equal to

$$\min\left\{I(X \wedge Y, Z), I(Y \wedge X, Z), I(Z \wedge X, Y), \frac{1}{2}\left[H(X) + H(Y) + H(Z) - H(X, Y, Z)\right]\right\}. \tag{3.5}$$

4. If $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ is set equal to a constant in the definition above, i.e., only a (single) ε-PK is generated by terminals $\mathcal{X}$ and $\mathcal{Y}$ with terminal $\mathcal{Z}$ serving as a helper terminal, then the entropy rate of such a private key is called an *achievable PK-rate*, and the largest achievable PK-rate is the *PK-capacity.* It is known (cf. [3], [16]) that the PK-capacity is equal to

$$I(X \wedge Y|Z). \tag{3.6}$$

Example 3.1: Let X and Y be independent rvs, each uniformly distributed on $\{0, 1\}$, and let $Z = X \oplus Y$, where $\oplus$ denotes addition modulo 2.

It is easily seen from (3.5) that the SK-capacity for the terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ equals $\frac{1}{2}$ bit/symbol, and from (3.6) that the PK-capacity for the terminals $\mathcal{X}$, $\mathcal{Y}$, with privacy from $\mathcal{Z}$, equals 1 bit/symbol. We claim in this elementary example that 1 bit of *perfect* SK (i.e., ε-SK with $\varepsilon = 0$) is achievable for all the terminals, with observation length $n = 2$, using the following scheme. Terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, with respective observations (X_1, X_2), (Y_1, Y_2), (Z_1, Z_2), transmit X_1, Y_2 and $Z_1 \oplus Z_2$, respectively. Then each terminal can perfectly recover all the observations of the other terminals. The secret key $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ is set to be X_2 (or Y_1 or Z_1 or Z_2). It can be shown that

$$I(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}} \wedge \mathbf{F}) = I(X_2 \wedge X_1, Y_2, Z_1 \oplus Z_2) = 0,$$

and

$$H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}) = 1.$$

On the other hand, it is shown in Example 2.3 that a perfect PK $K_{\mathcal{X}\mathcal{Y}}$ with rate 1 bit/symbol is achievable for terminals $\mathcal{X}$ and $\mathcal{Y}$, with privacy from $\mathcal{Z}$. By a time-sharing argument, every (SK, PK)-rate pair $(R_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, R_{\mathcal{X}\mathcal{Y}})$ satisfying

$$2R_{\mathcal{X}\mathcal{Y}\mathcal{Z}} + R_{\mathcal{X}\mathcal{Y}} \leq 1 \tag{3.7}$$

is perfectly achievable. The results in this chapter (cf. Theorem 3.1 below) will show that the secret key-private key capacity region $\mathcal{C}_{SP}$ for this example cannot be larger than the region in (3.7), so that (3.7) characterizes the capacity region $\mathcal{C}_{SP}$ in this example. ■

3.3 Statement of Results

For notational simplicity, we set

$$A \stackrel{\triangle}{=} I(Z \wedge X, Y),$$

$$B \stackrel{\triangle}{=} \min\{I(X \wedge Y, Z), I(Y \wedge X, Z)\},$$

$$C \stackrel{\triangle}{=} \frac{1}{2}[H(X) + H(Y) + H(Z) - H(X, Y, Z)],$$

Thus, the SK-capacity (3.5) for the terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ is equal to $\min\{A, B, C\}$.

Theorem 3.1 *(Outer bound for $\mathcal{C}_{SP}$): Let $(R_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, R_{\mathcal{X}\mathcal{Y}})$ be an achievable (SK, PK)-rate pair. Then*

$$R_{\mathcal{X}\mathcal{Y}\mathcal{Z}} \leq \min\{A, B, C\}, \tag{3.8}$$

$$R_{\mathcal{X}\mathcal{Y}} \leq I(X \wedge Y|Z), \tag{3.9}$$

$$R_{\mathcal{X}\mathcal{Y}\mathcal{Z}} + R_{\mathcal{X}\mathcal{Y}} \leq B, \tag{3.10}$$

$$2R_{\mathcal{X}\mathcal{Y}\mathcal{Z}} + R_{\mathcal{X}\mathcal{Y}} \leq 2C. \tag{3.11}$$

Remark: The bounds (3.8), (3.9) on the individual largest achievable SK- and PK-rates are directly from (3.5) and (3.6). Also, while (3.5) implies

$$R_{\mathcal{X}\mathcal{Y}\mathcal{Z}} \leq B, \qquad R_{\mathcal{X}\mathcal{Y}\mathcal{Z}} \leq C,$$

note that the conditions (3.10), (3.11) above are more stringent than (3.5).

Theorem 3.2 *(Inner bound for $\mathcal{C}_{SP}$): The (SK, PK)-capacity region $\mathcal{C}_{SP}$ is inner-bounded by the region*

$$\left\{ \begin{array}{ll} (R_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, R_{\mathcal{X}\mathcal{Y}}) : & \frac{\min\{A,B,C\} - \min\{I(X\wedge Z), I(Y\wedge Z)\}}{I(X\wedge Y|Z)} \cdot R_{\mathcal{X}\mathcal{Y}} + R_{\mathcal{X}\mathcal{Y}\mathcal{Z}} \leq \min\{A, B, C\}, \\ & R_{\mathcal{X}\mathcal{Y}} \leq I(X \wedge Y|Z) \end{array} \right\}. \tag{3.12}$$

Remark: The proof of Theorem 3.2 is based on the following idea: a modified version of the random binning technique developed in [17] is first used to generate the needed "common randomness." A SK and a PK, of rate pair $(\min\{I(X \wedge Z), I(Y \wedge Z)\}, I(X \wedge Y|Z))$, are then extracted from this common randomness, by a means from [17]. The achievability of the rate pair above means that besides a PK generated by terminals $\mathcal{X}$ and $\mathcal{Y}$, which approaches the PK-capacity, a SK, of rate $\min\{I(X \wedge Z), I(Y \wedge Z)\}$, can simultaneously be generated by terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$. An application of the time-sharing technique then leads to the achievability of the region in (3.12). Although interterminal communication between $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ is permitted, the region in (3.12) is shown to be achieved by a single autonomous transmission from each terminal based on its own local observation of its component of the DMMS.

Under a certain condition, the outer bound in Theorem 3.1 coincides with the inner bound in Theorem 3.2, which provides a characterization of the (SK, PK)-capacity region $\mathcal{C}_{SP}$.

Theorem 3.3 *If* $\min\{A, B, C\} = B$*, then* $\mathcal{C}_{SP}$ *equals the set of pairs* $(R_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, R_{\mathcal{X}\mathcal{Y}})$ *satisfying (3.9) and (3.10).*

Example 3.2: Let X, Y and Z be rvs, each uniformly distributed on $\{0, 1\}$, and satisfying the Markov condition Y —○— X —○— Z. Further, suppose that

$$P_{XY}(0,0) = P_{XY}(1,1) = \frac{1-p}{2}, \quad P_{XY}(0,1) = P_{XY}(1,0) = \frac{p}{2},$$

$$P_{XZ}(0,0) = P_{XZ}(1,1) = \frac{1-q}{2}, \quad P_{XZ}(0,1) = P_{XZ}(1,0) = \frac{q}{2},$$

where $0 < q < p < \frac{1}{2}$.

Straightforward calculations show that

$$A = I(Z \wedge X, Y) = 1 - h_b(q),$$

$$B = \min\{I(X \wedge Y, Z), I(Y \wedge X, Z)\} = 1 - h_b(p),$$

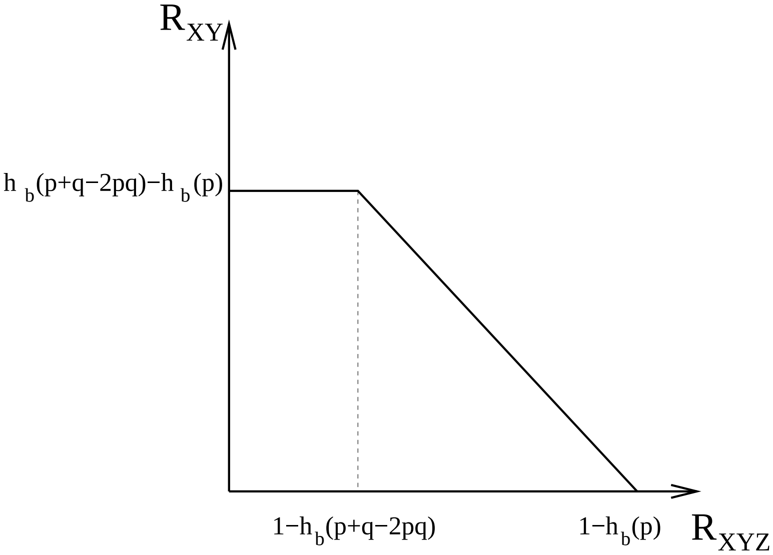


Figure 3.1: $\mathcal{C}_{SP}$ for Example 3.2.

and

$$C = \frac{1}{2}[H(X) + H(Y) + H(Z) - H(X,Y,Z)] = 1 - \frac{h_b(p) + h_b(q)}{2},$$

where $h_b(p) = -p \log_2 p - (1-p)\log_2(1-p)$. Since $0 < q < p < \frac{1}{2}$, we have that $\min\{A, B, C\} = B$. It follows from Theorem 3.3 that $\mathcal{C}_{SP}$ is the set of pairs $(R_{\mathcal{XYZ}}, R_{\mathcal{XY}})$ satisfying

$$\begin{aligned} R_{\mathcal{XY}} &\leq h_b(p+q-2pq) - h_b(p), \\ R_{\mathcal{XYZ}} + R_{\mathcal{XY}} &\leq 1 - h_b(p). \end{aligned}$$

This region is depicted in Figure 3.1. ■

3.4 Proofs

The technical tool used to prove Theorem 3.1 is supplied by Lemma 3.1 below.

Lemma 3.1 *Let* $(K_{\mathcal{XYZ}}, K_{\mathcal{XY}})$ *be an* ε*-(SK, PK) pair (with values in finite sets* $\mathcal{K}_{\mathcal{XYZ}}$

and $\mathcal{K}_{\mathcal{X}\mathcal{Y}}$, respectively), achieved with communication $\mathbf{F} = (F_1, \cdots, F_{3r})$. Then

$$\frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}|\mathbf{F}) = H(X,Y,Z) - (R_X + R_Y + R_Z) + \frac{3 + 3\varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}\mathcal{Z}}||\mathcal{K}_{\mathcal{X}\mathcal{Y}}|}{n} \tag{3.13}$$

for some (R_X, R_Y, R_Z) satisfying

$$R_X \geq H(X|Y,Z), \qquad R_Y + R_Z \geq H(Y,Z|X), \tag{3.14}$$

$$R_Y \geq H(Y|X,Z), \qquad R_X + R_Z \geq H(X,Z|Y), \tag{3.15}$$

$$R_Z \geq H(Z|X,Y), \qquad R_X + R_Y \geq H(X,Y|Z) - \frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}}). \tag{3.16}$$

The proof of Lemma 3.1 is analogous to that of Lemma 2.1. Still, for completeness, a proof is provided below.

Proof of Lemma 3.1: Since $\mathbf{F}$, $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ and $K_{\mathcal{X}\mathcal{Y}}$ are functions of (X^n, Y^n, Z^n),

$$\begin{aligned} H(X^n, Y^n, Z^n) &= H(\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}, X^n, Y^n, Z^n) \\ &= \sum_{t=1}^{3r} H(F_t|F_{[1,t-1]}) + H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}|\mathbf{F}) + H(X^n, Y^n, Z^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}). \end{aligned}$$

Setting

$$\begin{aligned} R_X &= \frac{1}{n}\sum_{t:t \ mod \ 3\equiv 1} H(F_t|F_{[1,t-1]}) + \frac{1}{n}H(X^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}) \\ &\quad + \frac{1 + \varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}\mathcal{Z}}||\mathcal{K}_{\mathcal{X}\mathcal{Y}}|}{n}, \\ R_Y &= \frac{1}{n}\sum_{t:t \ mod \ 3\equiv 2} H(F_t|F_{[1,t-1]}) + \frac{1}{n}H(Y^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}, X^n) \\ &\quad + \frac{1 + \varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}\mathcal{Z}}||\mathcal{K}_{\mathcal{X}\mathcal{Y}}|}{n}, \\ R_Z &= \frac{1}{n}\sum_{t:t \ mod \ 3\equiv 3} H(F_t|F_{[1,t-1]}) + \frac{1}{n}H(Z^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}, X^n, Y^n) \\ &\quad + \frac{1 + \varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}\mathcal{Z}}||\mathcal{K}_{\mathcal{X}\mathcal{Y}}|}{n}, \end{aligned}$$

the previous equality gives

$$\frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}|\mathbf{F}) = H(X,Y,Z) - (R_X + R_Y + R_Z) + \frac{3 + 3\varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}\mathcal{Z}}||\mathcal{K}_{\mathcal{X}\mathcal{Y}}|}{n}.$$

It remains to show that (R_X, R_Y, R_Z) as defined above satisfy (3.14) – (3.16). To this end,

$$\begin{aligned} H(X^n|Y^n,Z^n) &\leq H(\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}, X^n|Y^n,Z^n) \\ &\leq \sum_{t=1}^{3r} H(F_t|Y^n,Z^n,F_{[1,t-1]}) + H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}|\mathbf{F},Y^n,Z^n) \\ &\quad + H(X^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}), \end{aligned} \tag{3.17}$$

Since $t \bmod 3 \neq 1$, F_t is a function of $(Y^n, Z^n, F_{[1,t-1]})$,

$$\begin{aligned} \sum_{t=1}^{3r} H(F_t|Y^n,Z^n,F_{[1,t-1]}) &= \sum_{t:t \ mod \ 3\equiv 1} H(F_t|Y^n,Z^n,F_{[1,t-1]}) \\ &\leq \sum_{t:t \ mod \ 3\equiv 1} H(F_t|F_{[1,t-1]}). \end{aligned}$$

Further, it follows from Fano's inequality that

$$H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}|\mathbf{F},Y^n,Z^n) \leq 1 + \varepsilon \log |\mathcal{K}_{\mathcal{X}\mathcal{Y}\mathcal{Z}}||\mathcal{K}_{\mathcal{X}\mathcal{Y}}|.$$

Upon bounding those terms on the right side of (3.17) from above, we obtain that

$$H(X^n|Y^n,Z^n) \leq nR_X.$$

Again, from Fano's inequality, we show the latter part of (3.14) below.

$$\begin{aligned} H(Y^n,Z^n|X^n) &\leq H(\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}, Y^n,Z^n|X^n) \\ &= \sum_{t:t \ mod \ 3\equiv 2,3} H(F_t|X^n,F_{[1,t-1]}) + H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}|\mathbf{F},X^n) \\ &\quad + H(Y^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}, X^n) + H(Z^n|\mathbf{F}, K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}, X^n, Y^n) \\ &\leq n(R_Y + R_Z). \end{aligned}$$

By means of similar arguments used in the proof of (3.14), we can show (3.15) and (3.16) as follows:

$$H(Y^n|X^n,Z^n) \leq \sum_{t:t \ mod \ 3\equiv 2} H(F_t|X^n,Z^n,F_{[1,t-1]}) + H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}, K_{\mathcal{X}\mathcal{Y}}|\mathbf{F},X^n,Z^n)$$

$$
\begin{aligned}
&+H(Y^n|\mathbf{F}, K_{\mathcal{XYZ}}, K_{\mathcal{XY}}, X^n, Z^n) \\
\leq\ & nR_Y,
\end{aligned}
$$

$$
\begin{aligned}
H(X^n, Z^n|Y^n) \ \leq\ & H(\mathbf{F}|Y^n) + H(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}|\mathbf{F}, Y^n) + H(X^n|\mathbf{F}, K_{\mathcal{XYZ}}, K_{\mathcal{XY}}, Y^n) \\
& + H(Z^n|\mathbf{F}, K_{\mathcal{XYZ}}, K_{\mathcal{XY}}, X^n, Y^n) \\
\leq\ & n(R_X + R_Z),
\end{aligned}
$$

$$
\begin{aligned}
H(Z^n|X^n, Y^n) \ \leq\ & \sum_{t:t\ mod\ 3 \equiv 3} H(F_t|X^n, Y^n, F_{[1,t-1]}) + H(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}|\mathbf{F}, X^n, Y^n) \\
& + H(Z^n|\mathbf{F}, K_{\mathcal{XYZ}}, K_{\mathcal{XY}}, X^n, Y^n) \\
\leq\ & nR_Z,
\end{aligned}
$$

$$
\begin{aligned}
H(X^n, Y^n|Z^n) \ \leq\ & H(\mathbf{F}|Z^n) + H(K_{\mathcal{XYZ}}|\mathbf{F}, Z^n) + H(K_{\mathcal{XY}}|\mathbf{F}, K_{\mathcal{XYZ}}, Z^n) \\
& + H(X^n|\mathbf{F}, K_{\mathcal{XYZ}}, K_{\mathcal{XY}}, Z^n) + H(Y^n|\mathbf{F}, K_{\mathcal{XYZ}}, K_{\mathcal{XY}}, X^n, Z^n) \\
\leq\ & n(R_X + R_Y) + H(K_{\mathcal{XY}}).
\end{aligned}
$$

This completes the proof of the lemma. ■

Proof of Theorem 3.1: We only show (3.10) and (3.11), as (3.8) and (3.9) are from (3.6) and (3.7). Given an (arbitrary) $\varepsilon > 0$, suppose that $(K_{\mathcal{XYZ}}, K_{\mathcal{XY}})$ represent an ε-(SK, PK) pair (with values in finite sets $\mathcal{K}_{\mathcal{XYZ}}$ and $\mathcal{K}_{\mathcal{XY}}$, respectively), achieved with communication $\mathbf{F} = (F_1, \cdots, F_{3r})$. Then

$$
\begin{aligned}
& \frac{1}{n}H\left(K_{\mathcal{XYZ}}\right) + \frac{1}{n}H\left(K_{\mathcal{XY}}\right) \\
=\ & \frac{1}{n}H\left(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}\right) + \frac{1}{n}I\left(K_{\mathcal{XYZ}} \wedge K_{\mathcal{XY}}\right) \\
=\ & \frac{1}{n}H\left(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}|\mathbf{F}\right) + \frac{1}{n}I\left(K_{\mathcal{XYZ}} \wedge \mathbf{F}\right) + \frac{1}{n}I\left(K_{\mathcal{XY}} \wedge \mathbf{F}, K_{\mathcal{XYZ}}\right) \\
\leq\ & \frac{1}{n}H\left(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}|\mathbf{F}\right) + \frac{1}{n}I\left(K_{\mathcal{XYZ}} \wedge \mathbf{F}\right) + \frac{1}{n}I\left(K_{\mathcal{XY}} \wedge \mathbf{F}, Z^n\right) + \frac{1}{n}H\left(K_{\mathcal{XYZ}}|\mathbf{F}, Z^n\right) \\
\leq\ & \frac{1}{n}H\left(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}|\mathbf{F}\right) + 2\varepsilon + \frac{1 + \varepsilon \log|\mathcal{K}_{\mathcal{XYZ}}|}{n}, \qquad (3.18)
\end{aligned}
$$

where (3.18) follows from secrecy conditions (3.1), (3.3) and Fano's inequality.

Next, we shall bound $\frac{1}{n}H\left(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}|\mathbf{F}\right)$ from above using Lemma 3.1. It is implied by (3.13) and (3.14) that

$$\begin{aligned} & \frac{1}{n}H\left(K_{\mathcal{XYZ}}, K_{\mathcal{XY}}|\mathbf{F}\right) \\ \leq \quad & H(X,Y,Z) - [H(X|Y,Z) + H(Y,Z|X)] + \frac{3+3\varepsilon\log|\mathcal{K}_{\mathcal{XYZ}}|\,|\mathcal{K}_{\mathcal{XY}}|}{n} \\ = \quad & I(X \wedge Y,Z) + \frac{3+3\varepsilon\log|\mathcal{K}_{\mathcal{XYZ}}|\,|\mathcal{K}_{\mathcal{XY}}|}{n}. \qquad (3.19) \end{aligned}$$

Putting (3.19) into (3.18), we obtain that

$$\frac{1}{n}H\left(K_{\mathcal{XYZ}}\right) + \frac{1}{n}H\left(K_{\mathcal{XY}}\right) \leq I(X \wedge Y,Z) + 2\varepsilon + \frac{4+4\varepsilon\log|\mathcal{K}_{\mathcal{XYZ}}|\,|\mathcal{K}_{\mathcal{XY}}|}{n}.$$

Similarly, it follows from (3.13), (3.15) and (3.18) that

$$\frac{1}{n}H\left(K_{\mathcal{XYZ}}\right) + \frac{1}{n}H\left(K_{\mathcal{XY}}\right) \leq I(Y \wedge X,Z) + 2\varepsilon + \frac{4+4\varepsilon\log|\mathcal{K}_{\mathcal{XYZ}}|\,|\mathcal{K}_{\mathcal{XY}}|}{n},$$

which leads to (3.10).

Finally, from the latter inequalities of (3.14) – (3.16), we have

$$R_X + R_Y + R_Z \geq \frac{1}{2}\left[H(X,Y|Z) + H(X,Z|Y) + H(Y,Z|X) - \frac{1}{n}H\left(K_{\mathcal{XY}}\right)\right]. \qquad (3.20)$$

A comparison of (3.13), (3.18) and (3.20) shows that

$$\frac{2}{n}H\left(K_{\mathcal{XYZ}}\right)+\frac{1}{n}H\left(K_{\mathcal{XY}}\right) \leq H(X)+H(Y)+H(Z)-H(X,Y,Z)+4\varepsilon+\frac{8+8\varepsilon\log|\mathcal{K}_{\mathcal{XYZ}}|\,|\mathcal{K}_{\mathcal{XY}}|}{n},$$

proving (3.11). ■

In order to prove Theorem 3.2, we first show the achievability of a (SK,PK) pair, of rate

$$(\min\{I(X \wedge Z), I(Y \wedge Z)\}, I(X \wedge Y|Z)),$$

which is Lemma 3.2. The following proposition is a technical tool used to prove Lemma 3.2.

Proposition 3.1 *Let $X^n = (X_1, \cdots, X_n)$, $Y^n = (Y_1, \cdots, Y_n)$ and $Z^n = (Z_1, \cdots, Z_n)$ be n i.i.d. repetitions of rvs X, Y and Z with (known) joint pmf P_{XYZ}. For every $\varepsilon > 0$, $\nu > 0$, and all sufficiently large n, there exists a source code $(f_{\mathcal{X}}, f_{\mathcal{Z}}, \phi)$, where $f_{\mathcal{X}} : \mathcal{X}^n \to \{1, \cdots, b_1(n)\}$, $f_{\mathcal{Z}} : \mathcal{Z}^n \to \{1, \cdots, b_2(n)\}$, $\phi : \mathcal{Y}^n \times \{1, \cdots, b_1(n)\} \times \{1, \cdots, b_2(n)\} \to \mathcal{X}^n \times \mathcal{Z}^n$, such that*

$$\Pr\{\phi(Y^n, f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n)) = (X^n, Z^n)\} \geq 1 - \varepsilon, \tag{3.21}$$

$$\frac{1}{n} \log ||f_{\mathcal{X}}(X^n)|| \leq H(X|Y, Z) + \nu. \tag{3.22}$$

Further, for every such source code,

$$\frac{1}{n} I(f_{\mathcal{X}}(X^n) \wedge Y^n, Z^n) \leq \nu + \varepsilon \log |\mathcal{X}| + \frac{1}{n} h_b(\varepsilon).$$

Proof of Proposition 3.1: The existence part in (3.21), (3.22) follows directly from the Slepian-Wolf Theorem (cf. [15, Theorem 3.1.14], [65]). Next, let

$$(f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n), \phi(Y^n, f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n)))$$

be a source code satisfying (3.21) and (3.22). Then, it follows from Fano's inequality that

$$H(X^n | f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n), Y^n) \leq h_b(\varepsilon) + n\varepsilon \log |\mathcal{X}|.$$

From (3.22) and the inequality above, we have

$$\begin{aligned} H(f_{\mathcal{X}}(X^n)) &\leq nH(X|Y, Z) + n\nu \\ &= H(X^n, f_{\mathcal{X}}(X^n) | Y^n, Z^n) + n\nu \\ &= H(f_{\mathcal{X}}(X^n) | Y^n, Z^n) + H(X^n | f_{\mathcal{X}}(X^n), Y^n, Z^n) + n\nu \\ &\leq H(f_{\mathcal{X}}(X^n) | Y^n, Z^n) + n\nu + n\varepsilon \log |\mathcal{X}| + h_b(\varepsilon). \end{aligned}$$

Therefore,

$$\frac{1}{n} I(f_{\mathcal{X}}(X^n) \wedge Y^n, Z^n) \leq \nu + \varepsilon \log |\mathcal{X}| + \frac{1}{n} h_b(\varepsilon).$$

■

Lemma 3.2 *It holds that*

$$(\min \{I(X \wedge Z), I(Y \wedge Z)\}, I(X \wedge Y|Z)) \tag{3.23}$$

is an achievable (SK, PK)-rate pair.

Proof of Lemma 3.2: The idea underlying the proof is as follows. First, terminal $\mathcal{Z}$ helps terminals $\mathcal{X}$ and $\mathcal{Y}$ generate a PK at rate $I(X \wedge Y|Z)$, by not revealing "all" of Z^n at rate $H(Z)$, but at rate $\max\{H(Z|X), H(Z|Y)\}$. Then, the "remainder" of Z^n, of rate $\min\{I(X \wedge Z), I(Y \wedge Z)\}$, can be used for simultaneous SK-generation by terminals $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$.

