# ABSTRACT

Title of dissertation: PRIVATE COMMUNICATIONS WITH
CHAOTIC CODE DIVISION MULTIPLE ACCESS:
PERFORMANCE ANALYSIS AND SYSTEM DESIGN

Yeong-Sun Hwang, Doctor of Philosophy, 2004

Dissertation directed by: Assistant Professor Haralabos C. Papadopoulos
Department of Electrical and Computer Engineering

In this dissertation we develop a class of pseudochaotic direct-sequence code division multiple access (DS/CDMA) systems that can provide private and reliable communication over wireless channels. These systems exploit the sensitive dependence of chaotic sequences on initial conditions together with the presence of channel noise to provide a substantial gap between the bit error probabilities achievable by intended and unintended receivers. We illustrate how a desired level of private communication can be achieved with a systematic selection of the system parameters. This type of privacy can be readily combined with traditional encryption methods to further ensure the protection of information against eavesdroppers.

The systems we propose employ linear modulation of each user's symbol stream on a spreading sequence generated by iterating a distinct initial condition through a pseudochaotic map. We evaluate and compare the uncoded probability of error ($\Pr(\epsilon)$) achievable by intended receivers that know the initial condition used to generate the spreading sequence to the associated $\Pr(\epsilon)$ of unintended receivers that know the modulation scheme but not the initial condition. We identify the map attributes that affect privacy, and construct algorithmic design methods for generating pseudochaotic spreading sequences that successively and substantially degrade the unintended user performance, while yielding intended user performance similar to that of conventional DS/CDMA systems. We develop efficient metrics for quantifying the unintended receiver $\Pr(\epsilon)$ and prove that it decays at a constant rate of $1/\sqrt{\mathrm{SNR}}$ in AWGN and fading channels. In addition, we show that this decaying rate is independent of the available degrees of diversity in fading channels, showing in the process that only intended receivers can harvest the available diversity benefits. Moreover, we illustrate that the pseudochaotic DS/CDMA systems can provide reliable multiuser communication that is inherently resilient to eavesdropping, even in the worst-case scenarios where all receivers in a network except the intended one collude to better eavesdrop on the targeted transmission. We also develop optimized digital implementation methods for generating practical pseudochaotic spreading sequences that preserve the privacy characteristics associated with the underlying chaotic spreading sequences.

# PRIVATE COMMUNICATIONS WITH CHAOTIC CODE DIVISION MULTIPLE ACCESS: PERFORMANCE ANALYSIS AND SYSTEM DESIGN

by

Yeong-Sun Hwang

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
2004

Advisory Committee:

Professor Haralabos C. Papadopoulos, Chair
Professor Edward Ott
Professor K. J. Ray Liu
Professor André Tits
Professor Brian R. Hunt

# ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to the people whose support and help have guided the shaping of this dissertation and my graduate life at Maryland.

First and foremost, I would like to express my heartfelt gratitude to my advisor, Babis Papadopoulos. Babis is a truly inspiring mentor, whose enthusiasm, encouragement, keen technical insights, and unwavering dedication to the growth of his students have all been invaluable to my doctoral studies. I am indebted to fortune for having had Babis as my advisor.

I would like to gratefully acknowledge my Committee member Professor Ed Ott for his thoughtful feedbacks during the evolution of this work. I also would like to thank Professor Richard La for his many counsels on my professional development.

I have been blessed with a particularly cheery and supportive colleagues in our research group. Many, many thanks to Dzulkifli Scherber for his friendship and camaraderie, to Mohamed ”Guru” Abdallah for all the computer-related helps and numerous exciting technical and not-so-technical discussions, and to Tien Pham for just about everything else, including the sagely advices on married life and, of course, the cookies. Thanks are also due to Rengarajan Aravamudhan for being a great guinea pig of my lecture attempts. I wish them the best of luck in all their future endeavors.

I am grateful to the wonderful friends that I have met in Maryland. Special thanks go to Seung-Jong Baek for the innumerable airport rides, to Min-Young Kim for the grocery raids, and to Nuengwong ”Ohm” Tuaycharoen for the dinner gatherings. Their loyal friendship has provided many fond memories. Thanks also go to Rania Mameesh for the office chats, and to Junghwan Kim and Jae-Hwan Chang for their help during my rookie grad student days.