We now provide a formal proof. Without loss of generality, assume that $I(X \wedge Z) \leq I(Y \wedge Z)$. Then (3.23) becomes

$$(I(X \wedge Z), I(X \wedge Y|Z)).$$

Consider random partitions of X^n and Z^n into b_1 and b_2 bins, where $b_1 = b_1(n)$ and $b_2 = b_2(n)$ are two integers to be specified later. For each $x^n \in \mathcal{X}^n$ (resp. $z^n \in \mathcal{Z}^n$), let $F_{\mathcal{X}}(x^n)$ (resp. $F_{\mathcal{Z}}(z^n)$) be the random index of the bin containing x^n (resp. z^n), where $F_{\mathcal{X}}(x^n)$ (resp. $F_{\mathcal{Z}}(z^n)$) is uniformly distributed on the set of integers $\{1, \cdots, b_1\}$ (resp. $\{1, \cdots, b_2\}$). Then, clearly $F_{\mathcal{X}}(x^n)$, $x^n \in \mathcal{X}^n$ are mutually independent, as are $F_{\mathcal{Z}}(z^n)$, $z^n \in \mathcal{Z}^n$. Furthermore, assume that $(F_{\mathcal{X}}(x^n), x^n \in \mathcal{X}^n)$, $(F_{\mathcal{Z}}(z^n), z^n \in \mathcal{Z}^n)$ and (X^n, Y^n, Z^n) are mutually independent.

Terminals $\mathcal{X}$ and $\mathcal{Z}$, with respective observations x^n and z^n, transmit random indices $F_{\mathcal{X}}(x^n) = J_{\mathcal{X}}$ and $F_{\mathcal{Z}}(z^n) = J_{\mathcal{Z}}$, where $J_{\mathcal{X}}$ and $J_{\mathcal{Z}}$ are uniformly distributed on $\{1, \cdots, b_1\}$ and $\{1, \cdots, b_2\}$, respectively.

The decoding at terminal $\mathcal{X}$ is performed as follows. Fix $\xi > 0$. Terminal $\mathcal{X}$, upon observing $x^n \in \mathcal{X}^n$ as well as receiving the integer $j_{\mathcal{Z}}$, decodes according to the decoding rule $\phi_{\mathcal{X}}$, defined by

$$\phi_{\mathcal{X}}(x^n, j_{\mathcal{Z}}) = \hat{z}^n,$$

iff $\hat{z}^n$ is the unique element in $\mathcal{Z}^n$ such that

- $(x^n, \hat{z}^n) \in T^n_{XZ,\xi}$; and
- $F_{\mathcal{Z}}(z^n) = j_{\mathcal{Z}}$.

If no such $\hat{z}^n$ exists, an error is declared.

The probability of decoding error at terminal $\mathcal{X}$ is then

$$P^{(n)}_{e,\mathcal{X}} = \Pr\left\{\phi_{\mathcal{X}}(X^n, F_{\mathcal{Z}}(Z^n)) \neq Z^n\right\}.$$

Define the events

$$E_0 = \{(X^n, Z^n) \notin T^n_{XZ,\xi}\},$$

$$E_1 = \{\exists \tilde{z}^n \in \mathcal{Z}^n : Z^n \neq \tilde{z}^n; F_{\mathcal{Z}}(Z^n) = F_{\mathcal{Z}}(\tilde{z}^n); (X^n, \tilde{z}^n), (X^n, Z^n) \in T^n_{XZ,\xi}\}.$$

Clearly,

$$P^{(n)}_{e,\mathcal{X}} = \Pr\{E_0\} + \Pr\{E_1\},$$

noting that the events E_0 and E_1 are disjoint. By the Asymptotic Equipartition Property (AEP) (cf. e.g. [11, p. 51]), for every $\varepsilon > 0$ and all sufficiently large n, $\Pr\{E_0\} < \frac{\varepsilon}{6}$. To bound $\Pr\{E_1\}$, we have

$$\Pr\{E_1\} \quad = \sum_{(x^n,z^n)\in T^n_{XZ,\xi}} \Pr\{(X^n, Z^n) = (x^n, z^n)\}$$

$$
\begin{aligned}
& \cdot \sum_{\tilde{z}^n \neq z^n : (x^n, \tilde{z}^n) \in T^n_{XZ,\xi}} \Pr\left\{ F_{\mathcal{Z}}(\tilde{z}^n) = F_{\mathcal{Z}}(z^n) | (X^n, Z^n) = (x^n, z^n) \right\} \\
= & \sum_{(x^n, z^n) \in T^n_{XZ,\xi}} \Pr\{(X^n, Z^n) = (x^n, z^n)\} \sum_{\tilde{z}^n \neq z^n : (x^n, \tilde{z}^n) \in T^n_{XZ,\xi}} b_2^{-1} \qquad (3.24) \\
\leq & \sum_{(x^n, z^n) \in T^n_{XZ,\xi}} \Pr\{(X^n, Z^n) = (x^n, z^n)\} \cdot 2^{n[H(Z|X)+2\xi]} \cdot b_2^{-1} \qquad (3.25) \\
\leq & \; 2^{-n[\frac{1}{n} \log b_2 - H(Z|X) - 2\xi]}, \qquad (3.26)
\end{aligned}
$$

where (3.24) follows from the independence of $F_{\mathcal{Z}}(z^n)$ and (X^n, Z^n), and (3.25) follows from (A.1).

The decoding at terminal $\mathcal{Y}$ is performed as follows. Terminal $\mathcal{Y}$, upon observing $y^n \in \mathcal{Y}^n$ as well as receiving the integers $j_{\mathcal{X}}$ and $j_{\mathcal{Z}}$, decodes according to the decoding rule $\phi_{\mathcal{Y}}$, defined by

$$\phi_{\mathcal{Y}}(y^n, j_{\mathcal{X}}, j_{\mathcal{Z}}) = (\hat{x}^n, \hat{z}^n),$$

iff $(\hat{x}^n, \hat{z}^n)$ is the unique element in $\mathcal{X}^n \times \mathcal{Z}^n$ such that

- $(\hat{x}^n, y^n, \hat{z}^n) \in T^n_{XYZ,\xi}$; and
- $F_{\mathcal{X}}(x^n) = j_{\mathcal{X}}$, $F_{\mathcal{Z}}(z^n) = j_{\mathcal{Z}}$.

If no such $(\hat{x}^n, \hat{z}^n)$ exists, an error is declared.

The probability of decoding error at terminal $\mathcal{Y}$ is then

$$P^{(n)}_{e,\mathcal{Y}} = \Pr\left\{ \phi_{\mathcal{Y}}(Y^n, F_{\mathcal{X}}(X^n), F_{\mathcal{Z}}(Z^n)) \neq (X^n, Z^n) \right\}.$$

Define the events

$$E_2 = \{(X^n, Y^n, Z^n) \notin T^n_{XYZ,\xi}\},$$

$$E_3 = \{\exists \tilde{x}^n \in \mathcal{X}^n : X^n \neq \tilde{x}^n; F_{\mathcal{X}}(X^n) = F_{\mathcal{X}}(\tilde{x}^n); (\tilde{x}^n, Y^n, Z^n), (X^n, Y^n, Z^n) \in T^n_{XYZ,\xi}\},$$

$$E_4 = \{\exists \tilde{z}^n \in \mathcal{Z}^n : Z^n \neq \tilde{z}^n; F_{\mathcal{Z}}(Z^n) = F_{\mathcal{Z}}(\tilde{z}^n); (X^n, Y^n, \tilde{z}^n), (X^n, Y^n, Z^n) \in T^n_{XYZ,\xi}\},$$

and

$$E_5 = \{\exists (\tilde{x}^n, \tilde{z}^n) \in \mathcal{X}^n \times \mathcal{Z}^n : X^n \neq \tilde{x}^n; Z^n \neq \tilde{z}^n; F_{\mathcal{X}}(X^n) = F_{\mathcal{X}}(\tilde{x}^n);$$

$$F_{\mathcal{Z}}(Z^n) = F_{\mathcal{Z}}(\tilde{z}^n); (\tilde{x}^n, Y^n, \tilde{z}^n), (X^n, Y^n, Z^n) \in T^n_{XYZ,\xi}\}.$$

Clearly,

$$P^{(n)}_{e,\mathcal{Y}} = \Pr\left\{\bigcup_{i=2}^{5} E_i\right\} \le \sum_{i=2}^{5} \Pr\{E_i\}.$$

By the AEP, for all sufficiently large n, $\Pr\{E_2\} < \frac{\varepsilon}{6}$. To bound $\Pr\{E_3\}$, we have

$$\begin{aligned}
& \Pr\{E_3\} \\
= & \sum_{(x^n,y^n,z^n)\in T^n_{XYZ,\xi}} \Pr\{(X^n,Y^n,Z^n) = (x^n,y^n,z^n)\} \\
& \cdot \sum_{\tilde{x}^n \neq x^n : (\tilde{x}^n,y^n,z^n)\in T^n_{XYZ,\xi}} \Pr\left\{F_{\mathcal{X}}(\tilde{x}^n) = F_{\mathcal{X}}(x^n) | (X^n,Y^n,Z^n) = (x^n,y^n,z^n)\right\} \\
= & \sum_{(x^n,y^n,z^n)\in T^n_{XYZ,\xi}} \Pr\{(X^n,Y^n,Z^n) = (x^n,y^n,z^n)\} \sum_{\tilde{x}^n \neq x^n : (\tilde{x}^n,y^n,z^n)\in T^n_{XYZ,\xi}} b_1^{-1} \\
\le & \sum_{(x^n,y^n,z^n)\in T^n_{XYZ,\xi}} \Pr\{(X^n,Y^n,Z^n) = (x^n,y^n,z^n)\} \cdot 2^{n[H(X|Y,Z)+2\xi]} \cdot b_1^{-1} \\
\le & 2^{-n[\frac{1}{n}\log b_1 - H(X|Y,Z) - 2\xi]}. \qquad (3.27)
\end{aligned}$$

Similarly, we have

$$\Pr\{E_4\} \le 2^{-n[\frac{1}{n}\log b_2 - H(Z|X,Y) - 2\xi]}, \qquad (3.28)$$

and

$$\Pr\{E_5\} \le 2^{-n[\frac{1}{n}\log b_1 b_2 - H(X,Z|Y) - 2\xi]}. \qquad (3.29)$$

Upon picking the integers b_1, b_2 so as to satisfy

$$\frac{1}{n}\log b_1 \ge H(X|Y,Z) + 3\xi, \qquad (3.30)$$

$$\frac{1}{n}\log b_2 \ge H(Z|X) + 3\xi, \qquad (3.31)$$

it follows from (3.26) – (3.29) that for all sufficiently large n, $\Pr\{E_i\}$ is less than $\frac{\varepsilon}{6}$, $i \in \{1,3,4,5\}$. Hence, there exists of a pair of (deterministic) mappings $f_{\mathcal{X}} = f_{\mathcal{X}}(X^n)$ and $f_{\mathcal{Z}} = f_{\mathcal{Z}}(Z^n)$ satisfying

$$\Pr\left\{\phi_{\mathcal{X}}\left(X^n, f_{\mathcal{Z}}(Z^n)\right) \neq Z^n\right\} + \Pr\left\{\phi_{\mathcal{Y}}\left(Y^n, f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n)\right) \neq (X^n, Z^n)\right\} \le \varepsilon. \qquad (3.32)$$

Next, apply Lemma 2.3 with X, Z and $f_{\mathcal{X}}$ in the roles of U, V and f, with $R = \frac{1}{n}\log b_1$ and $H = H(X|Z) - \frac{1}{n}\log b_1 - \xi$, respectively. The following holds with probability exponentially tending to 1 in n. There exists a mapping $g_{\mathcal{X}} : \mathcal{X}^n \to \{1, \cdots, 2^{n[H(X|Z)-\frac{1}{n}\log b_1 - \xi]}\}$ such that $g_{\mathcal{X}}(X^n)$ is uniformly distributed and $g_{\mathcal{X}}(X^n)$ is independent of $(f_{\mathcal{X}}(X^n), Z^n)$.

Apply Lemma 2.3 again with Z, a constant and $f_{\mathcal{Z}}$ in the roles of U, V and f, with $R = \frac{1}{n}\log b_2$ and $H = H(Z) - \frac{1}{n}\log b_2 - \xi$, respectively. The following holds with probability exponentially tending to 1 in n. There exists a mapping $g_{\mathcal{Z}} : \mathcal{Z}^n \to \{1, \cdots, 2^{n[H(Z)-\frac{1}{n}log b_2 - \xi]}\}$ such that $g_{\mathcal{Z}}(Z^n)$ is uniformly distributed and $g_{\mathcal{Z}}(Z^n)$ is independent of $f_{\mathcal{Z}}(Z^n)$.

If no decoding error is declared by terminals $\mathcal{X}$ or $\mathcal{Y}$, the SK $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ is set as $g_{\mathcal{Z}}(Z^n)$ and the PK $K_{\mathcal{X}\mathcal{Y}}$ is set as $g_{\mathcal{X}}(X^n)$. Otherwise, the SK is set to be uniformly distributed on $\{1, \cdots, 2^{n[H(Z)-\frac{1}{n}\log b_2 - \xi]}\}$ and the PK is set to be uniformly distributed on

$$\{1, \cdots, 2^{n[H(X|Z)-\frac{1}{n}\log b_1 - \xi]}\},$$

independent of (X^n, Y^n, Z^n).

Since the sum of the decoding errors at terminals $\mathcal{X}$ and $\mathcal{Y}$ is less than ε by (3.32), $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ is ε-recoverable from the data available at terminals $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$, and $K_{\mathcal{X}\mathcal{Y}}$ is ε-recoverable from the data available at terminals $\mathcal{X}$ and $\mathcal{Y}$.

Clearly, if a decoding error is declared by terminal $\mathcal{X}$ or $\mathcal{Y}$, $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ and $K_{\mathcal{X}\mathcal{Y}}$ satisfy the secrecy conditions (3.1), (3.3), and the uniformity conditions (3.2), (3.4). Further, the lower bounds on $\frac{1}{n}\log b_1$ and $\frac{1}{n}\log b_2$ in (3.30), (3.32) imply that

$$\begin{aligned} \frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}) &= H(Z) - \frac{1}{n}\log b_2 - \xi \le I(X \wedge Z) - 4\xi, &(3.33)\\ \frac{1}{n}H(K_{\mathcal{X}\mathcal{Y}}) &= H(X|Z) - \frac{1}{n}\log b_1 - \xi \le I(X \wedge Y|Z) - 4\xi. &(3.34) \end{aligned}$$

If no decoding error is declared by both $\mathcal{X}$ and $\mathcal{Y}$, $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ and $K_{\mathcal{X}\mathcal{Y}}$ also satisfy the uniformity conditions (3.2), (3.4), with respective rates satisfying (3.33) and (3.34). It remains to show in this case that $K_{\mathcal{X}\mathcal{Y}\mathcal{Z}}$ and $K_{\mathcal{X}\mathcal{Y}}$ satisfy the secrecy conditions (3.1) and (3.3). With $\mathbf{F} = (f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n))$, it is clear that

$$I(K_{\mathcal{X}\mathcal{Y}} \wedge \mathbf{F}, Z^n) = I(g_{\mathcal{X}}(X^n) \wedge f_{\mathcal{X}}(X^n), Z^n) \leq \varepsilon,$$

for all sufficiently large n. Also,

$$\begin{aligned} I(K_{\mathcal{X}\mathcal{Y}\mathcal{Z}} \wedge \mathbf{F}) &= I(g_{\mathcal{Z}}(Z^n) \wedge f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n)) \\ &\leq I(g_{\mathcal{Z}}(Z^n) \wedge f_{\mathcal{Z}}(Z^n)) + I(f_{\mathcal{X}}(X^n) \wedge f_{\mathcal{Z}}(Z^n), g_{\mathcal{Z}}(Z^n)) \\ &\leq I(g_{\mathcal{Z}}(Z^n) \wedge f_{\mathcal{Z}}(Z^n)) + I(f_{\mathcal{X}}(X^n) \wedge Z^n). \end{aligned}$$

It is clear that

$$I(g_{\mathcal{Z}}(Z^n) \wedge f_{\mathcal{Z}}(Z^n)) \leq \varepsilon,$$

for all sufficiently large n. Since

$$\Pr\left\{\phi_{\mathcal{Y}}\left(Y^n, f_{\mathcal{X}}(X^n), f_{\mathcal{Z}}(Z^n)\right) \neq (X^n, Z^n)\right\} \leq \varepsilon$$

by (3.32), and $\frac{1}{n}\log||f_{\mathcal{X}}(X^n)||$ is arbitrarily close to $H(X|Y,Z)$ by (3.30), it follows from Proposition 1 that

$$I(f_{\mathcal{X}}(X^n) \wedge Z^n) \leq n\varepsilon.$$

This completes the proof of Lemma 3.2. ■

Remark: Note that the (SK, PK)-rate pair (3.23) is shown to be achieved by a single autonomous transmission from each terminal based on its own local observation of its component of the DMMS.

Proof of Theorem 3.2: Since $(\min\{A, B, C\}, 0)$, $(0, I(X \wedge Y|Z))$ and

$$\left(\min\left\{I(X \wedge Z), I(Y \wedge Z)\right\}, I(X \wedge Y|Z)\right)$$

are achievable (SK, PK)-rate pairs, it follows from a time-sharing argument that any (SK, PK)-rate pair inside the region (3.12) is achievable. Further, it is known [17] that there is no need for interactive communication to achieve (SK, PK)-rate pairs $(\min\{A, B, C\}, 0)$ and $(0, I(X \wedge Y|Z))$. Hence, one round of transmission (in any order) is sufficient to achieve any (SK, PK)-rate pair in this region. ∎

Proof of Theorem 3.3: Consider the outer bound for $\mathcal{C}_{SP}$ in Theorem 3.1. Under the condition $\min\{A, B, C\} = B$, the constraints (3.8) and (3.11) are implied by the constraint (3.10). Hence, the outer bound for $\mathcal{C}_{SP}$ is determined by (3.9) and (3.10).

On the other hand, considering that

$$\min\{A, B, C\} = B = I(X \wedge Y|Z) + \min\{I(X \wedge Z), I(Y \wedge Z)\},$$

the region (3.12) reduces to the constraints (3.9) and (3.10). ∎

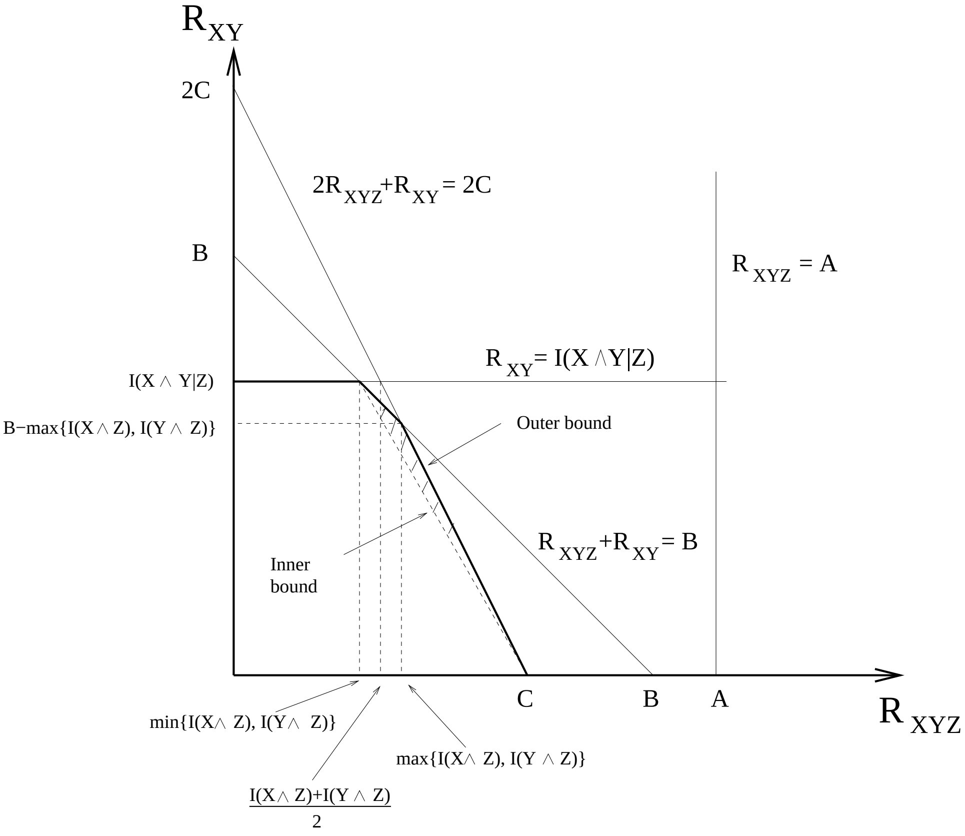
3.5 Discussion

Although we have shown the tightness of the outer bound for $\mathcal{C}_{SP}$ under the condition $\min\{A, B, C\} = B$, it remains open as to whether this outer bound is tight in general. To prove its tightness, it would suffice to show the tightness of the outer bound under the condition $\min\{A, B, C\} = \min\{A, C\}$.

Case 1: $\min\{A, B, C\} = C$:

Under this condition, the constraint (3.8) is implied by the constraint (3.11). Thus, the outer bound for the (SK, PK)-capacity region is given by the constraints (3.9), (3.10) and (3.11), and is depicted in Figure 3.2. By a time-sharing argument, to show the achievability of this region, it suffices to show that (SK, PK)-rate pairs $(0, I(X \wedge Y|Z))$, $(C, 0)$,

$$\left(\min\left\{I(X \wedge Z), I(Y \wedge Z)\right\}, I(X \wedge Y|Z)\right),$$



R_XY
2C
$2R_{XYZ}+R_{XY} = 2C$
B
$R_{XYZ} = A$
$R_{XY}= I(X \wedge Y|Z)$
$I(X \wedge Y|Z)$
$B-\max\{I(X \wedge Z), I(Y \wedge Z)\}$
Outer bound
$R_{XYZ}+R_{XY}= B$
Inner bound
C
B
A
R_XYZ
$\min\{I(X \wedge Z), I(Y \wedge Z)\}$
$\max\{I(X \wedge Z), I(Y \wedge Z)\}$
$\frac{I(X \wedge Z)+I(Y \wedge Z)}{2}$

Figure 3.2: Inner and outer bounds for $\mathcal{C}_{SP}$ for Case 1.

and

$$(\max\{I(X \wedge Z), I(Y \wedge Z)\}, B - \max\{I(X \wedge Z), I(Y \wedge Z)\}) \tag{3.35}$$

are all achievable. While the first three (SK, PK)-rate pairs are known to be achievable, it is unclear if the achievability of the (SK, PK)-rate pair (3.35) holds.

Case 2: $A < B < C$:

Upon writing C as

$$\frac{1}{2}[I(X \wedge Z) + I(Y \wedge X, Z)]$$

or

$$\frac{1}{2}[I(Y \wedge Z) + I(X \wedge Y, Z)],$$

we obtain from $B < C$ that

$$I(X \wedge Z) > I(Y \wedge X, Z), \tag{3.36}$$

or

$$I(Y \wedge Z) > I(X \wedge Y, Z). \tag{3.37}$$

On the other hand, upon writing C as

$$\frac{1}{2}[I(X \wedge Y) + I(Z \wedge X, Y)],$$

we obtain from $A < C$ that

$$I(X \wedge Y) > I(Z \wedge X, Y). \tag{3.38}$$

A contradiction arises when comparing (3.36), (3.38) or (3.37), (3.38). Therefore, the condition $C > \max(A, B)$ is not true.

Case 3: $A < C \leq B$:

The outer bound for the (SK, PK)-capacity region under this condition is depicted in Figure 3.3. To show that this region is achievable, it suffices to show the achievability of (SK, PK)-rate pairs $(0, I(X \wedge Y|Z))$, $(A, 0)$,

$$\left(\min\left\{I(X \wedge Z), I(Y \wedge Z)\right\}, I(X \wedge Y|Z)\right),$$

$$(\max\{I(X \wedge Z), I(Y \wedge Z)\}, B - \max\{I(X \wedge Z), I(Y \wedge Z)\}), \tag{3.39}$$

and

$$\left(I(Z \wedge X, Y), I(X \wedge Y) - I(Z \wedge X, Y)\right). \tag{3.40}$$

While the achievability of the first three (SK, PK)-rate pairs can be shown, it remains unclear whether (SK, PK)-rate pairs (3.39) and (3.40) are achievable.

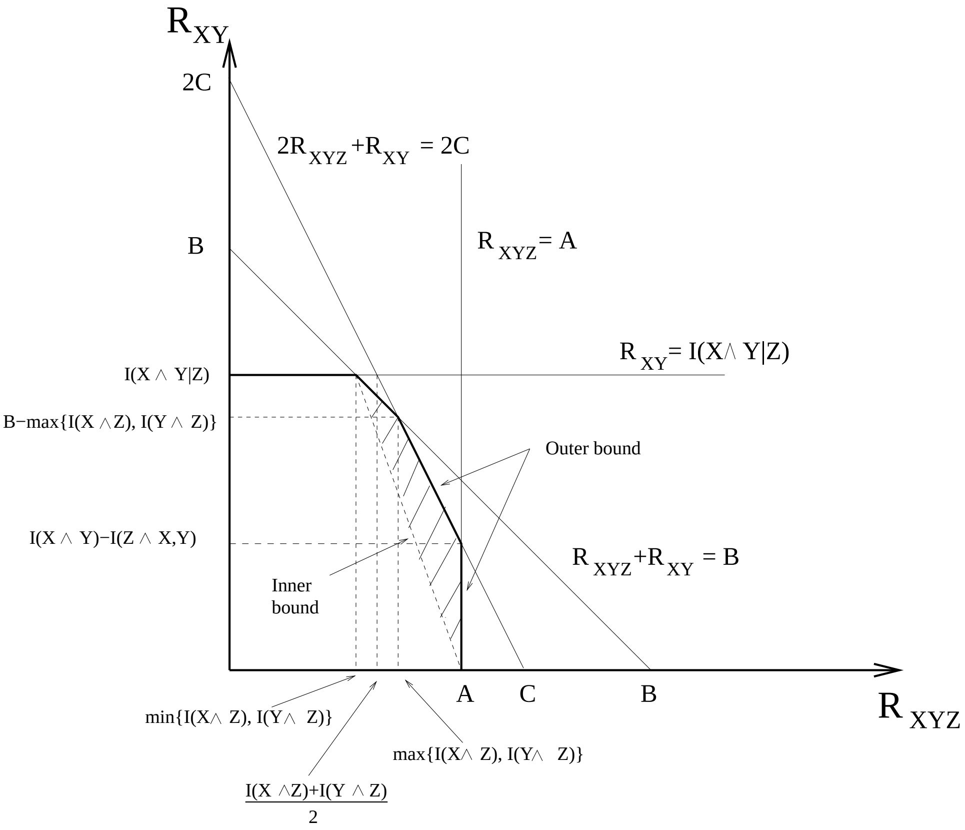

R_{XY}
2C
$2R_{XYZ}+R_{XY} = 2C$
B
$R_{XYZ} = A$
$R_{XY} = I(X \wedge Y|Z)$
$I(X \wedge Y|Z)$
$B-\max\{I(X \wedge Z), I(Y \wedge Z)\}$
Outer bound
$I(X \wedge Y)-I(Z \wedge X,Y)$
$R_{XYZ}+R_{XY} = B$
Inner bound
A
C
B
R_{XYZ}
$\min\{I(X \wedge Z), I(Y \wedge Z)\}$
$\max\{I(X \wedge Z), I(Y \wedge Z)\}$
$\frac{I(X \wedge Z)+I(Y \wedge Z)}{2}$

Figure 3.3: Inner and outer bounds for $\mathcal{C}_{SP}$ for Case 3.

Chapter 4

Secret Key and Private Key Constructions for Simple Multiterminal Source Models

4.1 Introduction

This part of the dissertation is motivated by recent results of Csiszár and Narayan [17], which highlight innate connections between secrecy generation by multiple terminals and multiterminal Slepian-Wolf near-lossless data compression (sans secrecy restrictions). We propose a new approach for *constructing* secret and private keys based on the long-known Slepian-Wolf code for sources connected by a virtual additive noise channel, due to Wyner [63]. Explicit procedures for such constructions, and their substantiation, are provided. In particular, we use low density parity check (LDPC) channel codes to construct a new class of secret keys.

Of particular relevance to the contents of this chapter are recent results in [17] for models with an arbitrary number of terminals, each of which observes a distinct component of a discrete memoryless multiple source (DMMS). Unrestricted public communication is allowed between these terminals. All the transmissions are observed by all the terminals and by the eavesdropper. Two models considered in [17] are directly relevant to our work, and these are first briefly described below.

(i) Suppose that $m \geq 2$ terminals $\mathcal{X}_1, \cdots, \mathcal{X}_m$[1] observe n independent and identically distributed (i.i.d.) repetitions of the random variables (rvs) $X_1, \cdots X_m$, denoted by $X_1^n, \cdots, X_m^n$, respectively. A SK generated by these terminals consists of "common ran-

[1] Since we shall consider the models with an arbitrary number of terminals hereafter, we shall use $\mathcal{X}_1, \cdots, \mathcal{X}_m$ in lieu of $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \cdots$ to denote the terminals.

domness," based on public communication which is concealed from an eavesdropper with access to this communication. The largest (entropy) rate of such a SK is termed the SK-capacity, denoted by C_S, and is shown in [17] to equal

$$C_S = H(X_1, \cdots, X_m) - R_{min}, \tag{4.1}$$

where

$$R_{min} = \min_{(R_1, \cdots, R_m) \in \mathcal{R}} \sum_{i=1}^{m} R_i,$$

with

$$\mathcal{R} = \left\{ (R_1, \cdots, R_m) : \sum_{i:\ \mathcal{X}_i \in \mathcal{B}} R_i \geq H(X_{\mathcal{B}} | X_{\mathcal{B}^c}), \mathcal{B} \subset \{\mathcal{X}_1, \cdots, \mathcal{X}_m\} \right\},$$

where $X_{\mathcal{B}} = \{X_i, \mathcal{X}_i \in \mathcal{B}\}$ and $\mathcal{B}^c = \{\mathcal{X}_1, \cdots, \mathcal{X}_m\} \backslash \mathcal{B}$.

(ii) For a given subset of the terminals $\mathcal{A} \subset \{\mathcal{X}_1, \cdots, \mathcal{X}_m\}$, a private key (PK) for the terminals in $\mathcal{A}$, private from the terminals in $\mathcal{A}^c$, is a SK generated by the terminals in $\mathcal{A}$ (with the possible help of the terminals in $\mathcal{A}^c$), which is concealed from an eavesdropper with access to the public communication and also from the "helper" terminals in $\mathcal{A}^c$ (and, hence, private). The largest (entropy) rate of such a PK is termed the PK-capacity, denoted by $C_P(\mathcal{A})$. It is shown in [17] that

$$C_P(\mathcal{A}) = H(X_{\mathcal{A}} | X_{\mathcal{A}^c}) - R_{min}(\mathcal{A}), \tag{4.2}$$

where

$$R_{min}(\mathcal{A}) = \min_{\{R_i,\ \mathcal{X}_i \in \mathcal{A}\} \in \mathcal{R}(\mathcal{A})} \sum_{i:\ \mathcal{X}_i \in \mathcal{A}} R_i,$$

with

$$\mathcal{R}(\mathcal{A}) = \left\{ \{R_i,\ \mathcal{X}_i \in \mathcal{A}\} : \sum_{i:\ \mathcal{X}_i \in \mathcal{B}} R_i \geq H(X_{\mathcal{B}} | X_{\mathcal{B}^c}), \mathcal{B} \subset \mathcal{A} \right\}.$$

The results above afford the following interpretation. The SK-capacity C_S, i.e., largest rate at which all the m terminals can generate a SK, is obtained by subtracting from the maximum rate of shared common randomness (CR) achievable by these terminals, viz. $H(X_1, \cdots, X_m)$, the smallest sum-rate R_{min} of the data-compressed interterminal communication which enables each of the terminals to acquire this maximal CR. A similar interpretation holds for the PK-capacity $C_P(\mathcal{A})$ as well, with the difference that the terminals in $\mathcal{A}^c$, which act as helpers but must not be privy to the secrecy generated, can simply "reveal" their observations. Hence, the entropy terms in (4.1) are now replaced in (4.2) with additional conditioning on $X_{\mathcal{A}^c}$. It should be noted that R_{min} and $R_{min}(\mathcal{A})$ are obtained as solutions to Slepian-Wolf (SW) multiterminal near-lossless data compression problems *not involving any secrecy constraints.* This characterization of the SK-capacity and PK-capacity in terms of the decompositions above also mirrors the consecutive stages in the random coding arguments used in establishing these results. For instance, and loosely speaking, to generate a SK, the m terminals first generate CR (without any secrecy restrictions), say a rv L of entropy rate $\frac{1}{n}H(L) > 0$, through SW-compressed interterminal communication $\mathbf{F}$. This means that all the m terminals acquire the rv L with probability $\cong 1$. The next step entails an extraction from L of a SK $K = g(L)$ of entropy rate $\frac{1}{n}H(L|\mathbf{F})$, by means of a suitable operation performed *identically* at each terminal on the acquired CR L. When the CR first acquired by the m terminals is maximal, i.e., $L = (X_1^n, \cdots, X_m^n)$ with probability $\cong 1$, then the corresponding SK $K = g(L)$ has the best rate C_S given by (4.1). A similar approach is used to generate a PK of rate given by (4.2). Recent independent work [45] for the special case of $m = 2$ terminals shows that the mentioned identical operation by the m terminals, to extract a SK from the previously acquired CR, can be accomplished by means of a linear transformation.

The discussion above suggests that techniques for multiterminal SW data compression could be used for the *constructions* of SKs and PKs. Next, in SW coding, the existence of linear data compression codes with rates arbitrarily close to the SW bound has been long known [12]. In particular, when the i.i.d. sequences observed at the terminals are related to each other through virtual communication channels characterized by independent additive noises, such linear data compression codes can be obtained in terms of the cosets of linear error-correction codes for these virtual channels, a fact first illustrated in [63] for the special case of $m = 2$ terminals connected by a virtual binary symmetric channel (BSC). This fact, exploited by most known linear constructions of SW codes (cf. e.g., [1], [10], [23], [24], [27], [29], [31]–[33], [44], [50], [56]), can enable us to translate such constructions and other significant recent developments in capacity-achieving linear codes into new constructions of SKs and PKs.

Motivated by these considerations, we seek to devise new *construction schemes* for secrecy generation. The main technical contribution of this work is the following: we consider four simple models of secrecy generation and show how a new class of SKs and PKs can be constructed, based on the SW data compression code from [63]. Additionally, we study the use of LDPC codes, a class of linear capacity-achieving channel codes, in the SW data compression step of the procedure to construct a new class of SKs with rates arbitrarily close to SK-capacity.

The rest of this chapter is organized as follows. Preliminaries are contained in Section 4.2. In Section 4.3, we consider four simple models for which we illustrate the constructions of appropriate SKs or PKs, which rely on suitable SW data compression codes. The SKs or PKs generated by these schemes are shown to satisfy the requisite secrecy conditions in Section 4.4. Implementations of these constructions using LDPC codes are illustrated in Section 4.5, and simulation results are also reported in Section 4.5.

4.2 Preliminaries

4.2.1 The Secret Key Capacity and the Private Key Capacity

Consider a DMMS with $m \geq 2$ components, and with corresponding generic rvs $X_1, \cdots, X_m$ taking values in finite alphabets $\mathcal{X}_1, \cdots, \mathcal{X}_m$, respectively. Let $X_i^n = (X_{i,1}, \cdots, X_{i,n})$ be n i.i.d. repetitions of rv X_i, $1 \leq i \leq m$. Terminals $\mathcal{X}_1, \cdots, \mathcal{X}_m$, with respective observations $X_1^n, \cdots, X_m^n$, represent the m users that wish to generate a SK by means of public communication. These terminals can communicate with each other through broadcasts over a noiseless public channel, possibly interactively in many rounds. In general, a transmission from a terminal is allowed to be any function of its observations, and of all previous transmissions. Let $\mathbf{F}$ denote collectively all the public transmissions.

Given $\varepsilon > 0$, the rv $K_{\mathcal{M}}$, with finite range $\mathcal{K}_{\mathcal{M}}$, represents an *$\varepsilon$-secret key* (*$\varepsilon$-SK*) for the terminals in $\mathcal{M} = \{\mathcal{X}_1, \cdots, \mathcal{X}_m\}$, achieved with communication $\mathbf{F}$, if $K_{\mathcal{M}}$ satisfies

- the common randomness condition: $K_{\mathcal{M}}$ is ε-recoverable from each of $(\mathbf{F}, X_i^n)$, $1 \leq i \leq m$;

- the secrecy condition:

$$\frac{1}{n} I(K_{\mathcal{M}} \wedge \mathbf{F}) \leq \varepsilon;$$

and

- the uniformity condition:

$$\frac{1}{n} H(K_{\mathcal{M}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{M}}| - \varepsilon.$$

Let $\mathcal{A} \subset \{\mathcal{X}_1, \cdots, \mathcal{X}_m\}$ be an arbitrary subset of the terminals. The rv $K_{\mathcal{A}}$, with finite range $\mathcal{K}_{\mathcal{P}}(\mathcal{A})$, represents an *$\varepsilon$-private key* (*$\varepsilon$-PK*) for the terminals in $\mathcal{A}$, private from the terminals in $\mathcal{A}^c = \mathcal{M} \backslash \mathcal{A}$, achieved with communication $\mathbf{F}$, if $K_{\mathcal{A}}$ satisfies

- the common randomness condition: $K_{\mathcal{A}}$ is ε-recoverable from each of $(\mathbf{F}, X_i^n)$, for

$\mathcal{X}_i \in \mathcal{A}$;

- the secrecy condition:

$$\frac{1}{n} I\left(K_{\mathcal{A}} \wedge \mathbf{F}, X^n_{\mathcal{A}^c}\right) \leq \varepsilon;$$

and

- the uniformity condition:

$$\frac{1}{n} H(K_{\mathcal{A}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{P}}(\mathcal{A})| - \varepsilon.$$

Definition 4.1 [17]*: A nonnegative number R is called an achievable SK rate if ε_n-SKs $K^{(n)}_{\mathcal{M}}$ are achievable with suitable communication (with the number of rounds possibly depending on n), such that $\varepsilon_n \to 0$ and $\frac{1}{n} H\left(K^{(n)}_{\mathcal{M}}\right) \to R$. The largest achievable SK rate is called the SK-capacity, denoted by C_S. The PK-capacity for the terminals in $\mathcal{A}$, denoted by $C_P(\mathcal{A})$, is similarly defined. An achievable SK rate (resp. PK rate) will be called strongly achievable if ε_n above can be taken to vanish exponentially in n. The corresponding capacities are termed strong capacities.*

Single-letter characterizations have been obtained for C_S in the case of $m = 2$ terminals in [3], [36] and for $m \geq 2$ terminals in [17], given by (4.1); and for $C_P(\mathcal{A})$ in the case of $m = 3$ terminals in [3] and for $m \geq 3$ terminals in [17], given by (4.2). The proofs of the achievability parts exploit the close connection between secrecy generation and SW data compression. Loosely speaking, CR sans any secrecy restrictions, is first generated through SW-compressed interterminal communication, whereby all the m terminals acquire a (common) rv with probability $\cong 1$. In the next step, secrecy is then extracted by means of a suitable *identical* operation performed at each terminal on the acquired CR. When the CR initially acquired by the m terminals is maximal, the corresponding SK has the best rate C_S given by (4.1).

In this chapter, we consider four simple models for which we illustrate the constructions of appropriate *strong* SKs or PKs.

4.2.2 Linear Codes for the Binary Symmetric Channel

The SW codes of interest will rely on the following result concerning the existence of "good" linear channel codes for a binary symmetric channel (BSC).

Hereafter, a BSC with crossover probability p, $0 < p < \frac{1}{2}$, will be denoted by BSC(p). Let $h_b(.)$ denote the binary entropy function.

Lemma 4.1 [20] *For every $\varepsilon > 0$, $0 < p < \frac{1}{2}$, and for all n sufficiently large, there exists a binary linear $(n, n-u)$ code for a BSC(p), with $u < n[h_b(p) + \varepsilon]$, such that the average error probability of maximum likelihood decoding is less than $2^{-n\eta}$, for some $\eta > 0$.* ■

4.3 Statement of Results

We now describe our main results on secrecy generation for four specific models.

Model 4.1: Let the terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ observe, respectively, n i.i.d. repetitions of the correlated rvs X_1 and X_2, where X_1, X_2 are binary rvs with joint probability mass function (pmf)

$$P_{X_1X_2}(0,0) = P_{X_1X_2}(1,1) = \frac{1-p}{2}, \quad P_{X_1X_2}(0,1) = P_{X_1X_2}(1,0) = \frac{p}{2}, \tag{4.3}$$

with $0 < p < \frac{1}{2}$. These terminals wish to generate a strong SK of maximal rate.

The SK-capacity for this model is [3], [17], [36]

$$C_S = I(X_1 \wedge X_2) = 1 - h_b(p) \ bit/symbol.$$

We show a simple scheme for the terminals to generate a SK with rate close to $1 - h_b(p)$ bit/symbol, which relies on Wyner's well-known method for SW data compression [63].

The SW problem of interest entails terminal $\mathcal{X}_2$ reconstructing the observed sequence x_1^n at terminal $\mathcal{X}_1$ from the SW codeword for x_1^n and its own observed sequence x_2^n.

Observe that under the given joint pmf (4.3), X_2^n can be considered as an input to a virtual BSC(p), while X_1^n is the corresponding output, i.e., we can write

$$X_1^n = X_2^n \oplus V^n, \tag{4.4}$$

where $V^n = (V_1, \cdots, V_n)$ is an i.i.d. sequence of $\{0,1\}$-valued rvs, independent of X_2^n, with $\Pr\{V_i = 1\} = p$, $1 \leq i \leq n$.

(i) SW data compression [63]:

Let $\mathcal{C}$ be a linear $(n, n-u)$ code as in Lemma 4.1 with parity check matrix $\mathbf{P}$. Both terminals know $\mathcal{C}$ (and $\mathbf{P}$).

Terminal $\mathcal{X}_1$ transmits the syndrome $\mathbf{P}x_1^n$ [2] to terminal $\mathcal{X}_2$. The maximum likelihood estimate of x_1^n at terminal $\mathcal{X}_2$ is:

$$\hat{x}_2^n(1) = x_2^n \oplus f_{\mathbf{P}}(\mathbf{P}x_1^n \oplus \mathbf{P}x_2^n),$$

where $f_{\mathbf{P}}(\mathbf{P}x_1^n \oplus \mathbf{P}x_2^n)$ is the most likely sequence v^n (under the pmf of V^n as above) with syndrome $\mathbf{P}v^n = \mathbf{P}x_1^n \oplus \mathbf{P}x_2^n$, with $\oplus$ denoting addition modulo 2. Note that in a standard array corresponding to the code $\mathcal{C}$ above, $f_{\mathbf{P}}(\mathbf{P}x_1^n \oplus \mathbf{P}x_2^n)$ is simply the coset leader of the coset with syndrome $\mathbf{P}x_1^n \oplus \mathbf{P}x_2^n$. Also, x_1^n and $\hat{x}_2(1)$ lie in the same coset.

The probability of decoding error at terminal $\mathcal{X}_2$ is given by

$$\Pr\{\hat{X}_2^n(1) \neq X_1^n\} = \Pr\{X_2^n \oplus f_{\mathbf{P}}(\mathbf{P}X_1^n \oplus \mathbf{P}X_2^n) \neq X_1^n\}.$$

It readily follows from (4.4) that

$$\Pr\{\hat{X}_2^n(1) \neq X_1^n\} = \Pr\{f_{\mathbf{P}}(\mathbf{P}V^n) \neq V^n\}.$$

[2] In the interests of avoiding repeated superscript, we shall hereafter use $\mathbf{P}x_1^n$ in lieu of the correct $\mathbf{P}(x_1^n)^t$, which should not cause any confusion.

By Lemma 4.1, $\Pr\{f_{\mathbf{P}}(\mathbf{P}V^n) \neq V^n\} < 2^{-n\eta}$ for some $\eta > 0$ and for all n sufficiently large, so that

$$\Pr\{\hat{X}_2^n(1) = X_1^n\} \geq 1 - 2^{-n\eta}.$$

(ii) SK construction:

Consider a (common) standard array for $\mathcal{C}$ known to both terminals. Denote by $a_{i,j}^n$ the element of the i^{th} row and the j^{th} column in the standard array, $1 \leq i \leq 2^u$, $1 \leq j \leq 2^{n-u}$.

Terminal $\mathcal{X}_1$ sets $K_1 = j_1$ if X_1^n equals a_{i,j_1}^n in its coset i in the standard array. Terminal $\mathcal{X}_2$ sets $K_2 = j_2$ if $\hat{X}_2^n(1)$ equals a_{i,j_2}^n in the coset i of same standard array.

(iii) SK criteria:

The following theorem shows that K_1 constitutes a strongly achievable SK with rate approaching the SK-capacity.

Theorem 4.1 *For some $\eta > 0$ and for all n sufficiently large, the pair of rvs (K_1, K_2) generated above, with (common) range $\mathcal{K}_1$ (say), satisfy*

$$\Pr\{K_1 = K_2\} \geq 1 - 2^{-n\eta}; \tag{4.5}$$

$$I(K_1 \wedge \mathbf{F}) = 0; \tag{4.6}$$

$$H(K_1) = \log |\mathcal{K}_1|. \tag{4.7}$$

Furthermore,

$$\frac{1}{n} H(K_1) > 1 - h_b(p) - \varepsilon. \tag{4.8}$$

Remark: The probability of K_1 being different from K_2 equals exactly the average error probability of maximum likelihood decoding when $\mathcal{C}$ is used on a BSC(p). Furthermore, the gap between the rate of the generated SK and the SK-capacity is as wide as the gap between the rate of $\mathcal{C}$ and the channel capacity. Therefore, if a "better" channel code for a BSC(p), in the sense that the rate of this code is closer to the channel capacity and the average error probability of maximum likelihood decoding is smaller, is applied, then a "better" SK can be generated at both terminals, in the sense that the rate of this SK is closer to the SK-capacity and the probability is smaller that the keys generated at different terminals do not agree with each other.

Model 4.2: Let the terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ observe, respectively, n i.i.d. repetitions of the correlated rvs X_1 and X_2, where X_1, X_2 are binary rvs with joint pmf

$$\begin{aligned} P_{X_1X_2}(0,0) &= (1-p)(1-q), \quad P_{X_1X_2}(0,1) = pq, \\ P_{X_1X_2}(1,0) &= p(1-q), \quad P_{X_1X_2}(1,1) = q(1-p), \end{aligned} \tag{4.9}$$

with $0 < p < \frac{1}{2}$ and $0 < q < 1$. These terminals wish to generate a strong SK of maximal rate.

Note that Model 4.1 is a special case of Model 4.2 for $q = \frac{1}{2}$. We show below a scheme for the terminals to generate a SK with rate close to the SK-capacity for this model [3], [17],[36], which is

$$C_S = I(X_1 \wedge X_2) = h_b(p + q - 2pq) - h_b(p) \ \mathit{bit/symbol}.$$

(i) SW data compression:

This step is identical to step *(i)* for Model 4.1. Note that under the given joint pmf (4.9), X_1^n and X_2^n can be written as in (4.4). It follows in the same manner as for Model 4.1 that for some $\eta > 0$ and for all sufficiently large n,

$$\Pr\{\hat{X}_2^n(1) = X_1^n\} \geq 1 - 2^{-n\eta}.$$

(ii) SK construction:

Both terminals know the linear $(n, n-u)$ code $\mathcal{C}$ specified in Lemma 4.1, and a (common) standard array for $\mathcal{C}$. Let $\{e_i^n : 1 \leq i \leq 2^u\}$ denote the set of coset leaders for all the cosets of $\mathcal{C}$.

Denote by A_i the set of $T^n_{X_1,\xi}$ sequences in the coset of $\mathcal{C}$ with coset leader e_i^n, $1 \leq i \leq 2^u$. If the number of sequences of the same type in A_i is more than $2^{n[I(X_1 \wedge X_2)-\varepsilon']}$, where $\varepsilon' > \xi + \varepsilon$ with ε being the parameter satisfying $u < n[h_b(p)+\varepsilon]$ in Lemma 4.1, then collect arbitrarily $2^{n[I(X_1 \wedge X_2)-\varepsilon']}$ such sequences to compose a subset, which we call a *regular subset* (as it consists of sequences of the same type). Continue this procedure until the number of sequences of every type in A_i is less than $2^{n[I(X_1 \wedge X_2)-\varepsilon']}$. Let N_i denote the number of distinct regular subsets of A_i.

Enumerate (in any way) the sequences in each regular subset. Let $b^n_{i,j,k}$, where $1 \leq i \leq 2^u$, $1 \leq j \leq N_i$, $1 \leq k \leq 2^{n[I(X_1 \wedge X_2)-\varepsilon']}$, denote the k^{th} sequence of the j^{th} regular subset in the i^{th} coset (i.e., the coset with coset leader e_i^n).

Terminal $\mathcal{X}_1$ sets $K_1 = k_1$ if X_1^n equals b^n_{i,j_1,k_1}. Otherwise, K_1 is set to be uniformly distributed on $\left\{1, \cdots, 2^{n[I(X_1 \wedge X_2)-\varepsilon']}\right\}$, independent of (X_1^n, X_2^n). Terminal $\mathcal{X}_2$ sets $K_2 = k_2$ if $\hat{X}_2^n(1)$ equals b^n_{i,j_2,k_2}. Otherwise, K_2 is set to be uniformly distributed on $\left\{1, \cdots, 2^{n[I(X_1 \wedge X_2)-\varepsilon']}\right\}$, independent of (X_1^n, X_2^n, K_1).

(iii) SK criteria:

The following theorem shows that K_1 constitutes a strongly achievable SK with rate approaching the SK-capacity.

Theorem 4.2 *For some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all n sufficiently large, the pair of rvs (K_1, K_2) generated above, with range $\mathcal{K}_1$ (say), satisfy*

$$\Pr\{K_1 = K_2\} \geq 1 - 2^{-n\eta'}; \tag{4.10}$$

$$I(K_1 \wedge \mathbf{F}) = 0; \tag{4.11}$$

$$H(K_1) = \log |\mathcal{K}_1|. \tag{4.12}$$

Furthermore,

$$\frac{1}{n} H(K_1) = I(X_1 \wedge X_2) - \varepsilon'. \tag{4.13}$$

The next model is an instance of a *Markov chain on a tree* (cf. [25], [17]), which considers a tree $\mathcal{T}$ with vertex set $V(\mathcal{T}) = \{1, \cdots, m\}$ and edge set $E(\mathcal{T})$. For $(i,j) \in E(\mathcal{T})$, let $B(i \leftarrow j)$ denote the set of all vertices connected with j by a path containing the edge (i,j). The rvs $X_1, \cdots, X_m$ form a *Markov chain on the tree* $\mathcal{T}$ if for each $(i,j) \in E(\mathcal{T})$, the conditional pmf of X_j given $\{X_l, l \in B(i \leftarrow j)\}$ depends only on X_i (i.e., is conditionally independent of $\{X_l, l \in B(i \leftarrow j)\} \backslash \{X_i\}$, conditioned on X_i. Note that when $\mathcal{T}$ is a chain, this concept reduces to that of a standard Markov chain.