Many friends near and far have rooted for me during the last five years. I want to express my sincerest thanks to Soyoung Lee and Aeree Chung in New York for their warm and caring friendship. I am particularly thankful to Soyoung for her encouragements during my early moody days in the States. Heejung Yang, Changsoo Kim, Juntae Park, Jangwon Hu, and Jongmin Kim deserve many thanks for remaining the old faithful friends they have always been. I am especially beholden to Heejung for continuing as my counselor and spokesperson throughout the years. I am also grateful to the ”oboe family” – Miseop Lee, Eunkang Park, and Soyoung Kwon – for the bright moments and deserts we’ve shared.

As always, I thank my parents and my little sister Oon-Kyung for their support and love. Indeed, my appreciation of mom’s sheer devotion is hard to convey in words. Along with the rest of my extended family, they have provided moral support time and again.

Finally, my loving thanks go to my dear wife Eunjung Lee, who has willingly shared the tumultuous final stage of doctoral studies during the last seven months. I look forward to the next chapter of adventure-filled saga that we are writing together.

# Contents

**1 Introduction** **1**

1.1 Outline of the Thesis . . . . . . . . . . . . . . . . . . . . . . . . . . 7

**2 A Class of Pseudochaotic DS/CDMA Systems** **10**

2.1 System Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11

2.2 Sequences Generated from a Class of Piecewise-Linear Chaotic Maps 13

2.2.1 Representations of Chaotic Sequences . . . . . . . . . . . . . 16

2.2.2 Sequence Power Characteristics . . . . . . . . . . . . . . . . . 18

2.3 Digital Realization of Sequences from $P \times Q$ Partition Maps . . . . . 22

**3 Analysis and Design of Pseudochaotic DS/SS Systems: AWGN Channels** **28**

3.1 Intended Receiver Performance . . . . . . . . . . . . . . . . . . . . . 31

3.2 Unintended Receiver Performance . . . . . . . . . . . . . . . . . . . . 35

3.2.1 Performance Evaluation for $P$-partition Maps . . . . . . . . . 37

3.2.2 Performance Dependence on System Parameters . . . . . . . . 39

3.2.3 Asymptotic Decaying Rate of $\Pr(\epsilon)$ for Odd $P$-partition Maps 44

3.2.4 Performance Evaluation for Odd $P \times Q$ Partition Maps . . . . 47

3.3 Iterative Constructions of $P \times Q$ Partition Map-based DS/SS . . . . 50

3.3.1 Closed-Form $\Pr(\epsilon)$ Prediction for a Class of Nested Maps . . . 53

3.4 Privacy via Pseudochaotic DS/SS . . . . . . . . . . . . . . . . . . . . 57

**4 Analysis and Design of Pseudochaotic DS/SS Systems: Fading Channels 62**

4.1 System Model . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 64

4.2 Design of Chaotic DS/SS for Fading Channels . . . . . . . . . . . . . 68

4.3 Intended Receiver Performance . . . . . . . . . . . . . . . . . . . . . 70

4.3.1 Slow Flat Fading . . . . . . . . . . . . . . . . . . . . . . . . 70

4.3.2 Fast Flat Fading . . . . . . . . . . . . . . . . . . . . . . . . 78

4.4 Unintended Receiver Performance . . . . . . . . . . . . . . . . . . . 83

4.4.1 Slow Flat Fading . . . . . . . . . . . . . . . . . . . . . . . . 84

4.4.2 Fast Flat Fading . . . . . . . . . . . . . . . . . . . . . . . . 90

4.4.3 Asymptotic Decaying Rate of $\Pr(\epsilon)$ . . . . . . . . . . . . . . . 93

4.5 Implications of Fading on Privacy . . . . . . . . . . . . . . . . . . . 96

**5 Analysis and Design of Pseudochaotic DS/CDMA Systems: Multiuser Case 100**

5.1 Correlation and Spectral Characteristics . . . . . . . . . . . . . . . . 102

5.2 ML Reception of Chaotic DS/CDMA Signals . . . . . . . . . . . . . . 107

5.3 Privacy Characteristics of Multiuser Systems . . . . . . . . . . . . . 111

**6 Contributions and Future Directions 117**

6.1 Contributions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 117

6.2 Future Directions . . . . . . . . . . . . . . . . . . . . . . . . . . . . 120

**A 123**

A.1 Definitions for Chaotic Map Characteristics . . . . . . . . . . . . . . 123

**B** **125**

B.1 Approximate Maximum Likelihood Sequence Estimation for Nested Maps . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 125

B.2 A Detection Scenario for Lower Bounding the Unintended Receiver $\Pr(\epsilon)$127

**C** **132**

C.1 Probability Density Function of Observables in Slow Flat Fading . . . 132

C.2 Maximum Likelihood Reception in Slow Flat Fading . . . . . . . . . . 134

C.3 Intended Receiver $\Pr(\epsilon|\mathbf{c}^L)$ in Slow Flat Rayleigh Fading . . . . . . . 136

C.4 Maximum Likelihood Reception in Fast Flat Fading . . . . . . . . . . 138

# List of Figures

1.1 Layers of communication privacy. . . . . . . . . . . . . . . . . . . . . . . 2

1.2 Block diagram of a chaotic DS/SS modulator. . . . . . . . . . . . . . 6

2.1 Block diagram of a chaotic DS/CDMA transmitter. . . . . . . . . . . 11

2.2 A discrete-time baseband model for a time-selective fading channel . 12

2.3 Example $P \times Q$ partition map and $P$-partition map. . . . . . . . . . 15

2.4 Dyadic map and its sequence power characteristics for $L = 4$. . . . . . 19

2.5 Sequences with minimum sequence power for dyadic map and $L = 2$. $\oplus$ marks correspond to the sequences with minimum $\left\|\mathbf{c}^L\right\|$. . . . . . . 21

2.6 Finite states representation of $(M \circ G)^{(n)}(x)$. Solid arrows correspond to $M(x) = x$ (2.23a) and dashed arrows correspond to $M(x) = q - x$ (2.23b), for $x \in \mathcal{S}_{Q'}$. . . . . . . . . . . . . . . . . . . . . . . . . . 26

2.7 An example masking operation on an $r$-adic map. $G(x)$ is the dyadic map, $M(x)$ is a masking map satisfying the conditions in Theorem 1, and $H(x) = M \circ G(x)$ is the output map of masking. . . . . . . . . . 27

3.1 Block diagram of a chaotic DS/SS modulator. . . . . . . . . . . . . . 29

3.2 Accuracy of itinerary distribution approximation of intended receiver $\Pr(\epsilon)$ for $P = 2$. Solid curves represent analytically computed $\Pr(\epsilon)$ expression (3.6), and dashed curves with circles represent analytically computed $\Pr(\epsilon)$ approximation (3.7). . . . . . . . . . . . . . . . . . . . 33

3.3 Intended receiver $\Pr(\epsilon)$ performance vs. SNR for various spreading gain $L$. Solid curves indicate analytically computed $\Pr(\epsilon)$'s and dashed curves indicate the lower and upper bounds for a given number of partitions. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35

3.4 Intended receiver $\Pr(\epsilon)$ performance vs. SNR for various number of partitions $P$. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36

3.5 Upper and lower bounds for the unintended receiver performance. . . 38

3.6 Pairwise signal trajectories for tent and dyadic map-based SS systems, in the cases $b[1] = b[0] = \sqrt{\mathcal{E}_b}$ (solid) and $b[1] = -b[0] = -\sqrt{\mathcal{E}_b}$ (dashed). 40

3.7 Upper graphs: valid signal trajectories $(x[L-1], x[L])$ for two odd 4-partition maps, under hypotheses $b[0]=b[1]$ (solid), and $b[0] = -b[1]$ (dashed). Lower graphs: associated decision regions based on $(y[L-1], y[L])$. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 41

3.8 Numerically computed upper bounds on the unintended receiver $\Pr(\epsilon)$ vs. spreading gain for several SS systems employing 4-partition maps. 42

3.9 Analytically computed intended receiver $\Pr(\epsilon)$'s vs. numerically computed upper bounds on $\Pr(\epsilon)$'s of unintended receivers, for $r$-adic map based SS systems. Dashed curve corresponds to the lower bound on the intended receiver $\Pr(\epsilon)$ (3.8). . . . . . . . . . . . . . . . . . . . . 44

3.10 Simulated upper bound and approximation to lower bound on the unintended receiver $\Pr(\epsilon)$ via (3.19) for dyadic map and various values of $w$ ($M_o = 4092$). . . . . . . . . . . . . . . . . . . . . . . . . . . 49

3.11 Upper graphs: signal trajectories for nested maps based on dyadic map, under hypotheses $b[0] = b[1]$ (solid), and $b[0] = -b[1]$ (dashed). Lower graphs: associated decision regions. . . . . . . . . . . . . . . . 50

3.12 Intended receiver $\Pr(\epsilon)$ vs. simulation-based upper bounds (3.20) on unintended receiver $\Pr(\epsilon)$, for nested maps based on dyadic map. . . . 52