Model 4.3: Let the terminals $\mathcal{X}_1, \cdots, \mathcal{X}_m$ observe, respectively, n i.i.d. repetitions of $\{0,1\}$-valued rvs $X_1, \cdots, X_m$ which form a Markov chain on the tree $\mathcal{T}$, and have a joint pmf $P_{X_1 \cdots X_m}$ described in the following manner: for $(i,j) \in E(\mathcal{T})$,

$$P_{X_i X_j}(x_i, x_j) = \frac{1}{2}(1 - p_{(i,j)})\delta_{x_i x_j} + \frac{1}{2} p_{(i,j)} \ (1 - \delta_{x_i x_j}), \quad 0 < p_{(i,j)} < \frac{1}{2},$$

for $x_i \in \{0,1\}$, $x_j \in \{0,1\}$. These m terminals wish to generate a strong SK of maximal rate.

Note that Model 4.1 is a special case of Model 4.3 for $m = 2$. Without any loss of generality, let

$$p_{max} = p_{(i^*,j^*)} = \max_{(i,j) \in E(\mathcal{T})} p_{(i,j)}.$$

Then, the SK-capacity for this model is [17]

$$C_{SK} = I(X_{i^*} \wedge X_{j^*}) = 1 - h_b(p_{max}) \ bit/symbol. \tag{4.14}$$

We show below how to extract a SK with rate close to $1-h_b(p_{max})$ by using an extension of the SW data compression scheme of Model 4.1 for reconstructing $x_{i^*}^n$ at all the terminals.

(i) SW data compression:

Let $\mathcal{C}$ be a linear $(n, n-u)$ code as in Lemma 4.1 for a BSC(p_{max}), with parity check matrix $\mathbf{P}$. Each terminal $\mathcal{X}_i$ transmits the syndrome $\mathbf{P}x_i^n$, $1 \leq i \leq m$.

Let $\hat{x}_i^n(j)$ denote the maximum likelihood estimate at terminal $\mathcal{X}_i$ of x_j^n, $1 \leq i \neq j \leq m$. For a terminal $\mathcal{X}_i$, $i \neq i^*$, denote by $(i_0, i_1, \cdots, i_r)$ the (only) path in the tree $\mathcal{T}$ from i to i^*, where $i_0 = i$ and $i_r = i^*$; this terminal $\mathcal{X}_i$, with the knowledge of (x_i^n, $\mathbf{P}x_{i_1}^n, \cdots, \mathbf{P}x_{i_{r-1}}^n, \mathbf{P}x_{i^*}^n$), forms its estimate $\hat{x}_i^n(i^*)$ of $x_{i^*}^n$ through the following successive maximum likelihood estimates of $x_{i_1}^n, \cdots, x_{i_{r-1}}^n$:

$$\begin{array}{rcl}
\hat{x}_i^n(i_1) & = & x_i^n \oplus f_{\mathbf{P}}(\mathbf{P}x_i^n \oplus \mathbf{P}x_{i_1}^n), \\
\hat{x}_i^n(i_2) & = & \hat{x}_i^n(i_1) \oplus f_{\mathbf{P}}(\mathbf{P}x_{i_1}^n \oplus \mathbf{P}x_{i_2}^n), \\
\vdots & \vdots & \vdots \\
\hat{x}_i^n(i_{r-1}) & = & \hat{x}_i^n(i_{r-2}) \oplus f_{\mathbf{P}}(\mathbf{P}x_{i_{r-2}}^n \oplus \mathbf{P}x_{i_{r-1}}^n)
\end{array}$$

and finally,

$$\hat{x}_i^n(i^*) = \hat{x}_i^n(i_{r-1}) \oplus f_{\mathbf{P}}(\mathbf{P}x_{i_{r-1}}^n \oplus \mathbf{P}x_{i^*}^n).$$

Proposition 4.1 *By the successive maximum likelihood estimates above, the estimate $\hat{X}_i^n(i^*)$ at terminal $\mathcal{X}_i$, $i \neq i^*$, satisfies*

$$\Pr\{\hat{X}_i^n(i^*) = X_{i^*}^n\} \geq 1 - m \cdot 2^{-n\eta}, \tag{4.15}$$

for some $\eta > 0$ and for all n sufficiently large.

Proof of Proposition 4.1: See Appendix B. ■

It follows directly from (4.15) that for some $\eta' = \eta'(\eta, m) > 0$ and for all n sufficiently large,

$$\Pr\{\hat{X}_i^n(i^*) = X_{i^*}^n, 1 \leq i \neq i^* \leq m\} \geq 1 - 2^{-n\eta'}.$$

(ii) SK construction:

Consider a (common) standard array for $\mathcal{C}$ known to all the terminals. Denote by $a_{l,k}^n$ the element of the l^{th} row and the k^{th} column in the standard array, $1 \leq l \leq 2^u$, $1 \leq k \leq 2^{n-u}$.

Terminal $\mathcal{X}_{i^*}$ sets $K_{i^*} = k_{i^*}$ if $X_{i^*}^n$ equals $a_{l,k_{i^*}}^n$ in the standard array. Terminals $\mathcal{X}_i$, $1 \leq i \neq i^* \leq m$, set $K_i = k_i$ if $\hat{X}_i^n(i^*)$ equals a_{l,k_i}^n in the same standard array.

(iii) SK criteria:

The following theorem shows that K_{i^*} constitutes a strongly achievable SK with rate approaching the SK-capacity.

Theorem 4.3 *For some $\eta' = \eta'(\eta, m) > 0$ and for all sufficiently large n, the set of rvs $(K_1, \cdots, K_m)$ generated above, with range $\mathcal{K}_{i^*}$ (say), satisfy*

$$\Pr\{K_1 = \cdots = K_m\} \geq 1 - 2^{-n\eta'}; \tag{4.16}$$

$$I(K_{i^*} \wedge \mathbf{F}) = 0; \tag{4.17}$$

$$H(K_{i^*}) = \log |\mathcal{K}_{i^*}|. \tag{4.18}$$

Furthermore,

$$\frac{1}{n} H(K_{i^*}) > 1 - h_b(p_{max}) - \varepsilon. \tag{4.19}$$

Model 4.4: Let the terminals $\mathcal{X}_1$, $\mathcal{X}_2$ and $\mathcal{X}_3$ observe, respectively, n i.i.d. repetitions of the $\{0,1\}$-valued correlated rvs X_1, X_2, X_3, with joint pmf $P_{X_1X_2X_3}$ given by:

$$\begin{aligned}
P_{X_1X_2X_3}(0,0,0) = P_{X_1X_2X_3}(0,1,1) &= \frac{(1-p)(1-q)}{2},\\
P_{X_1X_2X_3}(0,0,1) = P_{X_1X_2X_3}(0,1,0) &= \frac{pq}{2},\\
P_{X_1X_2X_3}(1,0,0) = P_{X_1X_2X_3}(1,1,1) &= \frac{p(1-q)}{2},\\
P_{X_1X_2X_3}(1,0,1) = P_{X_1X_2X_3}(1,1,0) &= \frac{q(1-p)}{2},
\end{aligned} \tag{4.20}$$

with $0 < p < \frac{1}{2}$ and $0 < q < 1$. Terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ wish to generate a strong PK of maximal rate, which is concealed from the helper terminal $\mathcal{X}_3$.

Note that under the joint pmf of X_1, X_2, X_3 above, we can write

$$X_1^n = X_2^n \oplus X_3^n \oplus V^n, \tag{4.21}$$

where $V^n = (V_1, \cdots, V_n)$ is an i.i.d. sequence of $\{0,1\}$-valued rvs, independent of (X_2^n, X_3^n), with $\Pr\{V_i = 1\} = p$, $1 \leq i \leq n$.

We show below a scheme for terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ to generate a PK with rate close to the PK-capacity for this model [3], [16], [17]

$$C_P(\{\mathcal{X}_1, \mathcal{X}_2\}) = I(X_1 \wedge X_2 | X_3) = h_b(p + q - 2pq) - h_b(p) \; bit/symbol.$$

The first step of this scheme entails terminal $\mathcal{X}_3$ simply revealing its observations x_3^n to both terminals $\mathcal{X}_1$ and $\mathcal{X}_2$. Then, Wyner's SW data compression scheme is used for reconstructing x_1^n at terminal $\mathcal{X}_2$ from the SW codeword for x_1^n and its own knowledge of $x_2^n \oplus x_3^n$.

(i) SW data compression:

This step is identical to step *(i)* for Model 4.1, as seen with the help of (4.21). Obviously,

$$\Pr\{\hat{X}_2^n(1) = X_1^n\} \geq 1 - 2^{-n\eta},$$

for some $\eta > 0$ and for all sufficiently large n.

(ii) SK construction:

Suppose that terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ know a linear $(n, n-u)$ code $\mathcal{C}$ as in Lemma 4.1, and a (common) standard array for $\mathcal{C}$. Let $\{e_i^n : 1 \leq i \leq 2^u\}$ denote the set of coset leaders for all the cosets of $\mathcal{C}$.

For a sequence $x_3^n \in \{0,1\}^n$, denote by $A_i(x_3^n)$ the set of $T^n_{X_1|X_3,\xi}(x_3^n)$ sequences in the coset of $\mathcal{C}$ with coset leader e_i^n, $1 \leq i \leq 2^u$. If the number of sequences of the same joint type with x_3^n in $A_i(x_3^n)$ is more than $2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$, where $\varepsilon' > 2\xi + \varepsilon$ and ε satisfies $u < n[h_b(p) + \varepsilon]$ (as in Lemma 4.1), then collect arbitrarily $2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$ such sequences to compose a regular subset. Continue this procedure until the number of sequences of every joint type with x_3^n in $A_i(x_3^n)$ is less than $2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$. Let $N_i(x_3^n)$ denote the number of distinct regular subsets of $A_i(x_3^n)$.

For a given sequence x_3^n, enumerate (in any way) the sequences in each regular subset. Let $b^n_{i,j,k}(x_3^n)$, where $1 \leq i \leq 2^u$, $1 \leq j \leq N_i(x_3^n)$, $1 \leq k \leq 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}$, denote the k^{th} sequence of the j^{th} regular subset in the i^{th} coset.

Terminal $\mathcal{X}_1$ sets $K_1 = k_1$ if X_1^n equals $b^n_{i,j_1,k_1}(x_3^n)$. Otherwise, K_1 is set to be uniformly distributed on $\left\{1, \cdots, 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\right\}$, independent of (X_1^n, X_2^n, X_3^n). Terminal $\mathcal{X}_2$ sets $K_2 = k_2$ if $\hat{X}_2^n(1)$ equals $b^n_{i,j_2,k_2}(x_3^n)$. Otherwise, K_2 is set to be uniformly distributed on $\left\{1, \cdots, 2^{n[I(X_1 \wedge X_2|X_3)-\varepsilon']}\right\}$, independent of $(X_1^n, X_2^n, X_3^n, K_1)$.

(iii) SK criteria:

The following theorem shows that K_1 constitutes a strongly achievable PK with rate approaching the PK-capacity.

Theorem 4.4 *For some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all sufficiently large n, the pair of* *rvs* (K_1, K_2) *generated above, with range* $\mathcal{K}_1$ *(say), satisfy*

$$\Pr\{K_1 = K_2\} \geq 1 - 2^{-n\eta'}; \tag{4.22}$$

$$I(K_1 \wedge X_3^n, \mathbf{F}) = 0; \tag{4.23}$$

$$H(K_1) = \log |\mathcal{K}_1|. \tag{4.24}$$

Furthermore,

$$\frac{1}{n} H(K_1) = I(X_1 \wedge X_2 | X_3) - \varepsilon'. \tag{4.25}$$

Remark: The PK construction scheme above applies for any joint pmf of X_1, X_2, X_3, satisfying (4.21), and is not restricted to the given joint pmf of X_1, X_2, X_3 in (4.20).

4.4 Proofs

Proof of Theorem 4.1: It follows from the SK construction scheme that

$$\Pr\{K_1 \neq K_2\} = \Pr\{\hat{X}_2^n(1) \neq X_1^n\} < 2^{-n\eta},$$

which is (4.5). Since the rv X_1 is uniformly distributed on $\{0, 1\}$, for $1 \leq i \leq 2^u$, $1 \leq j \leq 2^{n-u}$,

$$\Pr\{X_1^n = a_{i,j}^n\} = 2^{-n}.$$

Hence,

$$\Pr\{K_1 = j\} = \sum_{i=1}^{2^u} \Pr\{X_1^n = a_{i,j}^n\} = 2^{-(n-u)}, \quad 1 \leq j \leq 2^{n-u},$$

i.e., K_1 is uniformly distributed on $\{1, \cdots, 2^{n-u}\}$, and so

$$H(K_1) = \log 2^{n-u} = n - u = \log |\mathcal{K}_1|,$$

which is (4.7). Therefore, (4.8) holds since $u < n[h_b(p) + \varepsilon]$.

It remains to show that K_1 satisfies the secrecy condition (4.6), with $\mathbf{F} = \mathbf{P}X_1^n$. Let $\{e_i^n, 1 \leq i \leq 2^u\}$ be the set of coset leaders for all the cosets of $\mathcal{C}$. For $1 \leq i \leq 2^u$, $1 \leq j \leq 2^{n-u}$,

$$\begin{aligned} \Pr\{K_1 = j | \mathbf{P}X_1^n = \mathbf{P}e_i^n\} &= \frac{\Pr\{K_1 = j, \mathbf{P}X_1^n = \mathbf{P}e_i^n\}}{\Pr\{\mathbf{P}X_1^n = \mathbf{P}e_i^n\}} \\ &= \frac{\Pr\{X_1^n = a_{i,j}^n\}}{\sum_{j'=1}^{2^{n-u}} \Pr\{X_1^n = a_{i,j'}^n\}} \\ &= 2^{-(n-u)} \\ &= \Pr\{K_1 = j\}. \end{aligned}$$

Therefore, K_1 is independent of $\mathbf{F}$, and $I(K_1 \wedge \mathbf{F}) = 0$, establishing (4.6). ■

Proof of Theorem 4.2: Let $\mathcal{F}$ denote the union of all regular subsets in $\bigcup_{i=1}^{2^u} A_i$. Clearly, $\mathcal{F} \subseteq T_{X_1,\xi}^n$, so that

$$\Pr\{X_1^n \in \mathcal{F}\} = \Pr\{X_1^n \in T_{X_1,\xi}^n, X_1^n \in \mathcal{F}\} = \Pr\{X_1^n \in T_{X_1,\xi}^n\} - \Pr\{X_1^n \in T_{X_1,\xi}^n \backslash \mathcal{F}\}. \quad (4.26)$$

By Proposition A.1, $\Pr\{X_1^n \in T_{X_1,\xi}^n\}$ goes to 1 exponentially rapidly in n. We show below that $\Pr\{X_1^n \in T_{X_1,\xi}^n \backslash \mathcal{F}\}$ goes to 0 exponentially rapidly in n.

Recall from Appendix A.1 that the number of different types of sequences in $\{0,1\}^n$ does not exceed $(n+1)^2$. Thus,

$$\begin{aligned} \left| \{x_1^n : x_1^n \in T_{X_1,\xi}^n \backslash \mathcal{F}\} \right| &\leq 2^u \cdot (n+1)^2 \cdot 2^{n[I(X_1 \wedge X_2) - \varepsilon']} \\ &< (n+1)^2 \cdot 2^{n[H(X_1) + \varepsilon - \varepsilon']}, \end{aligned}$$

where the previous inequality is from $u < n[h_b(p) + \varepsilon] = n[H(X_1|X_2) + \varepsilon]$.

Since $P_{X_1}^n(x_1^n) \leq 2^{-n[H(X_1) - \xi]}$, $x_1^n \in T_{X_1,\xi}^n$, we get

$$\Pr\{X_1^n \in T_{X_1,\xi}^n \backslash \mathcal{F}\} < (n+1)^2 \cdot 2^{-n(\varepsilon' - \xi - \varepsilon)}.$$

Choosing $\varepsilon' > \xi + \varepsilon$, $\Pr\{X_1^n \in T_{X_1,\xi}^n \backslash \mathcal{F}\}$ goes to 0 exponentially rapidly. Therefore, it follows from (4.26) that $\Pr\{X_1^n \in \mathcal{F}\}$ goes to 1 exponentially rapidly in n, with exponent depending on $(\xi, \varepsilon, \varepsilon')$.

By the SK construction scheme,

$$\begin{aligned}
\Pr\{K_1 \neq K_2\} &= \Pr\{K_1 \neq K_2, X_1^n \in \mathcal{F}\} + \Pr\{K_1 \neq K_2, X_1^n \notin \mathcal{F}\} \\
&\leq \Pr\{\hat{X}_2^n(1) \neq X_1^n, X_1^n \in \mathcal{F}\} + \Pr\{X_1^n \notin \mathcal{F}\} \\
&\leq \Pr\{\hat{X}_2^n(1) \neq X_1^n\} + \Pr\{X_1^n \notin \mathcal{F}\}.
\end{aligned}$$

Since $\Pr\{\hat{X}_2^n(1) \neq X_1^n\} < 2^{-n\eta}$, by the observation in the previous paragraph, we have

$$\Pr\{K_1 \neq K_2\} < 2^{-n\eta'},$$

for some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all sufficiently large n, which is (4.10).

Next, we shall show that K_1 satisfies the uniformity condition (4.12). For $1 \leq k \leq 2^{n[I(X_1 \wedge X_2) - \varepsilon']}$, it is clear by choice that

$$\Pr\{K_1 = k | X_1^n \notin \mathcal{F}\} = 2^{-n[I(X_1 \wedge X_2) - \varepsilon']}, \tag{4.27}$$

and that

$$\begin{aligned}
\Pr\{K_1 = k | X_1^n \in \mathcal{F}\} &= \frac{\Pr\{K_1 = k, X_1^n \in \mathcal{F}\}}{\Pr\{X_1^n \in \mathcal{F}\}} \\
&= \frac{\sum_{i=1}^{2^u} \sum_{j=1}^{N_i} \Pr\{X_1^n = b_{i,j,k}^n\}}{\sum_{i=1}^{2^u} \sum_{j=1}^{N_i} 2^{n[I(X_1 \wedge X_2) - \varepsilon']} \Pr\{X_1^n = b_{i,j,k}^n\}} \qquad (4.28) \\
&= 2^{-n[I(X_1 \wedge X_2) - \varepsilon']}, \qquad (4.29)
\end{aligned}$$

where (4.28) is due to every regular subset consisting of sequences of the same type. From (4.27) and (4.29),

$$\Pr\{K_1 = k\} = 2^{-n[I(X_1 \wedge X_2) - \varepsilon']}, \tag{4.30}$$

i.e., K_1 is uniformly distributed on $\left\{1, \cdots, 2^{n[I(X_1 \wedge X_2) - \varepsilon']}\right\}$, with

$$\frac{1}{n} H(K_1) = I(X_1 \wedge X_2) - \varepsilon',$$

which is (4.13).

It remains to show that K_1 satisfies the secrecy condition (4.11), with $\mathbf{F} = \mathbf{P}X_1^n$. For $1 \leq i \leq 2^u$ and $1 \leq k \leq 2^{n[I(X_1 \wedge X_2) - \varepsilon']}$, we have

$$\Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \notin \mathcal{F}\} = 2^{-n[I(X_1 \wedge X_2) - \varepsilon']},$$

by choice, and

$$\begin{aligned} \Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \in \mathcal{F}\} &= \frac{\Pr\{K_1 = k, \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \in \mathcal{F}\}}{\Pr\{\mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \in \mathcal{F}\}} \\ &= \frac{\sum_{j=1}^{N_i} \Pr\{X_1^n = b_{i,j,k}^n\}}{\sum_{j=1}^{N_i} 2^{n[I(X_1 \wedge X_2) - \varepsilon']} \Pr\{X_1^n = b_{i,j,k}^n\}} \\ &= 2^{-n[I(X_1 \wedge X_2) - \varepsilon']}. \end{aligned}$$

Hence,

$$\begin{aligned} \Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n\} &= \Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \in \mathcal{F}\} \cdot \Pr\{X_1^n \in \mathcal{F} | \mathbf{P}X_1^n = \mathbf{P}e_i^n\} \\ &\quad + \Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \notin \mathcal{F}\} \cdot \Pr\{X_1^n \notin \mathcal{F} | \mathbf{P}X_1^n = \mathbf{P}e_i^n\} \\ &= 2^{-n[I(X_1 \wedge X_2) - \varepsilon']} \\ &= \Pr\{K_1 = k\}, \end{aligned}$$

where the previous equality follows from (4.30). In other words, K_1 is independent of $\mathbf{F}$, establishing (4.11). ■

Proof of Theorem 4.3: Applying the same arguments used in Theorem 4.1, we can show that the set of rvs $(K_1, \cdots, K_m)$ satisfy (4.16), (4.18) and (4.19). It then remains to show that K_{i^*} satisfies the secrecy condition (4.17), with $\mathbf{F} = (\mathbf{P}X_1^n, \cdots, \mathbf{P}X_m^n)$.

Under the given joint pmf $P_{X_1 \cdots X_m}$, for each $i \neq i^*$, we can write

$$X_i^n = X_{i^*}^n \oplus V_i^n,$$

where $V_i^n = (V_{i,1}, \cdots, V_{i,n})$ is an i.i.d. sequence of $\{0,1\}$-valued rvs. Further, V_i^n, $1 \leq i \neq$

$i^* \leq m$, and $X_{i^*}^n$ are mutually independent. Then,

$$\begin{aligned} I(K_{i^*} \wedge \mathbf{F}) &= I(K_{i^*} \wedge \{\mathbf{P}X_i^n,\ 1 \leq i \leq m\}) \\ &\leq I(K_{i^*} \wedge \mathbf{P}X_{i^*}^n, \{\mathbf{P}V_i^n,\ 1 \leq i \neq i^* \leq m\}) \\ &\leq I(K_{i^*} \wedge \mathbf{P}X_{i^*}^n) + I(K_{i^*}, \mathbf{P}X_{i^*}^n \wedge \{\mathbf{P}V_i^n,\ 1 \leq i \neq i^* \leq m\}). \quad (4.31) \end{aligned}$$

Clearly, the first term on the right side of (4.31) is zero. Since for a fixed $\mathbf{P}$, $(K_{i^*}, \mathbf{P}X_{i^*}^n)$ are functions of $X_{i^*}^n$,

$$I(K_{i^*}, \mathbf{P}X_{i^*}^n \wedge \{\mathbf{P}V_i^n,\ 1 \leq i \neq i^* \leq m\}) \leq I(X_{i^*}^n \wedge \{V_i^n,\ 1 \leq i \neq i^* \leq m\}) = 0,$$

i.e., K_{i^*} is independent of $\mathbf{F}$, establishing (4.17). ∎

Proof of Theorem 4.4: For every $x_3^n \in \{0,1\}^n$, let $\mathcal{F}(x_3^n)$ denote the union of all regular subsets in $\bigcup_{i=1}^{2^u} A_i(x_3^n)$. Since $\mathcal{F}(x_3^n) \subseteq T_{X_1|X_3,\xi}^n(x_3^n)$,

$$\Pr\{X_1^n \in \mathcal{F}(X_3^n)\} = \Pr\{X_1^n \in T_{X_1|X_3,\xi}^n(X_3^n)\} - \Pr\{X_1^n \in T_{X_1|X_3,\xi}^n(X_3^n) \backslash \mathcal{F}(X_3^n)\}. \quad (4.32)$$

It follows from Proposition A.1 that $\Pr\{X_1^n \in T_{X_1|X_3,\xi}^n(X_3^n)\}$ goes to 1 exponentially rapidly in n. We shall show below that $\Pr\{X_1^n \in T_{X_1|X_3,\xi}^n(X_3^n) \backslash \mathcal{F}(X_3^n)\}$ goes to 0 exponentially rapidly in n.

Recall from Appendix A.1 that the number of different joint types of pairs in $\{0,1\}^n \times \{0,1\}^n$ does not exceed $(n+1)^4$. Thus,

$$\begin{aligned} \left| \{x_1^n : x_1^n \in T_{X_1|X_3,\xi}^n(x_3^n) \backslash \mathcal{F}(x_3^n)\} \right| &\leq 2^u \cdot (n+1)^4 \cdot 2^{n[I(X_1 \wedge X_2|X_3) - \varepsilon']} \\ &< (n+1)^4 \cdot 2^{n[H(X_1|X_3) + \varepsilon - \varepsilon']}, \end{aligned}$$

where the previous inequality is from $u < n[h_b(p) + \varepsilon] = n[H(X_1|X_2, X_3) + \varepsilon]$.

Since $P_{X_1|X_3}^n(x_1^n|x_3^n) \leq 2^{-n[H(X_1|X_3) - 2\xi]}$, $(x_1^n, x_3^n) \in T_{X_1X_3,\xi}^n$, we get

$$\Pr\{X_1^n \in T_{X_1|X_3,\xi}^n(X_3^n) \backslash \mathcal{F}(X_3^n)\} < (n+1)^4 \cdot 2^{-n(\varepsilon' - 2\xi - \varepsilon)}.$$

Choosing $\varepsilon' > 2\xi + \varepsilon$, $\Pr\{X_1^n \in T^n_{X_1|X_3,\xi}(X_3^n)\backslash\mathcal{F}(X_3^n)\}$ goes to 0 exponentially rapidly. Therefore, it follows from (4.32) that $\Pr\{X_1^n \in \mathcal{F}(X_3^n)\}$ goes to 1 exponentially rapidly in n, with an exponent depending on $(\xi, \varepsilon, \varepsilon')$.

By the PK construction scheme,

$$\begin{aligned}
\Pr\{K_1 \neq K_2\} &= \Pr\{K_1 \neq K_2, X_1^n \in \mathcal{F}(x_3^n)\} + \Pr\{K_1 \neq K_2, X_1^n \notin \mathcal{F}(x_3^n)\} \\
&\leq \Pr\{\hat{X}_2^n(1) \neq X_1^n, X_1^n \in \mathcal{F}(x_3^n)\} + \Pr\{X_1^n \notin \mathcal{F}(x_3^n)\} \\
&\leq \Pr\{\hat{X}_2^n(1) \neq X_1^n) + \Pr(X_1^n \notin \mathcal{F}(X_3^n)\}.
\end{aligned}$$

Since $\Pr\{\hat{X}_2^n(1) \neq X_1^n\} < 2^{-n\eta}$, by the observation in the previous paragraph, we have

$$\Pr\{K_1 \neq K_2\} < 2^{-n\eta'},$$

for some $\eta' = \eta'(\eta, \xi, \varepsilon, \varepsilon') > 0$ and for all sufficiently large n, which is (4.22).