3.13 Simulation-based upper bounds on the unintended receiver $\Pr(\epsilon)$ vs. SNR for nested map-based DS/SS with various spreading gains. . . . 54

3.14 Upper graphs: signal trajectories for sequence of nested maps with $r = 2^\ell$ under hypotheses $i[1] = +1$. Lower graphs: associated decision regions. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55

3.15 Intended receiver $\Pr(\epsilon)$ vs. simulation-based upper bounds and prediction (3.22) on unintended receiver $\Pr(\epsilon)$ for nested maps $F_{r,\ell}(\cdot)$. . . 56

3.16 Left-hand side: Signal trajectories $\{x[L-1], x[L]\}$ for the $B$-bit implementation of the nested maps $F_{2,1}$, under hypotheses $b[0] = b[1]$ (solid), and $b[0] = -b[1]$ (dotted). Right-hand side: Close-up view of a part of the mapping, showing several circles representing the constellation points, under hypotheses $b[0] = b[1]$ (dark) and $b[0] = -b[1]$ (light). . 57

3.17 Unintended receiver $\Pr(\epsilon)$ via (3.19) for the nested map $F_{2,1}$ as a function of $\overline{\gamma}_b$ for various values of bit precision depth $B$. . . . . . . . . 59

3.18 Unintended receiver $\Pr(\epsilon)$ via (3.19) as a function of $\overline{\gamma}_b$ for various nested maps with $r = 2$ and $B = 8$. . . . . . . . . . . . . . . . . . . . 61

4.1 The effect of fading on the decision region partitioning of the nested maps $F_{2,0}(\cdot)$ and $F_{2,1}(\cdot)$. . . . . . . . . . . . . . . . . . . . . . . . . 69

4.2 Accuracy of Gaussian approximation of intended receiver $\Pr(\epsilon)$ for dyadic map, $K = 1$, and $\overline{\gamma}_p \to \infty$. Solid curves indicate analytically computed $\Pr(\epsilon)$ ((4.14) for $L = 8$ and 16, (4.16) for $L = 32$ and 64), and dash-dot curves with circles represent analytically computed $\Pr(\epsilon)$ approximation (4.20). . . . . . . . . . . . . . . . . . . . . . . . . 76

4.3 Intended receiver $\Pr(\epsilon)$ performance vs. $\overline{\gamma}_b$ for various level of pilot quality $\overline{\gamma}_p$. Dashed curves with markers represent simulated $\Pr(\epsilon)$ associated with imperfect channel estimation (4.7). Lower solid curve represents analytically computed $\Pr(\epsilon)$ (4.14) for perfect channel estimation and upper solid curve represents 3 dB shifted copy of the lower curve. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 77

4.4 Analytically computed intended receiver $\Pr(\epsilon)$ (4.14) vs. $\overline{\gamma}_b$ for various number of receiver antenna elements $K$ and perfect channel estimation. 78

4.5 Simulated intended receiver $\Pr(\epsilon)$ (4.21) vs. $\overline{\gamma}_b$ for various level of pilot quality $\overline{\gamma}_p$. The dashed curve indicate the $\Pr(\epsilon)$ curve for perfect channel estimation, and the solid curves with markers indicate the $\Pr(\epsilon)$ curves for imperfect channel estimation. . . . . . . . . . . . . . . . . 82

4.6 Simulated intended receiver $\Pr(\epsilon)$ vs. $\overline{\gamma}_b$ for various spreading gain $L$. 83

4.7 Simulated intended receiver $\Pr(\epsilon)$ vs. $\overline{\gamma}_b$ for various number of receiver antenna elements $K$. . . . . . . . . . . . . . . . . . . . . . . . . . 84

4.8 Simulated upper bound (4.37) and approximations to lower bound (4.33) on the unintended receiver $\Pr(\epsilon)$ for various values of $w$. . . . . 88

4.9 Simulated approximations to lower bounds (4.32) and (4.33) on the unintended receiver $\Pr(\epsilon)$ for various level of channel estimation quality $\overline{\gamma}_p$. The thicker dashed curve corresponds to the case of perfect channel estimation, and the solid curves with markers correspond to the case of imperfect channel estimation. . . . . . . . . . . . . . . . . . . . . . 89

4.10 Simulated approximations to lower bounds (4.42) and (4.43) on the unintended receiver $\Pr(\epsilon)$ for various levels of channel estimation quality $\overline{\gamma}_p$. The dashed curve corresponds to the case of perfect channel estimation, and the solid curves with markers correspond to the case of imperfect channel estimation. . . . . . . . . . . . . . . . . . . . . . 93