Next, we shall show that K_1 satisfies the uniformity condition (4.24). For $x_3^n \in \{0,1\}^n$ and $1 \leq k \leq 2^{n[I(X_1 \wedge X_2|X_3) - \varepsilon']}$, it is clear by choice that

$$\Pr\{K_1 = k | X_1^n \notin \mathcal{F}(x_3^n), X_3^n = x_3^n\} = 2^{-n[I(X_1 \wedge X_2|X_3) - \varepsilon']},$$

and that

$$\begin{aligned}
& \Pr\{K_1 = k | X_1^n \in \mathcal{F}(x_3^n), X_3^n = x_3^n\} \\
= \;& \frac{\Pr\{K_1 = k, X_1^n \in \mathcal{F}(x_3^n) | X_3^n = x_3^n\}}{\Pr\{X_1^n \in \mathcal{F}(x_3^n) | X_3^n = x_3^n\}} \\
= \;& \frac{\sum_{i=1}^{2^u} \sum_{j=1}^{N_i(x_3^n)} \Pr\{X_1^n = b^n_{i,j,k}(x_3^n) | X_3^n = x_3^n\}}{\sum_{i=1}^{2^u} \sum_{j=1}^{N_i(x_3^n)} 2^{n[I(X_1 \wedge X_2|X_3) - \varepsilon']} \Pr\{X_1^n = b^n_{i,j,k}(x_3^n) | X_3^n = x_3^n\}} \qquad (4.33) \\
= \;& 2^{-n[I(X_1 \wedge X_2|X_3) - \varepsilon']},
\end{aligned}$$

where (4.33) is due to every regular subset consisting of sequences of the same joint type with x_3^n. Therefore,

$$\Pr\{K_1 = k\} = \sum_{x_3^n \in \{0,1\}^n} \Pr\{K_1 = k, X_3^n = x_3^n\}$$

$$
\begin{aligned}
&= \sum_{x_3^n \in \{0,1\}^n} [\Pr\{X_1^n \in \mathcal{F}(x_3^n), X_3^n = x_3^n\} \cdot \Pr\{K_1 = k | X_1^n \in \mathcal{F}(x_3^n), X_3^n = x_3^n\} \\
&\qquad + \Pr\{X_1^n \notin \mathcal{F}(x_3^n), X_3^n = x_3^n\} \cdot \Pr\{K_1 = k | X_1^n \notin \mathcal{F}(x_3^n), X_3^n = x_3^n\}] \\
&= 2^{-n[I(X_1 \wedge X_2 | X_3) - \varepsilon']}, \qquad (4.34)
\end{aligned}
$$

i.e., K_1 is uniformly distributed on $\left\{1, \cdots, 2^{n[I(X_1 \wedge X_2 | X_3) - \varepsilon']}\right\}$, with

$$\frac{1}{n} H(K_1) = I(X_1 \wedge X_2 | X_3) - \varepsilon',$$

which is (4.25).

It remains to show that K_1 satisfies the secrecy condition (4.23), with $(X_3^n, \mathbf{F}) = (X_3^n, \mathbf{P}X_1^n)$. For $x_3^n \in \{0,1\}^n$, $1 \le i \le 2^u$ and $1 \le k \le 2^{n[I(X_1 \wedge X_2 | X_3) - \varepsilon']}$, we have

$$\Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \notin \mathcal{F}(x_3^n), X_3^n = x_3^n\} = 2^{-n[I(X_1 \wedge X_2 | X_3) - \varepsilon']},$$

by choice, and

$$
\begin{aligned}
&\Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \in \mathcal{F}(x_3^n), X_3^n = x_3^n\} \\
&= \frac{\Pr\{K_1 = k, \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \in \mathcal{F}(x_3^n) | X_3^n = x_3^n\}}{\Pr\{\mathbf{P}X_1^n = \mathbf{P}e_i^n, X_1^n \in \mathcal{F}(x_3^n) | X_3^n = x_3^n\}} \\
&= \frac{\sum_{j=1}^{N_i(x_3^n)} \Pr\{X_1^n = b_{i,j,k}^n(x_3^n) | X_3^n = x_3^n\}}{\sum_{j=1}^{N_i(x_3^n)} 2^{n[I(X_1 \wedge X_2 | X_3) - \varepsilon']} \Pr\{X_1^n = b_{i,j,k}^n(x_3^n) | X_3^n = x_3^n\}} \\
&= 2^{-n[I(X_1 \wedge X_2 | X_3) - \varepsilon']}.
\end{aligned}
$$

Hence,

$$\Pr\{K_1 = k | \mathbf{P}X_1^n = \mathbf{P}e_i^n, X_3^n = x_3^n\} = 2^{-n[I(X_1 \wedge X_2 | X_3) - \varepsilon']} = \Pr\{K_1 = k\},$$

where the previous equality follows from (4.34). In other words, K_1 is independent of $(X_3^n, \mathbf{F})$, establishing (4.23). ■

4.5 Implementation Using LDPC Codes

4.5.1 Preliminaries Concerning LDPC Codes

The following standard definitions on LDPC codes can be found, for instance, in [57], [34], [52], [60].

A linear code is associated with a graphical representation, by means of a bipartite graph whose *left* (or *variable*) nodes correspond to coordinates of a codeword and *right* (or *check*) nodes correspond to the set of parity check constraints satisfied by codewords of this code. The bipartite graph representing a linear $(n, n-u)$ code has n variable nodes and u check nodes. A variable node is connected with a check node if the coordinate corresponding to that variable node is involved in the parity check constraint corresponding to that check node.

Binary LDPC codes are binary linear codes with low density parity check matrices in the sense that the parity check matrices contain relatively few 1s. In a parity check matrix for a (l, r)-*regular* LDPC code, every row has r 1s and every column has l 1s. Thus, a (l, r)-regular LDPC code is represented by a bipartite graph in which the degree of every variable node is l and the degree of every check node is r.

An *irregular* LDPC code with degree distribution pair $(\lambda(x), \rho(x))$ is represented by a bipartite graph, in which the degrees of variable nodes (resp. check nodes) are chosen according to the distribution $\lambda(x) = \sum_i \lambda_i x^{i-1}$ (resp. $\rho(x) = \sum_i \rho_i x^{i-1}$), with λ_i (resp. ρ_i) denoting the fraction of edges connecting variable (resp. check) nodes of degree i.

The rate of a (l, r)-regular LDPC code is $1 - \frac{l}{r}$ and the rate of an irregular LDPC code with degree distribution pair $(\lambda(x), \rho(x))$ is given by $1 - \frac{\int_0^1 \rho(x)dx}{\int_0^1 \lambda(x)dx}$.

4.5.2 Implementation for Model 4.1

The implementation of the SK construction scheme for Model 4.1 is illustrated below by using binary LDPC codes.

(i) LDPC code:

Since every linear code is equivalent to a *systematic code* (cf. e.g., [49, p. 46]), without loss of generality, we consider a systematic $(n, n-u)$ LDPC code $\mathcal{C}$ with generator matrix $\mathbf{G} = [\mathbf{I}_{n-u}\ \mathbf{A}]$, where $\mathbf{I}_{n-u}$ is an $(n-u) \times (n-u)$ identity matrix and $\mathbf{A}$ is an $(n-u) \times u$ matrix. Then, the parity check matrix for $\mathcal{C}$ is $\mathbf{P} = [\mathbf{A}^t\ \mathbf{I}_u]$, where $\mathbf{I}_u$ is an $u \times u$ identity matrix.

The first $n-u$ bits of every codeword in $\mathcal{C}$, which are called *information bits*, are pairwise distinct. Further, since the coset of $\mathcal{C}$ with coset leader e_i^n, $1 \leq i \leq 2^u$, must contain the sequence $b_i^n = [0^{n-u}\ e_i^n \mathbf{P}^t]$, with 0^{n-u} denoting a sequence of $n-u$ zeros, the first $n-u$ bits of every sequence in this coset $\{b_i^n \oplus c^n,\ c^n \in \mathcal{C}\}$ are pairwise distinct.

(ii) SW data compression:

The following scheme is known from [32].

Terminal $\mathcal{X}_1$ transmits the syndrome $\mathbf{P}x_1^n$. Terminal $\mathcal{X}_2$, with the knowledge of x_2^n, $\mathbf{P}x_1^n$, and (the crossover probability) p, applies the following *belief-propagation* algorithm [32] to estimate $\hat{x}_2^n(1)$.

Let $(v_1, \cdots, v_n)$ and $(w_1, \cdots, w_u)$ denote variable-node sets and check-node sets in the bipartite graph representing $\mathcal{C}$. Depict by $v_i \sim w_j$ (or equivalently, $w_j \sim v_i$), if the variable node v_i is connected with the check node w_j. The decoding algorithm will proceed in iterations. Each iteration starts by propagating messages from variable nodes to check nodes and ends by sending messages from check nodes back to variable nodes. Messages are propagated only between the connected nodes.

Let $M^{(k)}_{v_i \to w_j}$ denote the message propagated from the variable node v_i to the check node w_j in the k^{th} iteration, $k \geq 1$. Let $M^{(k)}_{w_j \to v_i}$ denote the message propagated from the check node w_j to the variable node v_i in the k^{th} iteration. Then, set

$$M^{(k)}_{v_i \to w_j} = (1 - 2x_{2,i}) \log \frac{1-p}{p} + \sum_{l: l \neq j, w_l \sim v_i} M^{(k-1)}_{w_l \to v_i},$$

and

$$M^{(k)}_{w_j \to v_i} = 2 \tanh^{-1} \left[(1 - 2s_j) \prod_{l: l \neq i, v_l \sim w_j} \tanh \left(\frac{M^{(k)}_{v_l \to w_j}}{2} \right) \right],$$

where $x_{2,i}$ denotes the i^{th} bit of x_2^n and s_j denotes the j^{th} bit of $\mathbf{P}x_1^n$. By definition, $M^{(0)}_{w_l \to v_i} = 0$.

At the end of the k^{th} iteration, estimate $\hat{x}_2^n(1) = (\hat{x}_2(1,1), \cdots, \hat{x}_2(1,n))$ as

$$\hat{x}_2(1,i) = \begin{cases} 0, & \text{if } (1 - 2x_{2,i}) \log \frac{1-p}{p} + \sum_{j: w_j \sim v_i} M^{(k)}_{w_j \to v_i} \geq 0, \\ 1, & \text{if } (1 - 2x_{2,i}) \log \frac{1-p}{p} + \sum_{j: w_j \sim v_i} M^{(k)}_{w_j \to v_i} < 0. \end{cases}$$

This procedure is terminated if either $\mathbf{P}\hat{x}_2^n(1) = \mathbf{P}x_1^n$ or a designated number of iterations has been reached.

(iii) SK construction:

Since the first $n - u$ bits of every sequence in each coset of $\mathcal{C}$ are pairwise distinct, these $n - u$ bits can serve as the index of the sequence in its coset. Therefore, terminal $\mathcal{X}_1$ (resp. $\mathcal{X}_2$) could simply set K_1 (resp. K_2) as the first $n - u$ bits of x_1^n (resp. $\hat{x}_2^n(1)$).

The same implementation of the SW data compression scheme above applies for Models 4.2 and 4.4. They can also be applied repeatedly for the successive estimates in Model 4.3.

In Model 4.3, K_{i^*} (resp. K_i, $i \neq i^*$) is simply set as the first $n - u$ bits of $x_{i^*}^n$ (resp. $\hat{x}_i^n(i^*)$). However, the current complexity of generating regular subsets for Models 4.2 and 4.4 poses a hurdle in explicit constructions of SKs or PKs for these models.

4.5.3 Simulation Results

In this subsection, we provide simulation results on the tradeoff between the relative secrecy rate (i.e., the difference between the rate of the generated SK and the SK-capacity) and the rate of generating unequal SKs at different terminals, when LDPC codes are used in the SK construction problem for Model 4.1.

For the purposes of comparison, three different kinds of LDPC codes are used:

- a $(3, 4)$-regular LDPC code;
- a $(3, 6)$-regular LDPC code;

and

- an irregular LDPC code with degree distribution pair (cf. [32])

$$\begin{aligned}\lambda(x) &= 0.234029x + 0.212425x^2 + 0.146898x^5 + 0.102840x^6 + 0.303808x^{19},\\ \rho(x) &= 0.71875x^7 + 0.28125x^8.\end{aligned}$$

The codeword lengths of all the three LDPC codes are 10^3 bits. The rate of the first LDPC code is $\frac{1}{4}$ bit/channel use, while the rate of the other two LDPC codes is $\frac{1}{2}$ bit/channel use. Sixty iterations of the belief-propagation algorithm are allowed. More than 10^3 blocks are transmitted from terminal $\mathcal{X}_1$.

Simulation results are shown in Figures 4.1 and 4.2, where conditional entropy (i.e., $H(X_1|X_2) = h_b(p)$) is plotted against key bit error rate (KBER). We remark that in this work, SKs are generated at fixed rates, which are equal to the rates of LDPC codes used. Since the SK-capacity is given by $1 - h_b(p)$, the conditional entropy $h_b(p)$ can serve as an indicator of the gap between the rate of the generated SK and the SK-capacity. On the other hand, the KBER is related to the rate of generating unequal SKs at different terminals

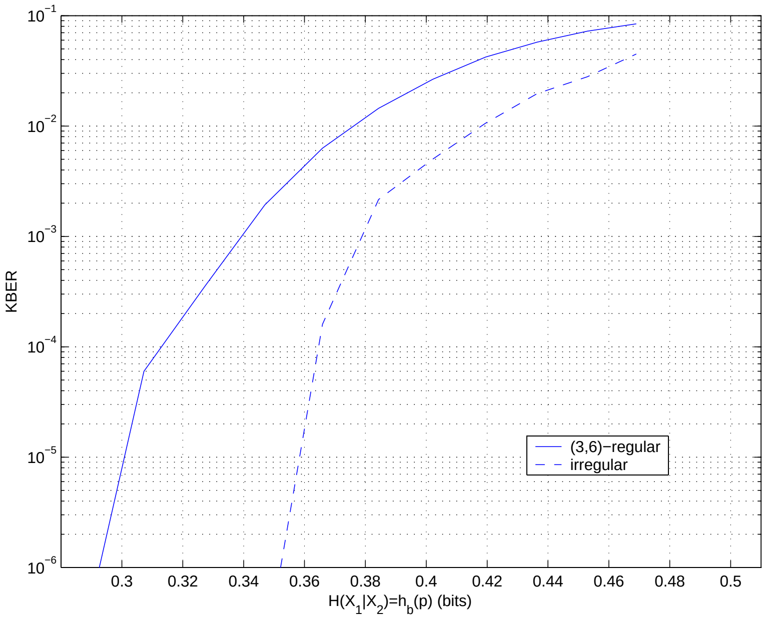


Figure 4.1: Simulation results for the $(3,6)$-regular and the irregular LDPC codes.

Figure 4.1 shows the performance of the $(3,6)$-regular and the irregular LDPC codes; figure 4.2 shows the performance of the $(3,4)$-regular LDPC code. It is seen in both figures that KBER increases with $h_b(p)$. Since the SK-capacity decreases with $h_b(p)$, the increase of $h_b(p)$ narrows the gap between the rate of the generated SK and the SK-capacity, but raises the possibility of generating unequal SKs at different terminals. In contrast, the decrease of $h_b(p)$ widens the gap between the rate of the generated SK and the SK-capacity, but reduces the possibility of generating unequal SKs at different terminals.

It is seen from Figure 4.1 that the irregular LDPC code outperforms the $(3,6)$-regular LDPC code. For instance, for a fixed crossover probability $p = 0.068$, say, and $h_b(p) \approx 0.3584$, the KBER with the use of the irregular LDPC code is as low as 10^{-5}, while the KBER with the use of the $(3,6)$-regular LDPC code is only about 4×10^{-3}.

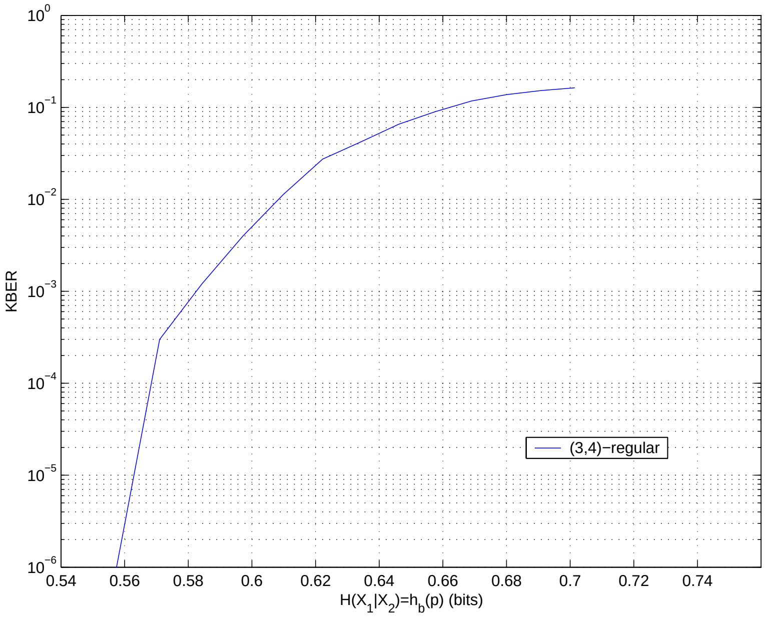


Figure 4.2: Simulation results for the $(3, 4)$-regular LDPC code.

Chapter 5

The Relationship Between the Common Randomness Capacity and the Secret Key Capacity for Source Models with Rate Constraints

5.1 Introduction

It has been described in Chapter 4 that for a source model consisting of an arbitrary number of terminals which respectively observe the distinct components of a DMMS followed by *unrestricted* public communication among themselves, the CR-capacity, i.e., the largest rate of CR that is achieved by the terminals, can be decomposed into the smallest sum-rate of the communication needed to achieve the CR-capacity, and the SK-capacity (i.e., the largest rate at which all the terminals can generate a SK). This leads to the following question: what is the relationship between the CR-capacity and the SK-capacity for a given source model with rate constraints on the public communication?

Ahlswede and Csiszár [4] have determined the CR-capacities for several two-terminal source models with rate constraints on the public communication. On the other hand, the SK-capacities for these two-terminal source models are given in [16]. However, the relationship between the CR-capacities and the SK-capacities for these models has not yet been examined. In this chapter, we shall discuss this relationship for several two-terminal source models[1] with rate constraints on the public communication.

The rest of this chapter is organized as follows. Section 5.2 contains the prelim-

[1] The CR-capacities are still unknown, in general, for source models consisting of more than two terminals, and with rate constraints on the public communication. We do not discuss the relationship between the CR-capacities and the SK-capacities for source models consisting of more than two terminals here.

inaries. In Section 5.3, we shall consider three simple two-terminal source models, the first two of which have known CR-capacities and SK-capacities. Our main results – the CR-capacity and the SK-capacity for the third model, as well as the smallest sum-rate of the communication needed to achieve the CR-capacity for each of the three models – are provided in Section 5.4. We observe that in each of the three models, the SK-capacity is equal to the difference between the CR-capacity and the smallest sum-rate of the communication needed to achieve the CR-capacity. The proofs are given in Section 5.5.

5.2 Preliminaries

Consider a DMMS with $m \geq 2$ components, with corresponding generic rvs $X_1, \cdots, X_m$ taking values in finite alphabets $\mathcal{X}_1, \cdots, \mathcal{X}_m$, respectively. Let $X_i^n = (X_{i,1}, \cdots, X_{i,n})$, $1 \leq i \leq m$, be n i.i.d. repetitions of the rv X_i. Terminals $\mathcal{X}_1, \cdots, \mathcal{X}_m$, with respective observations $X_1^n, \cdots, X_m^n$, represent the m users who wish to generate CR or a SK by public communication.

Each terminal can communicate with every other terminal through noiseless broadcasts. The transmissions can be assumed, without any loss of generality, to occur in rm $(r \geq 1)$ consecutive time slots in r rounds. The communication can be depicted by rm rvs $F_1, \cdots, F_{rm}$, where F_t denotes the transmission in time slot t, $1 \leq t \leq rm$, by the terminal $\mathcal{X}_i$, $i = t \bmod m$. In general, F_t is allowed to be any function, defined in terms of a mapping f_t, of the observations at the terminal $\mathcal{X}_i$ and of the previous transmissions $F_{[1,t-1]} = (F_1, \cdots, F_{t-1})$. No other resources are available to these m terminals; in particular, additional randomization is not permitted at the terminals.

Denote by $\mathbf{F}_i$, $1 \leq i \leq m$, all the transmissions from terminal $\mathcal{X}_i$. Since the transmissions from terminal $\mathcal{X}_i$ occur in time slots $i, \cdots, i+(r-1)m$, $\mathbf{F}_i = \{F_{i+jm}, 0 \leq j \leq r-1\}$. Suppose that $\mathbf{F}_i$, $1 \leq i \leq m$, is subject to the rate constraint R_i, i.e.,

$$\frac{1}{n} \log ||\mathbf{F}_i|| \triangleq \frac{1}{n} \sum_{j=0}^{r-1} \log ||F_{i+jm}|| \leq R_i, \quad 1 \leq i \leq m, \tag{5.1}$$

where $||F_{i+jm}||$ denotes the cardinality of the range of F_{i+jm}. Such rate constraints imposed on transmissions depict bandwidth limitations associated with the use of shared public channels. The notation $R_i = \infty$ will be used to denote the fact that constraint (5.1) is not imposed for that i.

The rv K, as a function of $(X_1^n, \cdots, X_m^n)$ and with finite range $\mathcal{K}$, represents ε-*common randomness* (ε-CR), achievable with communication $\mathbf{F} = (\mathbf{F}_1, \cdots, \mathbf{F}_m)$, if K is ε-recoverable from $(\mathbf{F}, X_i^n)$ for each $1 \leq i \leq m$.

Definition 5.1 *A nonnegative number R is an achievable CR rate if for every $\varepsilon > 0$ and all sufficiently large n, there exists ε-CR K, achieved with $\mathbf{F} = (\mathbf{F}_1, \cdots, \mathbf{F}_m)$ satisfying the rate constraints (5.1), such that*

$$\frac{1}{n} H(K) > R - \varepsilon.$$

The largest achievable CR rate is called the CR-capacity, denoted by $C_{CR}(R_1, \cdots, R_m)$.

Definition 5.2 *A nonnegative number R is an achievable sum-rate of "communication for largest common randomness" (CLCR sum-rate) if for every $\varepsilon > 0$ and all sufficiently large n, ε-CR with rate larger than $C_{CR}(R_1, \cdots, R_m) - \varepsilon$ is achievable with communication $\mathbf{F} = (\mathbf{F}_1, \cdots, \mathbf{F}_m)$ satisfying the rate constraints (5.1), such that for every $\xi > 0$,*

$$\frac{1}{n} \sum_{i=1}^{m} \log ||\mathbf{F}_i|| = \frac{1}{n} \sum_{i=1}^{m} \sum_{j=0}^{r-1} \log ||F_{i+jm}|| < R + \xi.$$

The smallest achievable CLCR sum-rate is denoted by $R_{min}(R_1, \cdots, R_m)$.

Remark: It follows directly from the definitions above that

$$C_{CR}(R_1, \cdots, R_m) \leq H(X_1, \cdots, X_m),$$

and

$$R_{min}(R_1, \cdots, R_m) \leq \sum_{i=1}^{m} R_i.$$

The rv $K_{\mathcal{M}}$, with finite range $\mathcal{K}_{\mathcal{M}}$, represents an ε-*secret key* (ε-SK), achieved with communication $\mathbf{F}$, if $K_{\mathcal{M}}$ is ε-CR and $K_{\mathcal{M}}$ satisfies the secrecy condition

$$\frac{1}{n} I(K_{\mathcal{M}} \wedge \mathbf{F}) < \varepsilon,$$

and the uniformity condition

$$\frac{1}{n} H(K_{\mathcal{M}}) \geq \frac{1}{n} \log |\mathcal{K}_{\mathcal{M}}| - \varepsilon.$$

Definition 5.3 *A nonnegative number R is called an achievable SK rate if for every $\varepsilon > 0$ and all sufficiently large n, there exist ε-SKs $K_{\mathcal{M}}$, achieved with $\mathbf{F}$ satisfying the rate constraints (5.1), such that*

$$\frac{1}{n} H(K_{\mathcal{M}}) > R - \varepsilon.$$

The largest achievable SK rate is called the SK-capacity, denoted by $C_S(R_1, \cdots, R_m)$.

Remark: Note that the definitions of the CR-capacity and the SK-capacity are in the "weak sense." (cf. e.g, [3], [17]) While all our results below are presented in the "weak sense," they can be established in the stronger sense of [37] by using the techniques developed in [40].

Let $C_{CR}(\infty, \cdots, \infty)$, $R_{min}(\infty, \cdots, \infty)$, and $C_S(\infty, \cdots, \infty)$ [2] respectively denote the CR-capacity, the smallest achievable CLCR sum-rate, and the SK-capacity, when there

[2] These notations are in effect, identical to R_{min} and C_S in Chapter 4.

are no rate constraints (5.1), i.e., $R_i = \infty$, $1 \leq i \leq m$. Clearly,

$$C_{CR}(\infty, \cdots, \infty) = H(X_1, \cdots, X_m),$$

$$R_{min}(\infty, \cdots, \infty) = \min_{(r_1, \cdots, r_m) \in \mathcal{R}} \sum_{i=1}^{m} r_i,$$

with

$$\mathcal{R} = \left\{ (r_1, \cdots, r_m) : \sum_{i:\ \mathcal{X}_i \in \mathcal{B}} r_i \geq H(X_{\mathcal{B}} | X_{\mathcal{B}^c}), \mathcal{B} \subset \{\mathcal{X}_1, \cdots, \mathcal{X}_m\} \right\},$$

and

$$C_S(\infty, \cdots, \infty) = H(X_1, \cdots, X_m) - R_{min}(\infty, \cdots, \infty).$$

This suggests that under unrestricted public communication, the CR-capacity $C_{CR}(\infty, \cdots, \infty)$ can be decomposed into the smallest achievable CLCR sum-rate $R_{min}(\infty, \cdots, \infty)$ and the SK-capacity $C_S(\infty, \cdots, \infty)$.

In this chapter, we study the relationship between $C_{CR}(R_1, \cdots, R_m)$, $R_{min}(R_1, \cdots, R_m)$ and $C_S(R_1, \cdots, R_m)$ in the presence of rate constraints (5.1); in particular, we examine whether and in which situations the relation

$$C_S(R_1, \cdots, R_m) = C_{CR}(R_1, \cdots, R_m) - R_{min}(R_1, \cdots, R_m)$$

holds.

5.3 Previous Results

Model 5.1: Let the terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ observe, respectively, n i.i.d. repetitions of the correlated rvs X_1 and X_2. These terminals wish to generate CR or a SK by means of a single transmission from terminal $\mathcal{X}_1$, which is subject to the rate constraint R_1.

Note that Model 5.1 is a special case of the general source model in Section 5.1 for $m = 2$, $r = 1$, $R_1 > 0$, and $R_2 = 0$. The CR-capacity for this model, denoted by

$C_{CR}(R_1, 0)$, is [4]

$$C_{CR}(R_1, 0) = \max_U I(U \wedge X_1),$$

where the maximum is over all rvs U that satisfy the Markov condition

$$U -\circ- X_1 -\circ- X_2, \tag{5.2}$$

and the rate condition

$$I(U \wedge X_1 | X_2) \leq R_1. \tag{5.3}$$

Furthermore, the maximum is attained by a rv U taking values in set $\mathcal{U}$ of cardinality $|\mathcal{U}| \leq |\mathcal{X}_1|$.

The SK-capacity for this model, denoted by $C_S(R_1, 0)$, is [16]

$$C_S(R_1, 0) = \max_U I(U \wedge X_2),$$

where the rv U satisfies (5.2) – (5.3). Also, it is known [3], [36] that if $R_1 \geq H(X_1|X_2)$,

$$C_{CR}(R_1, 0) = H(X_1),$$

and

$$C_S(R_1, 0) = I(X_1 \wedge X_2).$$

Model 5.2: Let the terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ observe, respectively, n i.i.d. repetitions of the correlated rvs X_1 and X_2. These terminals wish to generate CR or a SK by means of two transmissions: one from terminal $\mathcal{X}_1$, which is subject to the rate constraint R_1; the other from terminal $\mathcal{X}_2$, which is subject to the rate constraint R_2.

Note that Model 5.1 is a special case of the general source model in Section 5.1 for $m = 2$, $r = 1$, $R_1 > 0$, and $R_2 > 0$. The CR-capacity for this model, denoted by $C_{CR}(R_1, R_2)$, is [4]

$$C_{CR}(R_1, R_2) = \max_{U,V} I(U, V \wedge X_1, X_2),$$

where the maximum is over all pairs of rvs (U, V) that satisfy the Markov conditions

$$U -\!\!\circ\!\!- X_1 -\!\!\circ\!\!- X_2, \quad V -\!\!\circ\!\!- X_2, U -\!\!\circ\!\!- X_1, \tag{5.4}$$

and the rate conditions

$$I(U \wedge X_1|X_2) \le R_1, \quad I(V \wedge X_2|X_1, U) \le R_2. \tag{5.5}$$

Furthermore, the maximum is attained by a pair of rvs (U, V) taking values in sets $(\mathcal{U}, \mathcal{V})$ of cardinalities $|\mathcal{U}| \le |\mathcal{X}_1| + 3$, $|\mathcal{V}| \le |\mathcal{X}_2|$.

The SK-capacity for this model, denoted by $C_S(R_1, R_2)$, is [16]

$$C_S(R_1, R_2) = \max_{U,V}[I(U \wedge X_2) + I(V \wedge X_1|U)],$$

where the rvs U, V satisfy (5.4) – (5.5). Also, it is known [3], [17], [36] that if either $R_1 \ge H(X_1|X_2)$ or $R_2 \ge H(X_2|X_1)$,

$$C_S(R_1, R_2) = I(X_1 \wedge X_2),$$

and

$$C_{CR}(R_1, R_2) = \begin{cases} H(X_1, X_2), & \text{if } R_1 \ge H(X_1|X_2) \text{ and } R_2 \ge H(X_2|X_1), \\ R_2 + H(X_1), & \text{if } R_1 \ge H(X_1|X_2) \text{ and } R_2 < H(X_2|X_1), \\ R_1 + H(X_2), & \text{if } R_1 < H(X_1|X_2) \text{ and } R_2 \ge H(X_2|X_1). \end{cases}$$

Model 5.3: Let the terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ observe, respectively, n i.i.d. repetitions of the correlated rvs X_1 and X_2. These terminals wish to generate CR or a SK by means of two-way multiple rounds (say r rounds) of transmissions. The transmissions from terminal $\mathcal{X}_1$ (resp. $\mathcal{X}_2$) are subject to the rate constraint R_1 (resp. R_2).

Note that Model 5.1 is a special case of the general source model in Section 5.1 for $m = 2$, $R_1 > 0$, and $R_2 > 0$.

5.4 Statement of Results

The following theorem characterizes the smallest achievable CLCR sum-rate for Model 5.1. Further, the CR-capacity for Model 5.1 is found to be equal to the sum of the SK-capacity and the smallest achievable CLCR sum-rate.

Theorem 5.1 *The smallest achievable CLCR sum-rate for Model 5.1 is*

$$R_{min}(R_1, 0) = \min\{R_1, H(X_1|X_2)\}.$$

Further,

$$C_S(R_1, 0) = C_{CR}(R_1, 0) - R_{min}(R_1, 0).$$

Remark: It readily follows from the Slepian-Wolf theorem that if $R_1 \geq H(X_1|X_2)$, $R_{min}(R_1, 0) = H(X_1|X_2)$. Further, it is clear from the characterizations of $C_{CR}(R_1, 0)$, $R_{min}(R_1, 0)$ and $C_S(R_1, 0)$ that if $R_1 \geq H(X_1|X_2)$, $C_S(R_1, 0)$ is equal to the difference between $C_{CR}(R_1, 0)$ and $R_{min}(R_1, 0)$.

The following theorem characterizes the smallest achievable CLCR sum-rate for Model 5.2. Further, the CR-capacity for Model 5.2 is found to be equal to the sum of the SK-capacity and the smallest achievable CLCR sum-rate.

Theorem 5.2 *The smallest achievable CLCR sum-rate for Model 5.2 is*

$$R_{min}(R_1, R_2) = \min\{R_1, H(X_1|X_2)\} + \min\{R_2, H(X_2|X_1)\}.$$

Further,

$$C_S(R_1, R_2) = C_{CR}(R_1, R_2) - R_{min}(R_1, R_2).$$

Remark: It follows from the Slepian-Wolf theorem that if $R_1 \geq H(X_1|X_2)$ and $R_2 \geq H(X_2|X_1)$,

$$R_{min}(R_1, R_2) = H(X_1|X_2) + H(X_2|X_1).$$

Further, it is clear from the characterizations of $C_{CR}(R_1, R_2)$, $R_{min}(R_1, R_2)$ and $C_S(R_1, R_2)$ that if either $R_1 \geq H(X_1|X_2)$ or $R_2 \geq H(X_2|X_1)$, $C_{CR}(R_1, R_2)$ is equal to the sum of $C_S(R_1, R_2)$ and $R_{min}(R_1, R_2)$.

The following three theorems characterize $C_{CR}(R_1, R_2)$, $C_S(R_1, R_2)$, and $R_{min}(R_1, R_2)$ for Model 5.3, respectively. Further, the CR-capacity for Model 5.3 is found to be equal to the sum of the SK-capacity and the smallest achievable CLCR sum-rate.

Theorem 5.3 *The CR-capacity $C_{CR}(R_1, R_2)$ for Model 5.3 is*

$$C_{CR}(R_1, R_2) = \max_{U_1,\cdots,U_r,V_1,\cdots,V_r} I(U_1, \cdots, U_r, V_1, \cdots, V_r \wedge X_1, X_2),$$

where the rvs $U_1, \cdots, U_r, V_1, \cdots, V_r$ satisfy the Markov conditions

$$U_i -\circ- X_1, U_1, \cdots, U_{i-1}, V_1, \cdots, V_{i-1} -\circ- X_2, \qquad 1 \leq i \leq r, \tag{5.6}$$

$$V_i -\circ- X_2, U_1, \cdots, U_i, V_1, \cdots, V_{i-1} -\circ- X_1, \qquad 1 \leq i \leq r, \tag{5.7}$$

and the rate conditions

$$\sum_{i=1}^{r} I(U_i \wedge X_1|X_2, U_1, \cdots, U_{i-1}, V_1, \cdots, V_{i-1}) \leq R_1, \tag{5.8}$$

$$\sum_{i=1}^{r} I(V_i \wedge X_2|X_1, U_1, \cdots, U_i, V_1, \cdots, V_{i-1}) \leq R_2. \tag{5.9}$$

Theorem 5.4 *The SK-capacity $C_S(R_1, R_2)$ for Model 5.3 is*

$$\begin{aligned} C_S(R_1, R_2) \quad = \quad & \max_{U_1,\cdots,U_r,V_1,\cdots,V_r} \sum_{i=1}^{r} [I(U_i \wedge X_2|U_1, \cdots, U_{i-1}, V_1, \cdots, V_{i-1}) \\ & + I(V_i \wedge X_1|U_1, \cdots, U_i, V_1, \cdots, V_{i-1})], \end{aligned}$$

where the rvs $U_1, \cdots, U_r, V_1, \cdots, V_r$ satisfy (5.6) – (5.9).

Remark: The maxima in Theorems 5.3 and 5.4 are attainable, since by a direct application of the Support Lemma [15, p. 310], the rvs $U_1, \cdots, U_r, V_1, \cdots, V_r$ can be assumed, without restricting generality, to take values in finite sets.

Theorem 5.5 *The smallest achievable CLCR sum-rate for Model 5.3 is*

$$R_{min}(R_1, R_2) = \min\{R_1, H(X_1|X_2)\} + \min\{R_2, H(X_2|X_1)\}.$$

Further,

$$C_S(R_1, R_2) = C_{CR}(R_1, R_2) - R_{min}(R_1, R_2).$$

5.5 Proofs

The technical tools used to prove Theorem 5.1 are supplied by Lemmas 5.1 and 5.2 below.

For a given joint probability mass function (pmf) $P_{X_1X_2}$, define

$$\mathcal{S}(R_1) \triangleq \left\{ \begin{array}{ll} P_{UX_1X_2} : & P_{UX_1X_2} = P_{U|X_1}P_{X_1X_2}, \\ & \sum_{u,x_1,x_2} P_{UX_1X_2} \log \frac{P_{UX_1|X_2}}{P_{U|X_2}P_{X_1|X_2}} \leq R_1 \end{array} \right\}. \tag{5.10}$$

Note that the CR-capacity for Model 5.1 is

$$C_{CR}(R_1, 0) = \max_{U: P_{UX_1X_2} \in \mathcal{S}(R_1)} I(U \wedge X_1).$$

Lemma 5.1 *Let X_1 and X_2 be $\mathcal{X}_1$- and $\mathcal{X}_2$-valued rvs with joint pmf $P_{X_1X_2} = P_{X_1}P_{X_2|X_1}$, where P_{X_1} is fixed. Then, $I(X_1 \wedge X_2)$ is a convex function of $P_{X_2|X_1}$. Furthermore, $I(X_1 \wedge X_2)$ is a strictly convex function of $P_{X_2|X_1}$, iff $P_{X_2|X_1} \neq P_{X_2}$, i.e., X_1 is not independent of X_2.*

Proof of Lemma 5.1: Fix P_{X_1}. Consider the conditional pmfs $P_{X_2|X_1}$ and $P_{X_2'|X_1}$, and let the corresponding joint pmfs on $\mathcal{X}_1 \times \mathcal{X}_2$ be $P_{X_1X_2}$ and $P_{X_1X_2'}$, respectively, and their respective marginals on $\mathcal{X}_2$ be P_{X_2} and $P_{X_2'}$. Let

$$P_{X_2^\lambda|X_1} = \lambda P_{X_2|X_1} + \bar{\lambda} P_{X_2'|X_1},$$

where $0 \leq \lambda \leq 1$ and $\bar{\lambda} = 1 - \lambda$. Clearly, for a given P_{X_1},

$$P_{X_1X_2^\lambda} = \lambda P_{X_1X_2} + \bar{\lambda} P_{X_1X_2'},$$

and

$$P_{X_2^\lambda} = \lambda P_{X_2} + \bar{\lambda} P_{X_2'}.$$

Then,

$$\begin{aligned}
I(X_1 \wedge X_2^\lambda) &= \sum_{x_1,x_2} P_{X_1X_2^\lambda} \log \frac{P_{X_1X_2^\lambda}}{P_{X_1}P_{X_2^\lambda}} \\
&= \sum_{x_1,x_2} (\lambda P_{X_1X_2} + \bar{\lambda} P_{X_1X_2'}) \log \frac{\lambda P_{X_1X_2} + \bar{\lambda} P_{X_1X_2'}}{\lambda P_{X_1}P_{X_2} + \bar{\lambda} P_{X_1}P_{X_2'}} \\
&\leq \sum_{x_1,x_2} \left[\lambda P_{X_1X_2} \log \frac{P_{X_1X_2}}{P_{X_1}P_{X_2}} + \bar{\lambda} P_{X_1X_2'} \log \frac{P_{X_1X_2'}}{P_{X_1}P_{X_2'}} \right] \qquad (5.11) \\
&= \lambda I(X_1 \wedge X_2) + \bar{\lambda} I(X_1 \wedge X_2'),
\end{aligned}$$

where (5.11) follows from the log-sum inequality (cf. e.g., [11, p. 29]). Hence, $I(X_1 \wedge X_2)$ is a convex function of $P_{X_2|X_1}$ for fixed P_{X_1}. According to the log-sum inequality, equality in (5.11) holds iff $P_{X_1X_2} = P_{X_1}P_{X_2}$ and $P_{X_1X_2'} = P_{X_1}P_{X_2'}$, proving strict convexity. This completes the proof. ■

Lemma 5.2 [3]*: For arbitrary rvs U, V and sequences of rvs $\mathbf{Y} = (Y_1, \cdots, Y_n)$, $\mathbf{Z} = (Z_1, \cdots, Z_n)$,*

$$\begin{aligned}
I(U \wedge \mathbf{Y}|V) - I(U \wedge \mathbf{Z}|V) &= \sum_{i=1}^{n} [I(U \wedge Y_i|Y_1, \cdots, Y_{i-1}, Z_{i+1}, \cdots, Z_n, V) \\
&\quad - I(U \wedge Z_i|Y_1, \cdots, Y_{i-1}, Z_{i+1}, \cdots, Z_n, V)].
\end{aligned}$$

■

Proof of Theorem 5.1: To prove the first part of this theorem, it suffices to show that $R_{min}(R_1, 0) \geq R_1$ for $R_1 < H(X_1|X_2)$.

Let K (with values in $\mathcal{K}$) be arbitrary ε-CR with rate

$$\frac{1}{n}H(K) \geq C_{CR}(R_1, 0) - \varepsilon,$$

achieved by a single transmission $\mathbf{F} = F_1 = f_1(X_1^n)$. We shall show below that for every $\xi > 0$ and for all sufficiently large n,

$$\frac{1}{n}\log ||\mathbf{F}|| \geq R_1 - \xi.$$

Since K is ε-recoverable from X_1^n, there exists a rv K', as a function of X_1^n and taking values in $\mathcal{K}$, such that

$$\Pr\{K' \neq K\} \leq \varepsilon.$$

It follows from Fano's inequality that

$$\frac{1}{n}H(K') \geq \frac{1}{n}H(K) - \frac{\varepsilon \log |\mathcal{K}| + 1}{n} \geq C_{CR}(R_1, 0) - \varepsilon - \frac{\varepsilon \log |\mathcal{K}| + 1}{n}.$$

Let $\tilde{U} = K' X_{1,1} \cdots X_{1,J-1} X_{2,J+1} \cdots X_{2,n} J$, where J is a rv independent of (X_1^n, X_2^n) and uniformly distributed on $\{1, \cdots, n\}$. It is easily seen that

$$\tilde{U} -\!\circ\!- X_{1,J} -\!\circ\!- X_{2,J}.$$

By applying Lemma 5.2 and the fact that $(X_{1,i}, X_{2,i})$ is independent of $(X_{1,1}, \cdots, X_{1,i-1}, X_{2,i+1}, \cdots, X_{2,n})$, we have

$$I(K' \wedge X_1^n) - I(K' \wedge X_2^n) = n\left[I(\tilde{U} \wedge X_{1,J}) - I(\tilde{U} \wedge X_{2,J})\right].$$

Considering that

$$I(K' \wedge X_1^n) - I(K' \wedge X_2^n) \;\; = \;\; H(K'|X_2^n)$$

$$\begin{aligned} &= I(K' \wedge \mathbf{F}|X_2^n) + H(K'|X_2^n, \mathbf{F}) \\ &\leq H(\mathbf{F}) + 2\varepsilon \log|\mathcal{K}| + 1 \qquad (5.12) \\ &\leq nR_1 + 2\varepsilon \log|\mathcal{K}| + 1, \end{aligned}$$

where (5.12) follows from Fano's inequality, with K' being 2ε-recoverable from $(X_2^n, \mathbf{F})$, we have

$$I(\tilde{U} \wedge X_{1,J}) - I(\tilde{U} \wedge X_{2,J}) \leq R_1 + \frac{2\varepsilon \log|\mathcal{K}| + 1}{n}.$$

As $X_{1,J}$, $X_{2,J}$ can be identified with the rvs X_1, X_2 of the DMMS, the rv $\tilde{U}$ satisfies the Markov condition (5.2) and the rate condition (5.3). Note that

$$H(K') = I(K' \wedge X_1^n) = \sum_{i=1}^{n} I(K' \wedge X_{1,i}|X_{1,1}, \cdots, X_{1,i-1}) \leq nI(\tilde{U} \wedge X_{1,J}).$$

Hence,

$$\begin{aligned} I(\tilde{U} \wedge X_1) &\geq \frac{1}{n}H(K') \\ &\geq C_{CR}(R_1, 0) - \varepsilon - \frac{\varepsilon \log|\mathcal{K}| + 1}{n} \\ &= \max_{U: P_{UX_1X_2} \in \mathcal{S}(R_1)} I(U \wedge X_1) - \varepsilon - \frac{\varepsilon \log|\mathcal{K}| + 1}{n}, \qquad (5.13) \end{aligned}$$

i.e., $I(\tilde{U} \wedge X_1)$ is arbitrarily close to the maximum of $I(U \wedge X_1)$ on $\mathcal{S}(R_1)$.

Note that for every $P_{UX_1X_2} \in \mathcal{S}(R_1)$, we can write

$$I(U \wedge X_1) = I(U \wedge X_1, X_2) = I(U \wedge X_1|X_2) + I(U \wedge X_2),$$

where $I(U \wedge X_1|X_2)$ can be chosen to equal R_1, provided $R_1 < H(X_1|X_2)$. Hence,

$$\max_{U: P_{UX_1X_2} \in \mathcal{S}(R_1)} I(U \wedge X_1) = R_1 + \max_{U: P_{UX_1X_2} \in \mathcal{S}(R_1)} I(U \wedge X_2)$$

is achieved with

$$I(U \wedge X_1|X_2) = R_1. \qquad (5.14)$$

Furthermore, by Lemma 5.1, $I(U \wedge X_1)$ is a convex function of $P_{U|X_1}$ for fixed P_{X_1}, where the convexity is not strict iff U is independent of X_1, which corresponds to the minimum of $I(U \wedge X_1)$. Considering that $I(U \wedge X_1)$ is a continuous function of P_{UX_1}, with the rv $\tilde{U}$ defined above satisfying (5.13), we have for every $\delta > 0$,

$$I(\tilde{U} \wedge X_1) - I(\tilde{U} \wedge X_2) = I(\tilde{U} \wedge X_1|X_2) \geq R_1 - \delta.$$

It readily follows from (5.12) that

$$\frac{1}{n}\log||\mathbf{F}|| \geq \frac{1}{n}H(\mathbf{F}) \geq I(\tilde{U} \wedge X_1) - I(\tilde{U} \wedge X_2) - \frac{2\varepsilon\log|\mathcal{K}|+1}{n} \geq R_1 - \delta - \frac{2\varepsilon\log|\mathcal{K}|+1}{n},$$

completing the proof of the first part of this theorem.

Next, we show that

$$C_S(R_1, 0) = C_{CR}(R_1, 0) - R_{min}(R_1, 0),$$

for $R_1 < H(X_1|X_2)$. Let

$$U^* = \arg\max_U I(U \wedge X_1),$$

where the maximum is over all the rvs U satisfying (5.2) – (5.3). Since by definition, $P_{U^*X_1X_2} \in \mathcal{S}(R_1)$ and

$$I(U^* \wedge X_1) = \max_{U: P_{UX_1X_2} \in \mathcal{S}(R_1)} I(U \wedge X_1),$$

it follows from (5.14) that

$$I(U^* \wedge X_1) = I(U^* \wedge X_2) + R_1.$$

Hence,

$$C_{CR}(R_1, 0) = I(U^* \wedge X_2) + R_1 \leq C_S(R_1, 0) + R_{min}(R_1, 0).$$

By symmetry, it is easily seen that

$$C_S(R_1, 0) \leq C_{CR}(R_1, 0) - R_{min}(R_1, 0).$$

■

For a given joint pmf $P_{X_1X_2}$, define

$$\mathcal{S}(R_1,R_2)=\left\{\begin{array}{ll} P_{UVX_1X_2}: & P_{UX_1X_2}=P_{U|X_1}P_{X_1X_2},\\ & P_{UVX_1X_2}=P_{V|UX_2}P_{UX_1X_2},\\ & \sum_{u,x_1,x_2}P_{UX_1X_2}\log\frac{P_{UX_1|X_2}}{P_{U|X_2}P_{X_1|X_2}}\le R_1,\\ & \sum_{u,v,x_1,x_2}P_{UVX_1X_2}\log\frac{P_{VX_2|UX_1}}{P_{V|UX_1}P_{X_2|UX_1}}\le R_2. \end{array}\right\} \tag{5.15}$$

Note that the CR-capacity for Model 5.2 is

$$C_{CR}(R_1,R_2)=\max_{(U,V):P_{UVX_1X_2}\in\mathcal{S}(R_1,R_2)} I(U,V\wedge X_1,X_2).$$

Proof of Theorem 5.2: To prove the first part of this theorem, it suffices to show that $R_{min}(R_1,R_2)\ge\min\{R_1,H(X_1|X_2)\}+\min\{R_2,H(X_2|X_1)\}$, for $R_1<H(X_1|X_2)$ or $R_2<H(X_2|X_1)$. We now discuss it for three cases.

Case 1: $R_1<H(X_1|X_2)$ and $R_2<H(X_2|X_1)$:

Let K (with values in $\mathcal{K}$) be arbitrary ε-CR with rate

$$\frac{1}{n}H(K)\ge C_{CR}(R_1,R_2)-\varepsilon,$$

achieved by transmissions $\mathbf{F}=(F_1,F_2)$, where $F_1=f_1(X_1^n)$ and $F_2=f_2(X_2^n,F_1)$.