4.11 Approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ in Rayleigh fading and AWGN. . . . . . . . . . . . . . . . . . . . . . . . . . . . 97

4.12 Intended receiver $\Pr(\epsilon)$ (dashed) and approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ (solid) for $K$ degrees of spatial diversity in slow flat Rayleigh fading. . . . . . . . . . . . . . . . . . . . . . . . . . 98

4.13 Intended receiver $\Pr(\epsilon)$ (dashed) and approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ (solid) for $K$ degrees of spatial diversity and imperfect channel estimation in fast flat Rayleigh fading. . . . . . . . 99

5.1 Comparison of analytically computed autocorrelation of sequences from nested maps and empirical autocorrelation estimates of their pseudochaotic implementation. The lines represent analytically obtained autocorrelations of true chaotic trajectories, and the circles represent empirical estimates of numerical trajectories. Empirical estimates are obtained via (5.3) with $L_o = 100000$ on 48-bit precision realization. . 104

5.2 Analytically computed autocorrelation of the sequences from nested maps and the tent map. . . . . . . . . . . . . . . . . . . . . . . . . 105

5.3 Empirical power spectra of sequences from the nested maps and the tent map. The spectra are obtained by applying periodogram averaging with a window length of 1024 to a numerical trajectory of length 1024000.108

5.4 Simulated lower bound on the $\Pr(\epsilon)$ of the intended receiver for the 1st transmitter via (5.7) vs. SNR for various nested maps in a two-transmitter system ($H_2 = 2028$). Solid curves with markers correspond to $M = 2$, and solid curve without markers corresponds to analytically computed $\Pr(\epsilon)$ for single-user case ($M = 1$). . . . . . . . . . . . . . . 112

5.5 Simulated lower bounds on the $\Pr(\epsilon)$ of the intended and unintended receiver for 1st transmitter via (5.7) vs. SNR for various nested maps in a two-transmitter system. Dashed curves correspond to the intended receiver ($H_2 = 2028$) and solid curves correspond to the unintended receiver ($H_1 = 2028$). . . . . . . . . . . . . . . . . . . . . . . . . . . . 114

5.6 Simulated $\Pr(\epsilon)$ of single-user intended receiver (5.8) in $M = 4$ system (dashed curve) and simulated unintended receiver $\Pr(\epsilon)$ in $M = 1$ system via (3.19) (solid curve), for the nested map $F_{16,4}$ and $L = 64$. . 116

# List of Tables

2.1 The largest prime $q$, $q < 2^B$, such that nonzero sequences from (2.21) have period $q-1$, for $r = 2$ (dyadic map) and $r = 3$ (3-adic map). . . 24

4.1 Analytically computed error floor (4.26) of the intended receiver with $K$-element receiver antenna array for spreading gain $L$ in fast flat fading. 81

# Chapter 1

# Introduction

In this dissertation we examine the physical-layer privacy potential of a class of pseudochaotic direct sequence code division multiple access (DS/CDMA) systems for wireless communications. In particular, we consider linear modulation schemes based on spreading sequences generated from a class of one-dimensional (1D) piecewise-linear chaotic maps, and investigate the relative probability of error ($\Pr(\epsilon)$) performance advantages these systems provide to intended receivers over unintended ones. In the process we identify chaotic map properties that affect the $\Pr(\epsilon)$ gap between intended and unintended receivers and construct methods for designing maps that maximize these $\Pr(\epsilon)$ performance gaps. For DS/CDMA based on these maps, we develop metrics that quantify the unintended receiver $\Pr(\epsilon)$. For the chaotic spreading sequences of interest, we also develop optimized digital implementation methods, and analyze the associated unintended receiver performance characteristics.

Communication privacy, or keeping the informational content of transmitted messages private from unwanted entities, can be provided at different stages, or layers, of a communication system, as schematically illustrated in Fig. 1.1. Communication privacy can be provided via encoding messages with certain side information that is made available only to intended receivers to create asymmetry in the ability to

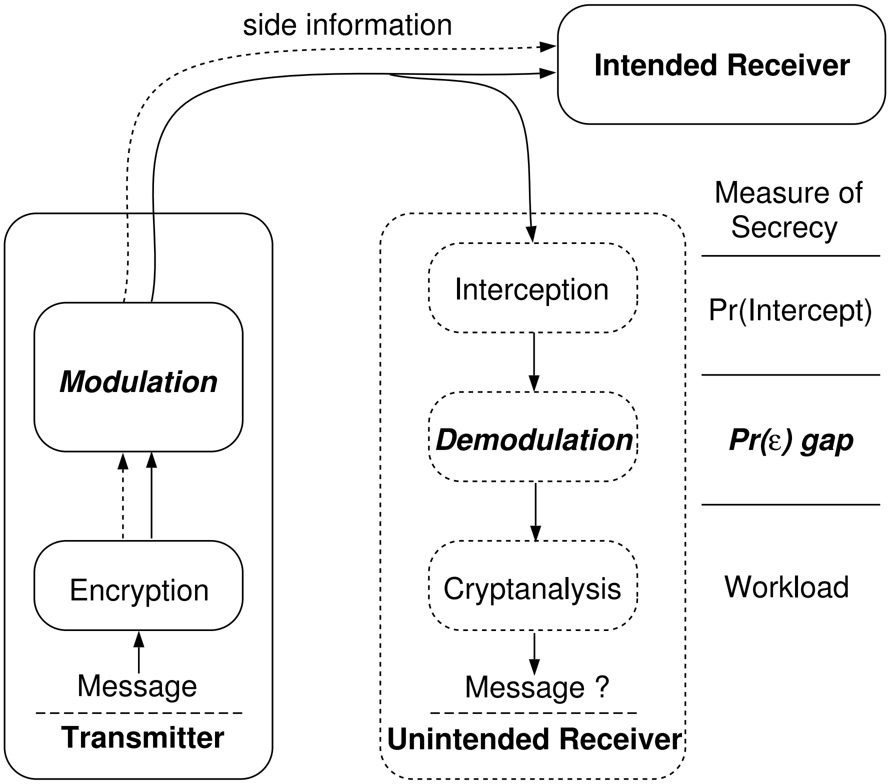


Figure 1.1: Layers of communication privacy.

receive and decode the message between intended and unintended receivers. The mainstream approach to communication privacy has been cryptographic methods. In cryptographic methods, the message is encrypted with some cipher such that decryption is computationally prohibitive for unintended receivers that do not know an input parameter, known as the key, to the encryption process. This type of privacy can be complemented by concealment systems, whereby the signal containing the message is hidden such that the probability of interception, or detection of the presence of the signal, by eavesdroppers is low. Concealment is especially viable in the context of communication over noisy channels, as in transmissions using electromagnetic waveform carriers, where listeners without appropriate modulation parameters have difficulty detecting the presence of low-power, wideband transmissions masked by channel noise. In addition, employing a modulator also as an encoder can provide additional privacy at the physical-layer, by means of degrading the bit error probability performance of unintended receivers without certain side information.

Spread spectrum (SS) systems, with their inherent low probability-of-intercept (LPI) capability, are good multiuser platforms for concealment of signal transmission, and have been employed in military communications with this purpose in mind [1]. In direct sequence spread spectrum (DS/SS) systems, the information-bearing signal is modulated onto a pseudorandom (PN) sequence at a rate much higher than the information rate. This spreads the signal power over a larger bandwidth, making it difficult for an unintended receiver to detect the signal in the presence of background noise. The large bandwidth also reduces the detrimental effects of narrowband interference and jamming. Furthermore, these schemes scale naturally to CDMA systems for multiuser environment by assigning different PN spreading sequences to different users. Since PN sequences can be chosen from sets of sequences with good auto- and cross-correlation properties, CDMA systems are robust against multiuser interference as well as self-interference due to multipath propagation. Moreover, withholding knowledge of a PN sequence (or the seed used to generate it) from unintended receivers results in a layer of communication privacy, where identifying the presence of the target signal in noisy observation does not guarantee sufficient demodulation performance for reconstructing the message without the knowledge of the PN sequence [1].