Since K is ε-recoverable from $(X_2^n,\mathbf{F})$, there exists a rv K', as a function of $(X_2^n,\mathbf{F})$ and taking values in $\mathcal{K}$, such that $\Pr\{K'\ne K\}\le\varepsilon$. It follows from Fano's inequality that

$$\frac{1}{n}H(K')\ge C_{CR}(R_1,R_2)-\varepsilon-\frac{\varepsilon\log|\mathcal{K}|+1}{n}.$$

Let $\tilde{U}=F_1X_{1,1}\cdots X_{1,J-1}X_{2,J+1}\cdots X_{2,n}J$ and $\tilde{V}=K'$, where J is a rv independent of (X_1^n,X_2^n) and uniformly distributed on $\{1,\cdots,n\}$. It is easily seen that

$$\tilde{U} -\!\!\circ\!\!- X_{1,J} -\!\!\circ\!\!- X_{2,J}$$

and

$$\tilde{V} \mathrel{-\!\!\circ\!\!-} X_{2,J}, \tilde{U} \mathrel{-\!\!\circ\!\!-} X_{1,J}.$$

By applying Lemma 5.2 and the fact that $(X_{1,i}, X_{2,i})$ is independent of $(X_{1,1}, \cdots, X_{1,i-1}, X_{2,i+1}, \cdots, X_{2,n})$, we have

$$I(F_1 \wedge X_1^n) - I(F_1 \wedge X_2^n) = n\left[I(\tilde{U} \wedge X_{1,J}) - I(\tilde{U} \wedge X_{2,J})\right],$$

and

$$I(\tilde{V} \wedge X_1^n|F_1) - I(\tilde{V} \wedge X_2^n|F_1) = n\left[I(\tilde{V} \wedge X_{1,J}|\tilde{U}) - I(\tilde{V} \wedge X_{2,J}|\tilde{U})\right].$$

Thus,

$$I(\tilde{U} \wedge X_{1,J}) - I(\tilde{U} \wedge X_{2,J}) = \frac{1}{n}\left[I(F_1 \wedge X_1^n) - I(F_1 \wedge X_2^n)\right] \le \frac{1}{n}H(F_1) \le R_1. \tag{5.16}$$

Also,

$$\begin{aligned} I(\tilde{V} \wedge X_{2,J}|\tilde{U}) - I(\tilde{V} \wedge X_{1,J}|\tilde{U}) &= \frac{1}{n}\left[I(\tilde{V} \wedge X_2^n|F_1) - I(\tilde{V} \wedge X_1^n|F_1)\right] \\ &= \frac{1}{n}H(K'|X_1^n) \\ &= \frac{1}{n}\left[I(K' \wedge F_2|X_1^n) + H(K'|X_1^n, F_2)\right] \\ &\le \frac{1}{n}H(F_2|F_1) + \frac{2\varepsilon \log|\mathcal{K}| + 1}{n} \qquad (5.17) \\ &\le R_2 + \frac{2\varepsilon \log|\mathcal{K}| + 1}{n}. \end{aligned}$$

As $X_{1,J}$, $X_{2,J}$ can be identified with the rvs X_1, X_2 of the DMMS, the rvs $\tilde{U}$, $\tilde{V}$ satisfy (5.4) – (5.5). Note that

$$I(K' \wedge X_1^n) = \sum_{i=1}^{n} I(K' \wedge X_{1,i}|X_{1,1}, \cdots, X_{1,i-1}) \le nI(\tilde{U}, \tilde{V} \wedge X_{1,J}).$$

Hence,

$$\begin{aligned} I(\tilde{U}, \tilde{V} \wedge X_1, X_2) &= I(\tilde{U}, \tilde{V} \wedge X_1) + I(\tilde{V} \wedge X_2|\tilde{U}) - I(\tilde{V} \wedge X_1|\tilde{U}) \\ &\ge \frac{1}{n}I(K' \wedge X_1^n) + \frac{1}{n}H(K'|X_1^n) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{n} H(K') \\
&\geq C_{CR}(R_1, R_2) - \varepsilon - \frac{\varepsilon \log |\mathcal{K}| + 1}{n} \\
&= \max_{(U,V): P_{UVX_1X_2} \in \mathcal{S}(R_1,R_2)} I(U, V \wedge X_1, X_2) - \varepsilon - \frac{\varepsilon \log |\mathcal{K}| + 1}{n} \qquad (5.18)
\end{aligned}
$$

i.e., $I(\tilde{U}, \tilde{V} \wedge X_1, X_2)$ is arbitrarily close to the maximum of $I(U, V \wedge X_1, X_2)$ on $\mathcal{S}(R_1, R_2)$.

Note that for every $P_{UVX_1X_2} \in \mathcal{S}(R_1, R_2)$, we can write

$$
\begin{aligned}
I(U, V \wedge X_1, X_2) &= I(U \wedge X_1, X_2) + I(V \wedge X_1, X_2|U) \\
&= I(U \wedge X_1|X_2) + I(U \wedge X_2) + I(V \wedge X_2|X_1, U) + I(V \wedge X_1|U),
\end{aligned}
$$

where $I(U \wedge X_1|X_2)$ can be chosen to equal R_1, provided $R_1 < H(X_1|X_2)$, and $I(V \wedge X_2|X_1, U)$ can be chosen to equal R_2, provided $R_2 < H(X_2|X_1)$. Hence,

$$
\max_{(U,V): P_{UVX_1X_2} \in \mathcal{S}(R_1,R_2)} I(U, V \wedge X_1, X_2) = R_1 + R_2 + \max_{(U,V): P_{UVX_1X_2} \in \mathcal{S}(R_1,R_2)} [I(U \wedge X_2) + I(V \wedge X_1|U)]
$$

is achieved with

$$
I(U \wedge X_1|X_2) = R_1, \tag{5.19}
$$

and

$$
I(V \wedge X_2|X_1, U) = R_2. \tag{5.20}
$$

Furthermore, by Lemma 5.1, $I(U, V \wedge X_1, X_2)$ is a convex function of $P_{UV|X_1X_2}$ for fixed $P_{X_1X_2}$, where the convexity is not strict iff (U, V) is independent of (X_1, X_2), which corresponds to the minimum of $I(U, V \wedge X_1, X_2)$. Considering that $I(U, V \wedge X_1, X_2)$ is a continuous function of $P_{UVX_1X_2}$, with the rvs $\tilde{U}$, $\tilde{V}$ defined above satisfying (5.18), we have for every $\delta_1 > 0$ and $\delta_2 > 0$,

$$
I(\tilde{U} \wedge X_1) - I(\tilde{U} \wedge X_2) = I(\tilde{U} \wedge X_1|X_2) \geq R_1 - \delta_1,
$$

and

$$
I(\tilde{V} \wedge X_2|\tilde{U}) - I(\tilde{V} \wedge X_1|\tilde{U}) = I(\tilde{V} \wedge X_2|X_1, \tilde{U}) \geq R_2 - \delta_2.
$$

It readily follows from (5.16) and (5.17) that

$$\frac{1}{n}H(F_1) \geq R_1 - \delta_1,$$

and

$$\frac{1}{n}H(F_2|F_1) \geq R_2 - \delta_2 - \frac{2\varepsilon \log|\mathcal{K}| + 1}{n}.$$

Therefore,

$$\frac{1}{n}\log||\mathbf{F}|| \geq \frac{1}{n}H(F_1) + \frac{1}{n}H(F_2|F_1) \geq R_1 + R_2 - \delta_1 - \delta_2 - \frac{2\varepsilon \log|\mathcal{K}| + 1}{n}.$$

Case 2: $R_1 < H(X_1|X_2)$ and $R_2 \geq H(X_2|X_1)$:

Let K be arbitrary ε-CR with rate

$$\frac{1}{n}H(K) \geq C_{CR}(R_1, R_2) - \varepsilon = R_1 + H(X_2) - \varepsilon,$$

achieved by transmissions $\mathbf{F} = (F_1, F_2)$. Then,

$$\begin{aligned}
\frac{1}{n}H(F_1) &\geq \frac{1}{n}H(X_2^n, F_1) - \frac{1}{n}H(X_2^n) \\
&\geq \frac{1}{n}H(K) - \frac{\varepsilon \log|\mathcal{K}| + 1}{n} - H(X_2) \\
&\geq R_1 - \varepsilon - \frac{\varepsilon \log|\mathcal{K}| + 1}{n}.
\end{aligned}$$

Also,

$$\begin{aligned}
\frac{1}{n}H(F_2|F_1) &\geq \frac{1}{n}I(F_2 \wedge X_2^n|X_1^n) \\
&= \frac{1}{n}[H(X_2^n|X_1^n) - H(X_2^n|X_1^n, F_2)] \\
&\geq H(X_2|X_1) - \frac{\varepsilon \log|\mathcal{X}_2| + 1}{n},
\end{aligned}$$

where the last inequality follows since in this case, X_2^n is ε-recoverable from (X_1^n, F_2). Therefore,

$$\frac{1}{n}\log||\mathbf{F}|| \geq R_1 + H(X_2|X_1) - \varepsilon - \frac{\varepsilon \log|\mathcal{K}| + \varepsilon \log|\mathcal{X}_2| + 2}{n}.$$

Case 3: $R_1 \geq H(X_1|X_2)$ and $R_2 < H(X_2|X_1)$:

The same arguments used for Case 2 apply here.

Next, we show that if $R_1 < H(X_1|X_2)$ and $R_2 < H(X_2|X_1)$,

$$C_S(R_1, R_2) = C_{CR}(R_1, R_2) - R_{min}(R_1, R_2).$$

Let

$$(U^*, V^*) = \arg\max_{U,V} I(U, V \wedge X_1, X_2),$$

where the maximum is for all the pairs of rvs (U, V) satisfying (5.4) – (5.5). Since by definition, $P_{U^*V^*X_1X_2} \in \mathcal{S}(R_1, R_2)$ and

$$I(U^*, V^* \wedge X_1, X_2) = \max_{(U,V): P_{UVX_1X_2} \in \mathcal{S}(R_1,R_2)} I(U, V \wedge X_1, X_2),$$

it follows from (5.19) and (5.20) that

$$I(U^* \wedge X_1) = I(U^* \wedge X_2) + R_1,$$

and

$$I(V^* \wedge X_2|U^*) = I(V^* \wedge X_1|U^*) + R_2.$$

Hence,

$$C_{CR}(R_1, R_2) = I(U^* \wedge X_2) + I(V^* \wedge X_1|U^*) + R_1 + R_2 \leq C_S(R_1, R_2) + R_{min}(R_1, R_2).$$

The counterpart follows by symmetry. ■

Proof of Theorems 5.3 and 5.4:

Converse part of Theorem 5.3: For every $\varepsilon > 0$, let K (with values in $\mathcal{K}$) be an arbitrary ε-CR, achieved by transmissions $\mathbf{F} = (\mathbf{F}_1, \mathbf{F}_2) = (F_1, F_2, \cdots, F_{2r-1}, F_{2r})$ satisfying (5.1). Since K is ε-recoverable from $(X_2^n, \mathbf{F})$, there exists a rv K', as a function of $(X_2^n, \mathbf{F})$

and taking values in $\mathcal{K}$, such that $\Pr\{K' \neq K\} \leq \varepsilon$. Let

$$\tilde{U}_i = \begin{cases} F_1 X_{1,1} \cdots X_{1,J-1} X_{2,J+1} \cdots X_{2,n} J, & i = 1, \\ F_{2i-1}, & 2 \leq i \leq r, \end{cases} \tag{5.21}$$

and

$$\tilde{V}_i = \begin{cases} F_{2i}, & 1 \leq i \leq r-1, \\ K', & i = r. \end{cases} \tag{5.22}$$

It is shown in Appendix C.1 that $\{(\tilde{U}_i, \tilde{V}_i),\ 1 \leq i \leq r\}$ satisfy the Markov conditions (5.6) – (5.7). By applying Lemma 5.2, we have

$$I(\tilde{U}_1 \wedge X_{1,J}) - I(\tilde{U}_1 \wedge X_{2,J}) = \frac{1}{n}[I(F_1 \wedge X_1^n) - I(F_1 \wedge X_2^n)] \leq \frac{1}{n} H(F_1),$$

and for $2 \leq i \leq r$,

$$\begin{aligned} & I(\tilde{U}_i \wedge X_{1,J} | \tilde{U}_1, \cdots, \tilde{U}_{i-1}, \tilde{V}_1, \cdots, \tilde{V}_{i-1}) - I(\tilde{U}_i \wedge X_{2,J} | X_{2,J}, \tilde{U}_1, \cdots, \tilde{U}_{i-1}, \tilde{V}_1, \cdots, \tilde{V}_{i-1}) \\ = \ & \frac{1}{n}[I(F_{2i-1} \wedge X_1^n | F_{[1,2i-2]}) - I(F_{2i-1} \wedge X_2^n | F_{[1,2i-2]})] \\ \leq \ & \frac{1}{n} H(F_{2i-1} | F_1, F_3, \cdots, F_{2i-3}). \end{aligned}$$

As $X_{1,J}$, $X_{2,J}$ can be identified with the rvs X_1, X_2,

$$R_1 \geq \frac{1}{n} H(\mathbf{F}_1) \geq \sum_{i=1}^{r} I(\tilde{U}_i \wedge X_1 | X_2, \tilde{U}_1, \cdots, \tilde{U}_{i-1}, \tilde{V}_1, \cdots, \tilde{V}_{i-1}). \tag{5.23}$$

Also, it can be shown that

$$\begin{aligned} H(\tilde{V}_1, \cdots, \tilde{V}_r | X_1^n) &= \sum_{i=1}^{r} H(\tilde{V}_i | X_1^n, \tilde{U}_1, \cdots, \tilde{U}_i, \tilde{V}_1, \cdots, \tilde{V}_{i-1}) \\ &= n \sum_{i=1}^{r} I(\tilde{V}_i \wedge X_2 | X_1, \tilde{U}_1, \cdots, \tilde{U}_i, \tilde{V}_1, \cdots, \tilde{V}_{i-1}). \end{aligned} \tag{5.24}$$

Hence,

$$\begin{aligned} R_2 &\geq \frac{1}{n} H(\mathbf{F}_2 | \mathbf{F}_1) \geq \frac{1}{n} H(\mathbf{F}_2 | X_1^n) \\ &\geq \frac{1}{n} H(\tilde{V}_1, \cdots, \tilde{V}_r | X_1^n) - \frac{1}{n} H(K' | X_1^n, \mathbf{F}_2) \\ &\geq \sum_{i=1}^{r} I(\tilde{V}_i \wedge X_2 | X_1, \tilde{U}_1, \cdots, \tilde{U}_i, \tilde{V}_1, \cdots, \tilde{V}_{i-1}) - \frac{2\varepsilon \log |\mathcal{K}| + 1}{n}. \end{aligned} \tag{5.25}$$

Therefore, $\{(\tilde{U}_i, \tilde{V}_i),\ 1 \leq i \leq r\}$ satisfy the rate conditions (5.8) – (5.9).

It follows from (5.24) and

$$\begin{aligned} I(\tilde{V}_1, \cdots, \tilde{V}_r \wedge X_1^n) &= nI(\tilde{V}_1, \cdots, \tilde{V}_r, X_{1,1}, \cdots, X_{1,J-1} \wedge X_{1,J}) \\ &\leq n\sum_{i=1}^{r} I(\tilde{U}_i, \tilde{V}_i \wedge X_1 | \tilde{U}_1, \cdots, \tilde{U}_{i-1}, \tilde{V}_1, \cdots, \tilde{V}_{i-1}), \end{aligned}$$

that

$$\begin{aligned} \frac{1}{n}H(K) &\leq \frac{1}{n}H(K') + \frac{\varepsilon \log|\mathcal{K}| + 1}{n} \\ &\leq \frac{1}{n}H(\tilde{V}_1, \cdots, \tilde{V}_r) + \frac{\varepsilon \log|\mathcal{K}| + 1}{n} \\ &\leq I(\tilde{U}_1, \cdots, \tilde{U}_r, \tilde{V}_1, \cdots, \tilde{V}_r \wedge X_1, X_2) + \frac{\varepsilon \log|\mathcal{K}| + 1}{n}. \end{aligned}$$

Converse part of Theorem 5.4: For every $\varepsilon > 0$, let K (with values in $\mathcal{K}$) be an arbitrary ε-SK, achieved by transmissions $\mathbf{F} = (\mathbf{F}_1, \mathbf{F}_2)$ satisfying (5.1). Let $L = (K, \mathbf{F})$. Clearly, L represents an ε-CR. Hence,

$$\frac{1}{n}H(L) \leq I(\tilde{U}_1, \cdots, \tilde{U}_r, \tilde{V}_1, \cdots, \tilde{V}_r \wedge X_1, X_2), \tag{5.26}$$

where the rvs $\{(\tilde{U}_i, \tilde{V}_i),\ 1 \leq i \leq r\}$ are given by (5.21) – (5.22) (with K' replaced by a suitable $L' = L'(X_2^n, \mathbf{F})$). Since K is an ε-SK,

$$H(L) \geq H(K, \mathbf{F}) = H(K) + H(\mathbf{F}) - I(K \wedge \mathbf{F}) \geq H(K) + H(\mathbf{F}) - n\varepsilon.$$

Therefore, it follows from (5.23), (5.25) and (5.26) that

$$\begin{aligned} \frac{1}{n}H(K) &\leq \frac{1}{n}H(L) - H(\mathbf{F}) + \varepsilon \\ &\leq \sum_{i=1}^{r}[I(\tilde{U}_i \wedge X_2 | \tilde{U}_1, \cdots, \tilde{U}_{i-1}, \tilde{V}_1, \cdots, \tilde{V}_{i-1}) \\ &\quad + I(\tilde{V}_i \wedge X_1 | \tilde{U}_1, \cdots, \tilde{U}_i, \tilde{V}_1, \cdots, \tilde{V}_{i-1})] + \varepsilon + \frac{2\varepsilon \log|\mathcal{K}| + 1}{n}. \end{aligned}$$

Achievability Parts of Theorems 5.3 and 5.4: The proof is analogous to that of [4, Theorem 4.4], with a direct extension from one round of transmissions to r rounds of transmissions. The details of the proof are omitted here, but the idea behind the proof is given in Appendix C.2. ■

Proof of Theorem 5.5:

The proof is analogous to that of Theorem 5.2, with the setting of $\{(\tilde{U}_i, \tilde{V}_i),\ 1 \leq i \leq r\}$ as in (5.21) – (5.22). ■

Chapter 6

Conclusions and Future Research

6.1 Conclusions

In this dissertation, we discussed the problems of

(i). the simultaneous generation of multiple keys by different groups of terminals;

(ii). the constructions of SKs and PKs by multiple terminals; and

(iii). the examination of the relationship between the CR-capacity and the SK-capacity for source models with rate constraints on the public communication.

In part (i), we considered three-terminal source models. We determined in Chapter 2 the inner and outer bounds for the PK-capacity region. Under certain special conditions, these bounds coincide to yield the exact PK-capacity region. We determined in Chapter 3 the inner and outer bounds for the (SK, PK)-capacity region. Under a certain condition, these bounds coincide to yield the exact (SK, PK)-capacity region.

In part (ii), we considered several simple secrecy generation models involving multiple terminals, and proposed a new approach for constructing SKs and PKs. This approach is based on Wyner's well-known SW data compression scheme for sources connected by virtual channels with additive independent noise. It has been shown that the generated SKs and PKs satisfy the desired common randomness, secrecy and uniformity conditions.

In part (iii), we considered several two-terminal source models with rate constraints on the public communication between these terminals. It has been shown that for each of these models, the CR-capacity is equal to the sum of the SK-capacity and the smallest achievable CLCR sum-rate.

6.2 Future Research

There are many opportunities to expand beyond the research presented here.

For part (i), it would be of interest to seek the exact PK-capacity region and the exact (SK, PK)-capacity region. A potential approach is to characterize the PK-capacity region and the (SK, PK)-capacity region in terms of suitable decompositions of the overall CR, *a la* the SK-capacity and the PK-capacity when a single key is generated [17]. It is known in the case of a single key that the SK-capacity is obtained by subtracting from the maximum rate of shared CR achievable by these terminals the smallest sum-rate of the data-compressed interterminal communication which enables each of the terminals to acquire this maximal CR. For counterpart problem involving the PK-capacity region, it is open whether the largest sum of two individual PK rates is obtained by subtracting from the maximum rate of shared CR the smallest sum-rate of the data-compressed interterminal communication which enables each of the terminals to acquire the randomness *used for the PK generation at that terminal.* It is also open whether a similar decomposition holds for the (SK,PK)-capacity region.

Furthermore, an obvious generalization of the three-terminal source models considered in Chapters 2 and 3 is the one in which a SK is generated by all three terminals, and – simultaneously – all three pairs of terminals generate distinct PKs, each of which is effectively concealed from the remaining terminal. Entropy rates of these simultaneously generated SK and PKs constitute a (SK, 3-PK)-rate quadruple. The set of all achievable (SK, 3-PK)-rate quadruples is called (SK, 3-PK)-capacity region. Following arguments similar to those used in the proof of Theorem 3.1, we can easily obtain an outer bound for this (SK, 3-PK)-capacity region. Achievability proofs leading to inner bounds for this (SK, 3-PK)-capacity region are still open.

For part (ii), in all of the multiterminal source models considered in Chapter 4, the i.i.d. sequences observed at different terminals are related to each other through virtual communication channels characterized by additive independent noises. Consider the model in which terminals $\mathcal{X}_1$ and $\mathcal{X}_2$, which respectively observe i.i.d. repetitions of the correlated $\{0,1\}$-valued rvs. X_1 and X_2 with joint pmf $P_{X_1X_2}$, wish to generate a SK of maximal rate. The observations at terminal $\mathcal{X}_2$ can be considered as inputs to a virtual binary symmetric channel (BSC), while the observations at terminal $\mathcal{X}_1$ are the corresponding outputs. Thus, this channel has the transition probability matrix $P_{X_1|X_2}$.

There are two steps in the SK construction schemes in Chapter 4. The first step constitutes SW data compression for the purpose of CR generation at the terminals. Although the existence of linear data compression codes with rate arbitrarily close to the SW bound has been long known for *arbitrarily correlated sources* [12], constructions of such linear data compression codes are understood in terms of the cosets of linear error-correction codes for the virtual channel $P_{X_1|X_2}$ only when this virtual channel is characterized by (independent) additive noise [63]. For instance, when the two sources are connected by a BSC from $\mathcal{X}_2$ to $\mathcal{X}_1$, a linear data compression code, which attains the SW rate $H(X_1|X_2)$ for terminal $\mathcal{X}_2$ to reconstruct the observations at $\mathcal{X}_1$, is then provided by a linear channel code which achieves the capacity of the BSC $P_{X_1|X_2}$.

However, if the i.i.d. sequences observed at terminals $\mathcal{X}_1$ and $\mathcal{X}_2$ are *arbitrarily correlated*, the virtual communication channel $P_{X_1|X_2}$ involved in the data compression problem is no longer symmetric. It is shown in [21] that linear codes could not achieve the capacity of a nonsymmetric channel in general. Therefore, it is not clear if the linear data compression codes that achieve the SW bound can be provided by the linear capacity-achieving channel codes anymore.

The second step in the SK construction schemes involves SK extraction from the previously acquired CR. Recent work [45] shows that for the special case of two-terminal source model, this extraction can be accomplished by means of a linear transformation. However, it is still unknown whether such a result holds for a general source model with more than two terminals.

Next, as mentioned in Section 4.3, for the situation in which the marginal pmfs at the two terminals differ from the uniform, the extraction of a SK or a PK from the previously acquired CR involves regular subsets. Loosely speaking, a SK or a PK is set as the index of a sequence in a regular subset containing that sequence. Since by definition, each regular subset consists of sequences of the same type or the same joint type with regard to a given sequence, the generation of regular subsets is based on the procedure of collecting a large number of sequences of the same type or of the same joint type relative to a given sequence. However, the current complexity of such a collection poses a hurdle in the generation of regular subsets, and subsequently, the explicit implementation of SK or PK extraction.

Furthermore, the simultaneous construction of multiple keys by different groups of terminals is an interesting new topic, which is completely unexplored.

For part (iii), the examination of the relationship between the SK-capacity and the CR-capacity for a given source model, with more than two terminals and with rate constraints on the public communication between the terminals, is an interesting challenge for future research. The first step of the overall effort is to characterize the CR-capacity for such a model.

Appendix A

Types and Typical Sequences

The following standard results on types and typical sequences can be found, for instance, in [15], [11].

A.1 Types

The *type* of a sequence $x^n \in \mathcal{X}^n$, $\mathcal{X}$ a finite set, is the probability mass function (pmf) P_{x^n} on $\mathcal{X}$ given by

$$P_{x^n}(a) = \frac{1}{n}|\{i : x_i = a\}|, \quad a \in \mathcal{X}.$$

The *joint type* of a pair of sequences $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$ is the joint pmf $P_{x^n y^n}$ on $\mathcal{X} \times \mathcal{Y}$ given by

$$P_{x^n y^n}(a, b) = \frac{1}{n}|\{i : x_i = a, y_i = b\}|, \quad a \in \mathcal{X},\ b \in \mathcal{Y}.$$

The number of different types of sequences in $\mathcal{X}^n$ does not exceed $(n+1)^{|\mathcal{X}|}$, and the number of different joint types of pairs of sequences in $\mathcal{X}^n \times \mathcal{Y}^n$ is less than $(n+1)^{|\mathcal{X}||\mathcal{Y}|}$.

A.2 Typical Sequences

Given generic rvs X, Y (taking values in the finite sets $\mathcal{X}$, $\mathcal{Y}$), with joint pmf P_{XY} on $\mathcal{X} \times \mathcal{Y}$, the set of sequences in $\mathcal{X}^n$ which are X*-typical with constant* ξ, denoted by $T^n_{X,\xi}$, is defined as

$$T^n_{X,\xi} \overset{\triangle}{=} \left\{ x^n \in \mathcal{X}^n : 2^{-n[H(X)+\xi]} \leq P^n_X(x^n) \leq 2^{-n[H(X)-\xi]} \right\},$$

where $P_X^n(x^n) \triangleq \Pr\{X^n = x^n\}$, $x^n \in \mathcal{X}^n$; and the set of pairs of sequences in $\mathcal{X}^n \times \mathcal{Y}^n$ which are *XY-typical with constant* ξ, denoted by $T^n_{XY,\xi}$, is defined as

$$T^n_{XY,\xi} \triangleq \left\{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : x^n \in T^n_{X,\xi},\ y^n \in T^n_{Y,\xi},\ 2^{-n[H(X,Y)+\xi]} \le P^n_{XY}(x^n, y^n) \le 2^{-n[H(X,Y)-\xi]}\right\},$$

where $P^n_{XY}(x^n, y^n) \triangleq \Pr\{X^n = x^n, Y^n = y^n\}$, $x^n \in \mathcal{X}^n$, $y^n \in \mathcal{Y}^n$.

It readily follows that for every $(x^n, y^n) \in T^n_{XY,\xi}$,

$$2^{-n[H(X|Y)+2\xi]} \le P^n_{X|Y}(x^n|y^n) \le 2^{-n[H(X|Y)-2\xi]},$$

where $P^n_{X|Y}(x^n|y^n) \triangleq \Pr\{X^n = x^n|Y^n = y^n\}$, $x^n \in \mathcal{X}^n$, $y^n \in \mathcal{Y}^n$.

For every $y^n \in \mathcal{Y}^n$, the set of sequences in $\mathcal{X}^n$ which are *$X|Y$-typical with respect to y^n with constant* ξ, denoted by $T^n_{X|Y,\xi}(y^n)$, is defined as

$$T^n_{X|Y,\xi}(y^n) \triangleq \left\{x^n \in \mathcal{X}^n : (x^n, y^n) \in T^n_{XY,\xi}\right\};$$

note that $T^n_{X|Y,\xi}(y^n)$ is an empty set if $y^n \notin T^n_{Y,\xi}$.