Sequences arising from suitably chosen chaotic maps can be employed in place of conventional binary PN spreading sequences generated from linear shift registers to provide an array of advantages. Indeed, the defining characteristics of trajectories from chaotic dynamics – deterministic, aperiodic, and exhibiting sensitive dependence on initial conditions [2]– have appealing implications in the context of single- and multiuser communications, and have naturally been proposed for communication in various forms in the last decade. The first communication system employing chaos was reported by Cuomo *et al.* [3] and pertains to a chaotic signal masking technique that employs chaotic systems decomposable into drive and response subsystems and exploits synchronization of the two (transmitter/receiver) subsystems to a common coupled signal [2, 4, 5]. Since chaotic sequences have broadband spectra and excellent auto- and cross-correlation properties, they are also well suited as spreading sequences in direct sequence spread spectrum (DS/SS) and multiuser communication applications. Chaotic DS/SS systems were originally suggested by Heidari-Bateni and McGillem [6]. Since then, two main classes of methods for incorporating chaotic dynamics into DS/SS systems have emerged. The first class includes methods whereby a continuous-time chaotic waveform is used as both modulating carrier and spreading signal [7], and where synchronization of two chaotic circuitries is exploited to reliably demodulate the information-bearing signal. The latter class employs spreading sequences based on trajectories from 1D chaotic maps. Such spreading sequences can be multilevel sequences generated by quantizing the original chaotic sequences [6, 8–13], unstable periodic orbits [14], or binary sequences suitably obtained from underlying chaotic sequences, *e.g.*, by exploiting the base-2 representation of numbers in the unit interval [15]. The performance of legitimate communicating pairs in a multiuser environment has been a key emphasis in the above and related literature. The statistics of chaotic sequences have been analyzed, and the correlation properties of certain such sequences were found to outperform those of binary-valued pseudonoise (PN) sequences [8, 10, 13]. In particular, it was shown that CDMA systems employing time-varying pseudochaotic spreading sequences can provide improvements in (intended) user $\Pr(\epsilon)$ with respect to their conventional CDMA counterparts (employing binary-valued PN spreading sequences). Indeed, for many of these systems the cochannel interference characteristics and the associated bit error probabilities of intended receivers have been evaluated and found to compare favorably to those of existing CDMA systems [8, 11, 12]. One such attractive example involves CDMA systems where all users employ spreading sequences generated by the same map but from distinct initial conditions.

In this dissertation we focus on DS/SS and CDMA systems employing pseudochaotic spreading sequences. We study the $\Pr(\epsilon)$ benefits these systems can provide to intended receivers over their unintended counterparts that do not know the seed used to generate the chaotic spreading sequence. We develop computationally efficient approximations and associated bounds for the $\Pr(\epsilon)$ of intended and unintended receivers over additive white Gaussian noise (AWGN) and fading channels, and determine the dependence of the receiver performance on system parameters. Such relationships are then exploited to design systems that optimize the relative $\Pr(\epsilon)$ advantages provided to intended users. For these systems, we develop efficient metrics that quantify the unintended receiver $\Pr(\epsilon)$ in various single-user and multiuser communication settings. As we show, these systems can be designed to provide substantially higher $\Pr(\epsilon)$ performance to unintended receivers. In particular, for suitably designed systems, the unintended receiver $\Pr(\epsilon)$ decays at a significantly slower rate as a function of signal-to-noise ratio (SNR) than the intended receiver $\Pr(\epsilon)$ does. This is in contrast to conventional DS/CDMA (assuming the seed used to generate the binary-valued PN spreading sequence is not made available to unintended receivers), where the unintended receiver $\Pr(\epsilon)$ decays at the same rate as that of the intended receiver.

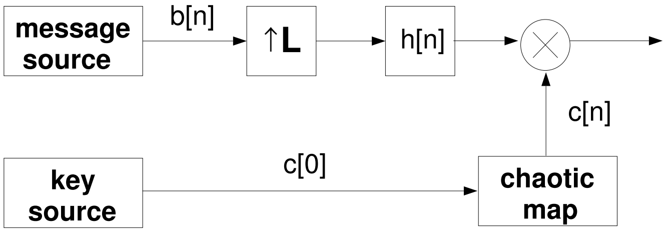


Figure 1.2: Block diagram of a chaotic DS/SS modulator.

The discrete-time baseband model of the chaotic DS/SS transmitters of interest is shown in Fig. 1.2, and involves a symbol stream $b[n]$ that is modulated on a sequence $c[n]$, generated by iterating an initial condition $c[0]$ through an 1D chaotic map. The inherent privacy potential of these systems is due to the combined effect of channel distortion and the sensitive dependence on initial conditions of chaotic trajectories. Due to the deterministic nature of chaotic dynamics, knowledge of the initial condition allows reconstruction of the spreading sequence, rendering the initial condition an ideal candidate for the key made available to intended users. The key allows the intended receiver to reconstruct the spreading sequence and form a (time-varying) matched-filter detector, in the same manner that intended receivers in conventional DS/SS systems use the initial seed to reconstruct via a linear feedback shift-register (LFSR) the spreading PN sequence that is used in forming a matched-filter detector.