For every $y^n \in T^n_{Y,\xi}$,

$$\left|T^n_{X|Y,\xi}(y^n)\right| \le 2^{n[H(X|Y)+2\xi]}. \tag{A.1}$$

Proposition A.1 *Given a joint pmf P_{XY} on $\mathcal{X} \times \mathcal{Y}$ with $P_{XY}(x, y) > 0$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$, for each $\xi > 0$,*

$$\sum_{x^n \in T^n_{X,\xi}} P^n_X(x^n) \ge 1 - (n+1)^{|\mathcal{X}|} \cdot 2^{-n \frac{\xi^2}{2\ln 2\left[\sum_{a\in\mathcal{X}} \log \frac{1}{P_X(a)}\right]^2}}, \tag{A.2}$$

and

$$\sum_{(x^n, y^n) \in T^n_{XY,\xi}} P^n_{XY}(x^n, y^n) \ge 1 - (n+1)^{|\mathcal{X}||\mathcal{Y}|} \cdot 2^{-n \frac{\xi^2}{2\ln 2\left[\sum_{(a,b)\in\mathcal{X}\times\mathcal{Y}} \log \frac{1}{P_{XY}(a,b)}\right]^2}}, \tag{A.3}$$

for all $n \ge 1$.

Proof of Proposition A.1: We shall prove (A.2) here. The proof of (A.3), which is similar, is omitted. Fix $\delta > 0$ and consider the set $T^n_{[P_X]_\delta}$ of sequences in $\mathcal{X}^n$ which are P_X*-typical with constant* δ (cf. [15, p. 33]), i.e.,

$$T^n_{[P_X]_\delta} = \{x^n \in \mathcal{X}^n : \max_{a\in\mathcal{X}} |P_{x^n}(a) - P_X(a)| \leq \delta\}.$$

Since $T^n_{[P]_\delta}$ is the union of the sets of these types $\tilde{P}$ of sequences in $\mathcal{X}^n$ which satisfy

$$\max_{a\in\mathcal{X}} |\tilde{P}(a) - P_X(a)| \leq \delta, \tag{A.4}$$

we have

$$\begin{aligned} \sum_{x^n \in \left(T^n_{[P_X]_\delta}\right)^c} P^n_X(x^n) &= \sum_{\tilde{P}:\max_{a\in\mathcal{X}} |\tilde{P}(a)-P_X(a)|>\delta} P^n_X\left(\{x^n : P_{x^n} = \tilde{P}\}\right) \\ &\leq (n+1)^{|\mathcal{X}|} \cdot 2^{-n \min_{\tilde{P}:\min_{a\in\mathcal{X}} |\tilde{P}(a)-P_X(a)|>\delta} D(\tilde{P}||P_X)}, \end{aligned} \tag{A.5}$$

using the fact that $P^n_X(\{x^n : P_{x^n} = \tilde{P}\}) \leq 2^{-nD(\tilde{P}||P)}$ (cf. [15, Lemma 2.6]).

Next, by Pinsker's inequality (cf. e.g., [15, p. 58]),

$$\begin{aligned} D(\tilde{P}||P) &\geq \frac{1}{2ln2}\left(\min_{a\in\mathcal{X}} |\tilde{P}(a) - P_X(a)|\right)^2 \\ &\geq \frac{\delta^2}{2ln2}, \end{aligned} \tag{A.6}$$

with the previous inequality holding for every $\tilde{P}$ in (A.4). It follows from (A.5) and (A.6) that

$$\sum_{x^n \in T^n_{[P]_\delta}} P^n_X(x^n) \geq 1 - (n+1)^{|\mathcal{X}|} \cdot 2^{-n\frac{\delta^2}{2ln2}} \tag{A.7}$$

for all $n \geq 1$.

Finally, observe that

$$T^n_{[P_X]_\delta} \subseteq T^n_{X,\xi}, \quad \text{if} \quad \xi = \delta\left[\sum_{a\in\mathcal{X}} \log\frac{1}{P_X(a)}\right], \tag{A.8}$$

which is readily seen from the fact that for each $x^n \in \mathcal{X}^n$,

$$\begin{aligned}
-\frac{1}{n}\log P_X^n(x^n) - H(P_X) &= -\frac{1}{n}\log\left(2^{-n[H(P_{x^n})+D(P_{x^n}||P_X)]}\right) - H(P_X)\\
&= H(P_{x^n}) + D(P_{x^n}||P_X) - H(P_X)\\
&= H(P_{x^n}) - H(P_{x^n}) + \sum_{a\in\mathcal{X}} P_{x^n}(a)\log\frac{1}{P_X(a)} - H(P_X)\\
&= \sum_{a\in\mathcal{X}} [P_{x^n}(a) - P_X(a)]\log\frac{1}{P_X(a)}.
\end{aligned}$$

Clearly, (A.7) and (A.8) imply (A.2). ■

Appendix B

Proof of Proposition 4.1

The proof of Proposition 4.1 relies on the lemma below concerning the average error probability of maximum likelihood decoding.

A sequence $u^n \in \{0,1\}^n$ is called a *descendent* of a sequence $v^n \in \{0,1\}^n$ if $u_i = 1$ implies that $v_i = 1$, $1 \leq i \leq n$. A subset $\Omega \subset \{0,1\}^n$ is called *quasiadmissible* if the conditions that $u^n \in \Omega$ and u^n is a descendent of v^n together imply that $v^n \in \Omega$.

Lemma B.1 [35] *If Ω is a quasiadmissible subset of $\{0,1\}^n$, then for $0 \leq p \leq 1$,*

$$\frac{d\mu_p(\Omega)}{dp} > 0,$$

where

$$\mu_p(\Omega) = \sum_{x^n \in \Omega} p^{wt(x^n)}(1-p)^{n-wt(x^n)},$$

with $wt(x^n)$ denoting the weight of x^n. ■

For a binary linear code, let $\mathbf{E}$ denote the set of coset leaders. It is known (cf. [49, Theorem 3.11]) that $\omega = \{0,1\}^n \backslash \mathbf{E}$ is a quasiadmissible subset of $\{0,1\}^n$. If a binary linear code is used on BSC(p), the average error probability of maximum likelihood decoding is given by (cf. [54, Theorem 5.3.3])

$$\mu_p(\omega) = \sum_{x^n \in \omega} p^{wt(x^n)}(1-p)^{n-wt(x^n)}.$$

It follows from Lemma B.1 that this average error probability increases with the crossover probability p. In other words, if the same binary linear code is used on two binary symmetric channels with different crossover probabilities, say, $0 < p_1 < p_2 < \frac{1}{2}$, then the average error probability of maximum likelihood decoding for a BSC(p_1) is strictly less than that for a BSC(p_2). This can also be interpreted since a BSC(p_2) is equivalent to a cascade of a BSC(p_1) and a BSC($\frac{p_2-p_1}{1-2p_1}$).

We now return to the proof of Proposition 4.1. It follows from Lemma 4.1 that for some $\eta > 0$ and for all sufficiently large n,

$$\Pr\{\hat{X}^n_{j^*}(i^*) \neq X^n_{i^*}\} < 2^{-n\eta}.$$

Recall that $p_{(i^*,j^*)} = \max_{(i,j)\in E(\mathcal{T})} p_{(i,j)}$ and $(i = i_0, i_1, \cdots, i_r = i^*)$ is the path from i to i^*. It is readily seen from Lemma B.1 that

$$\Pr\{\hat{X}^n_i(i_1) \neq X^n_{i_1}\} < \Pr\{\hat{X}^n_{j^*}(i^*) \neq X^n_{i^*}\} < 2^{-n\eta}.$$

Subsequently,

$$\begin{aligned}\Pr\{\hat{X}^n_i(i_2) \neq X^n_{i_2}\} &\leq \Pr\{\hat{X}^n_i(i_2) \neq X^n_{i_2}, \hat{X}^n_i(i_1) \neq X^n_{i_1}\}\\ &\quad + \Pr\{\hat{X}^n_i(i_2) \neq X^n_{i_2}, \hat{X}^n_i(i_1) = X^n_{i_1}\}\\ &< 2\cdot 2^{-n\eta}.\end{aligned}$$

Continue this procedure, and finally we have

$$\Pr\{\hat{X}^n_i(i^*) \neq X^n_{i^*}\} < r\cdot 2^{-n\eta} < m\cdot 2^{-n\eta}.$$

■

Appendix C

Supplemental Proofs for Theorems 5.3 and 5.4

For notational simplicity, we shall use $A_{[i,j]}$ to denote $(A_i, \cdots, A_j)$ in this appendix.

C.1 Proof of the Markov Conditions

We shall show that $\{(\tilde{U}_i, \tilde{V}_i),\ 1 \leq i \leq r\}$ defined in (5.21) and (5.22) satisfy the Markov conditions in (5.6) and (5.7).

It is easily seen that

$$\tilde{U}_1 -\!\!\!\circ\!\!\!- X_{1,J} -\!\!\!\circ\!\!\!- X_{2,J}.$$

To show that for $2 \leq i \leq r$, $\tilde{U}_{[1,r]}$ and $\tilde{V}_{[1,r]}$ satisfy (5.6), it suffices to show that

$$X_{1,[J+1,n]} -\!\!\!\circ\!\!\!- X_{1,[1,J]}, X_{2,[J+1,n]}, F_{[1,2i-2]}, J -\!\!\!\circ\!\!\!- X_{2,J}, \tag{C.1}$$

which implies that

$$F_{2i-1} -\!\!\!\circ\!\!\!- X_{1,[1,J]}, X_{2,[J+1,n]}, F_{[1,2i-2]}, J -\!\!\!\circ\!\!\!- X_{2,J}.$$

In order to establish (C.1), it suffices to show that

$$P_{X_{2,J}|X_{1,[1,n]},X_{2,[J+1,n]},F_{[1,2i-2]},J} = P_{X_{2,J}|X_{1,[1,J]},X_{2,[J+1,n]},F_{[1,2i-2]},J}. \tag{C.2}$$

Recalling that F_{2i-1} is a function of $(X_1^n, F_{[1,2i-2]})$, the left hand side of (C.2) can be written as

$$P_{X_{2,J}|X_{1,J},J} \prod_{l=1}^{i-1} \frac{P_{F_{2l}|X_{1,[1,n]},X_{2,[J,n]},F_{[1,2l-1]},J}}{P_{F_{2l}|X_{1,[1,n]},X_{2,[J+1,n]},F_{[1,2l-1]},J}},$$

or equivalently,

$$P_{X_{2,J}|X_{1,J},J} \prod_{l=1}^{i-1} \frac{P_{F_{2l}|X_{1,[1,J-1]},X_{2,[J,n]},F_{[1,2l-1]},J}}{P_{F_{2l}|X_{1,[1,J]},X_{2,[J+1,n]},F_{[1,2l-1]},J}}, \tag{C.3}$$

since F_{2l} is a function of $(X_2^n, F_{[1,2l-1]})$. It is clear that the right hand side of (C.2) can also be written as (C.3), proving (5.6).

Following the similar arguments used to show (C.1), we have for $1 \leq i \leq r-1$,

$$X_{2,[1,J-1]} \mathrel{-\!\!\circ\!\!-} X_{1,[1,J-1]}, X_{2,[J,n]}, F_{[1,2i-1]}, J \mathrel{-\!\!\circ\!\!-} X_{1,J},$$

which implies that

$$F_{2i} \mathrel{-\!\!\circ\!\!-} X_{1,[1,J-1]}, X_{2,[J,n]}, F_{[1,2i-1]}, J \mathrel{-\!\!\circ\!\!-} X_{1,J}.$$

Further, it is easily seen that

$$\tilde{V}_r \mathrel{-\!\!\circ\!\!-} X_{2,J}, \tilde{U}_{[1,r]}, \tilde{V}_{[1,r-1]} \mathrel{-\!\!\circ\!\!-} X_{1,J}.$$

Hence, (5.7) is proved.

C.2 Idea of the Achievability Proofs

Given a DMMS with two components corresponding to generic rvs X_1, X_2, and auxiliary rvs $U_{[1,r]}, V_{[1,r]}$ satisfying (5.6) – (5.9), for every $\delta > 0$ and $1 \leq i \leq r$, set

$$\begin{aligned}
N_{1,i} &= 2^{n[I(U_i \wedge X_1 | X_2, U_{[1,i-1]}, V_{[1,i-1]}) + 2\delta]}, \\
N_{2,i} &= 2^{n[I(V_i \wedge X_2 | X_1, U_{[1,i]}, V_{[1,i-1]}) + 2\delta]}, \\
M_{1,i} &= 2^{n[I(U_i \wedge X_2 | U_{[1,i-1]}, V_{[1,i-1]}) - \delta]}, \\
M_{2,i} &= 2^{n[I(V_i \wedge X_1 | U_{[1,i]}, V_{[1,i-1]}) - \delta]}.
\end{aligned}$$

In the i^{th} round, $1 \leq i \leq r$, sequences ${u_i^n}_{j_i,k_i}$, $1 \leq j_i \leq N_{1,i}$, $1 \leq k_i \leq M_{1,i}$, which are *jointly typical* (cf. [11], [15]) with

$$({u_1^n}_{j_1,k_1}, \cdots, {u_{i-1}^n}_{j_{i-1},k_{i-1}}, {v_1^n}_{p_1,q_1}, \cdots, {v_{i-1}^n}_{p_{i-1},q_{i-1}})$$

are selected at random. Then, with probability close to 1, there exists a ${u^n_i}_{j_i,k_i}$ jointly typical with

$$(x^n_1, {u^n_1}_{j_1,k_1}, \cdots, {u^n_{i-1}}_{j_{i-1},k_{i-1}}, {v^n_1}_{p_1,q_1}, \cdots, {v^n_{i-1}}_{p_{i-1},q_{i-1}}),$$

such that if terminal $\mathcal{X}_1$ transmits the index j_i to terminal $\mathcal{X}_2$, the latter can reconstruct k_i by the joint typicality of ${u^n_i}_{j_i,k_i}$ with

$$(x^n_2, {u^n_1}_{j_1,k_1}, \cdots, {u^n_{i-1}}_{j_{i-1},k_{i-1}}, {v^n_1}_{p_1,q_1}, \cdots, {v^n_{i-1}}_{p_{i-1},q_{i-1}}).$$

Next, sequences ${v^n_i}_{p_i,q_i}$, $1 \leq p_i \leq N_{2,i}$, $1 \leq q_i \leq M_{2,i}$, which are jointly typical with

$$({u^n_1}_{j_1,k_1}, \cdots, {u^n_i}_{j_i,k_i}, {v^n_1}_{p_1,q_1}, \cdots, {v^n_{i-1}}_{p_{i-1},q_{i-1}})$$

are selected at random. Then, with probability close to 1, there exists a ${v^n_i}_{p_i,q_i}$ jointly typical with

$$(x^n_2, {u^n_1}_{j_1,k_1}, \cdots, {u^n_i}_{j_i,k_i}, {v^n_1}_{p_1,q_1}, \cdots, {v^n_{i-1}}_{p_{i-1},q_{i-1}}),$$

such that if terminal $\mathcal{X}_2$ transmits the index p_i to terminal $\mathcal{X}_1$, the latter can reconstruct q_i by the joint typicality of ${v^n_i}_{p_i,q_i}$ with

$$(x^n_1, {u^n_1}_{j_1,k_1}, \cdots, {u^n_i}_{j_i,k_i}, {v^n_1}_{p_1,q_1}, \cdots, {v^n_{i-1}}_{p_{i-1},q_{i-1}}).$$

It can be shown that the entropy of the set of random integers $\{(j_i, k_i, p_i, q_i),\ 1 \leq i \leq r\}$ is close to $\log(\prod_{i=1}^r N_{1,i}N_{2,i}M_{1,i}M_{2,i})$. Hence, this set of random integers will represent CR of rate close to $\frac{1}{n}\log(\prod_{i=1}^r N_{1,i}N_{2,i}M_{1,i}M_{2,i})$. The subset of the random integers, $\{(k_i, q_i),\ 1 \leq i \leq r\}$, will represent the SK of rate close to $\frac{1}{n}\log(\prod_{i=1}^r N_{2,i}M_{2,i})$.

BIBLIOGRAPHY

[1] A. Aaron and B. Girod, "Compression with side information using turbo codes," *Proc. IEEE Data Compression Conference,* pp. 252–261, Snowbird, UT, Apr. 2002.

[2] R. Ahlswede and P. Gács, "Spreading of sets in product spaces and hypercontraction of the Markov operator," *Annals of Probability*, vol. 4, pp. 925–939, 1976.

[3] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, July 1993.

[4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography, Part II: CR capacity," *IEEE Trans. Inform. Theory,* vol. 44, pp. 225–240, Jan. 1998.

[5] C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory,* vol. 41, pp. 1915–1923, Nov. 1995.

[6] B. Bing, *Wireless Local Area Networks: The New Wireless Revolution.* New York: Wiley, 2002.

[7] M. Brooks, *Quantum Computing and Communications.* London: Springer-Verlag, 1999.

[8] J. A. Buchmann, *Introduction to Cryptography,* New York: Springer, 2000.

[9] C. Cachin and U. Maurer, "Unconditional security against memory-bounded adversaries," *Advances in Cryptology - CRYPTO '97*, B.S. Kaliski Jr. (Ed.), Lecture Notes in Computer Science, Springer–Verlag, pp. 292–306, 1997.

[10] T. P. Coleman, A. H. Lee, M. Médard and M. Effros, "On some new approaches to practical Slepian-Wolf compression inspired by channel coding," *Proc. IEEE Data Compression Conference,* pp. 282–291, Snowbird, UT, March 2004.

[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory,* New York: Wiley, 1991.

[12] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Trans. Inform. Theory,* vol. 28, no. 4, pp. 585–592, July, 1982.

[13] I. Csiszár, "Almost independence and secrecy capacity," *Probl. Pered. Inform. (Special issue devoted to M.S. Pinsker),* vol. 32, no. 1, pp. 48–57, 1996.

[14] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory,* vol. IT-24, pp. 339–348, May 1978.

[15] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* Academic, New York, N.Y., 1982.

[16] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inform. Theory*, vol. 46, pp. 344–366, March 2000.

[17] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3047–3061, Dec. 2004.

[18] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory,* vol. IT-22, pp. 644–654, Nov. 1976.

[19] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory,* vol. 4, pp. 469–472, July 1985.

[20] P. Elias, “Coding for noisy channels,” *IRE Convention Record*, Part 4, pp. 37–46, 1955.

[21] E. M. Gabidulin, “Bounds for the probability of decoding error when using linear codes over memoryless channels,” *Prob. Pered. Inform.*, vol. 3, pp. 55–62, 1967.

[22] P. Gács and J. Körner, “Common information is far less than mutual information,” *Probl. Contr. Inform. Theory*, vol. 2, pp. 149–162, 1973.

[23] J. Garcia-Frias and Y Zhao, “Compression of correlated binary sources using turbo codes,” *IEEE Commun. Lett.,* vol. 5, pp. 417–419, Oct. 2001.

[24] J. Garcia-Frias and W. Zhong, “LDPC codes for compression of multi-terminal sources with hidden Markov correlation,” *IEEE Commun. Lett.,* vol. 7, no. 3, pp. 115–117, March 2003.

[25] H. O. Georgii, *Gibbs Measures and Phase Transitions.* de Gruyter, Berlin – New York, 1988.

[26] M. E. Hellman, “An overview of public key cryptography,” *IEEE Comm. Mag.*, vol. 40, pp. 42–49, May 2002.

[27] R. Hu, R. Viswanathan and J. Li, “A new coding scheme for the noisy-channel Slepian-Wolf problem: Separate design and joint decoding,” *Proc. Global Commun. Conference,* Dallas, TX, 2004.

[28] J. Korhonen, *Introduction to 3G Mobile Communications,* 2nd edition, Norwood: Artech House, 2003.

[29] C. Lan, A. Liveris, K. Narayanan, Z. Xiong and C. N. Georghiades, "Slepian-Wolf coding of multiple M-ary sources using LDPC codes," *Proc. IEEE Data Compression Conference,* p. 549, Snowbird, UT, March 2004.

[30] A. K. Lanstra and E. R. Verheul, "Selecting cryptographic key sizes," *Journal of Cryptology,* vol. 14, No. 4, pp. 255–293, 2001.

[31] J. Li, Z. Tu and R. Blum, "Slepian-Wolf coding for nonuniform sources using turbo codes," *Proc. IEEE Data Compression Conference,* pp. 312–321, Snowbird, UT, March 2004.

[32] A. D. Liveris, Z. Xiong and C. N. Georghiades, "Compression of binary sources with side information at the decoding using LDPC codes," *IEEE Commun. Lett.*, vol. 6, pp. 440–442, Oct. 2002.

[33] A. D. Liveris, C. Lan, K. R. Narayanan, Z. Xiong and C. N. Georghiades, "Slepian-Wolf coding of three binary sources using LDPC codes," *Proc. Intl. Symp. Turbo Codes and Related Topics,* Brest, France, Sept. 2003.

[34] D. J. C. Mackay, "Good error correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory,* vol. 45, pp. 399–431, Mar. 1999.

[35] G. A. Margulis, "Probabilistic characteristics of graphs with large connectivity," *Probl. Inform. Trans.* vol. 10, pp. 174–179, Apr. 1974.

[36] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory,* vol. 39, pp. 733–742, May 1993.

[37] U. M. Maurer, “The strong secret key rate of discrete random triples,” *Communications and Cryptography: Two Sides of One Tapestry*, R. E. Blahut *et al.*, Ed., Kluwer, Norwell, MA, Ch. 26, pp. 271–285, 1994.

[38] U. M. Maurer, “Information-theoretically secure secret-key agreement by NOT authenticated public discussion,” in *Advances in Cryptology — EUROCRYPT ’97, Lecture Notes in Computer Science,* (W. Fumy, Eds.), Berlin, Germany: Springer-Verlag, 1997.

[39] U. M. Maurer and S. Wolf, “Unconditionally secure key agreement and the intrinsic conditional information,” *IEEE Trans. Inform. Theory,* vol. 45, pp. 499-514, Mar. 1999.

[40] U. M. Maurer and S. Wolf, “Information-theoretic key agreement: from weak to strong secrecy for free,” *Proc. EUROCRYPT 2000*, Lecture notes in Computer Science, pp. 352–368, Springer-Verlag, 2000.

[41] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result,” *IEEE Trans. Inform. Theory,* vol. 49, pp. 822–831, Apr. 2003.

[42] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition,” *IEEE Trans. Inform. Theory,* vol. 49, pp. 832–838, Apr. 2003.

[43] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels—Part III: Privacy amplification,” *IEEE Trans. Inform. Theory,* vol. 49, pp. 839–851, Apr. 2003.

[44] P. Mitran and J. Bajcsy, "Turbo source coding: A noise-robust approach to data compression," *IEEE Data Compression Conference,* p. 465, Snowbird, UT, Apr. 2002.

[45] J. Muramatsu, "Secret key agreement from correlated source outputs using LDPC matrices," *IEICE Trans. Fundamentals,* vol. E87-A, pp. 1–10, 2004.

[46] V. Niemi and K. Nyberg, *UMTS Security,* London: Wiley, 2004.

[47] NIST (National Institute of Standards and Technology) *FIPS (Federal Information Processing Standard) Publication 46: Data encryption standard.* 1977.

[48] NIST (National Institute of Standards and Technology) *FIPS (Federal Information Processing Standard) Publication 197: Specification for the advanced encryption standard (AES).* 2001.

[49] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, 2nd edition, MIT Press: Cambridge, Mass. 1972.

[50] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inform. Theory,* vol. 49, pp. 626–643, March 2003.

[51] R. Renner and S. Wolf, "New bounds in secret-key agreement: the gap between formation and secrecy extraction," *Proc. EUROCRYPT'03, Lecture Notes in Computer Science,* E. Biham, Ed., Heidelberg, Germany: Springer-Verlag, 2003, pp. 562–577.

[52] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inform. Theory,* vol. 47, pp. 599–618, Feb. 2001.

[53] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digial signatures and public-key cryptosystems," *Commun. ACM,* vol. 21, no. 2, pp. 120–126, 1978.

[54] S. Roman, *Introduction to Coding and Information Theory,* New York: Springer, 1996.

[55] G. Schäfer, *Security in Fixed and Wireless Networks: An Introduction to Securing Data Communications,* London: Wiley, 2003.

[56] D. Schonberg, K. Ramchandran and S. S. Pradhan, " Distributed code constructions for the entire Slepian-Wolf rate region for arbitrarily correlated sources," *Proc. IEEE Data Compression Conference,* pp. 292–301 Snowbird, UT, March 2004.

[57] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory,* vol. 27, pp. 533–547, Sept. 1981.

[58] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin and J. M. Merolla, "Capacity achieving codes for the wiretap channel with applications to quantum key distribution," e-print cs. IT/0411003, 2004.

[59] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory,* London: Prentice Hall, 2001.

[60] R. Urbanke, *Modern Coding Theory,* to appear, http://lthcwww.epfl.ch/mct/index.php.

[61] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set eqaulity," *J. Comput. Syst. Sci.,* vol. 22, pp. 265–279, 1981.

[62] S. Wolf, “Unconditional security in cryptography,” *Lectures on Data Security: Modern Cryptology in Theory and Practice*, I. Damgard (Ed.), Lecture Notes in Computer Science, Springer–Verlag, pp. 217–250, 1999.

[63] A. D. Wyner, “Recent results in the Shannon theory,” *IEEE Trans. Inform. Theory,* vol. 20, pp. 2–10, Jan. 1974.

[64] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.,* vol. 54, pp. 1355–1387, Oct. 1975.

[65] A. D. Wyner, J. K. Wolf and F. M. J. Willems, “Communicating via a processing broadcast satellite,” *IEEE Trans. Inform. Theory,* vol. 48, pp. 1243–1249, June. 2002.