Although for properly designed chaotic DS/SS systems with moderate/large spreading gains the intended receiver $\Pr(\epsilon)$ performance is effectively the same as that of their conventional DS/SS counterparts, as we show, chaotic DS/SS can result in substantially higher $\Pr(\epsilon)$ for unintended receivers that do not know the initial condition. Specifically, unintended receivers without the key face a composite detection problem, whereby, under each hypothesis, the unknown spreading sequence lies within an enormous set of valid chaotic trajectories. For the class of chaotic spreading sequences we consider, due to their sensitive dependence on initial conditions, consistent estimates of the initial conditions used to generate the spreading sequences cannot be formed from their noisy observations. Furthermore, not only these estimates are not efficient, but the ratio of the estimate error variance over the associated Cramér-Rao Lower Bound grows exponentially fast with the length of the observed sequence, for chip energy-to-noise ratios ($\mathcal{E}_c/N_o$) below a certain high threshold [16]. These properties are consistent with the fact that the number of local maxima of the likelihood function increases exponentially with the length of the sequence. In contrast, the seed of conventional binary-valued PN spreading sequences from known LFSRs can be consistently estimated based on noisy observations; indeed simple suboptimal estimators of the initial state of the LFSR can correctly identify the seed with very high probability based on just a fraction of the sequence period, even at very low $\mathcal{E}_c/N_o$ [17, 18].

Quantized chaotic system implementations are required to ensure that the number of bits needed to describe the key $c[0]$ is finite. Although such digital implementations inherently yield periodic pseudochaotic sequences, if properly designed, they can retain, in some sense, the sensitivity to initial conditions of the original systems, while generating trajectories with enormous periods that, for all practical purposes, can be viewed as aperiodic. In particular, for the chaotic maps of interest in this dissertation, given a $B$-bit description for $c[0]$, we develop digitized implementations that generate spreading sequences with periods of order $2^{B-1}$–$2^B$.

## 1.1 Outline of the Thesis

In this dissertation we develop and analyze a class of pseudochaotic DS/CDMA systems that allow reliable and private communication over AWGN and fading channels.

In Chapter 2, we describe the pseudochaotic DS/CDMA systems and the general channel model that captures all channels of interest, and introduce the class of chaotic maps employed to generate the spreading sequences in this work. In the process, we investigate the properties of the associated chaotic sequences that affect the $\Pr(\epsilon)$ performance of intended and unintended receivers. In addition, for certain subclasses of chaotic systems of practical interest, we develop attractive and efficient digital realization techniques and discuss their ramifications on communication privacy.

In Chapter 3, we study the communication privacy potential of single-user chaotic DS/SS systems in AWGN. We develop computationally efficient metrics for the $\Pr(\epsilon)$ of intended and unintended receivers, and obtain relationships between various system parameters and receiver performance. Based on these relationships, we develop iterative algorithms that yield sequences of chaotic DS/SS systems that monotonically improve the privacy benefits provided to intended receivers. For a certain class of system parameters with attractive associated receiver performance, we deduce the decaying rate of unintended receiver $\Pr(\epsilon)$ in high signal-to-noise ratio. This decaying rate is then exploited to establish efficient predictors of the unintended receiver $\Pr(\epsilon)$ for a subclass of these systems. We also investigate the effects of digital implementation of spreading sequences of interest on the unintended receiver performance, and deduce the range of system parameters over which the privacy trends for pseudochaotic DS/SS can approximate the privacy provided with true chaotic spreading.

In Chapter 4, we focus our investigation on the performance of chaotic DS/SS over fading channels. In particular, we examine the privacy potential of chaotic DS/SS given imperfect channel estimates at the receiver, for various diversity settings. We first validate the design methods of chaotic DS/SS in Chapter 3 in the context of fading channels. For an attractive class of systems developed in Chapter 3, we obtain computationally viable metrics for the $\Pr(\epsilon)$ of intended and unintended receivers in fading, and derive the decaying rate of unintended receiver $\Pr(\epsilon)$ in high signal-to-noise ratio. Finally, we study the dependence of communication privacy on the quality of channel estimates available at the receiver, along with its dependence on the available degrees of diversity. In the process, we demonstrate that a suitably designed chaotic DS/SS can indeed meet the required level of communication privacy over wireless channels.

In Chapter 5, we consider synchronous multiuser CDMA extensions of the class of chaotic DS/SS systems in Chapter 3. We characterize the spectral properties of the sequences of interest in an effort to verify their suitability as spreading codes in DS/CDMA systems. We then develop a multiuser detector framework that can capture various intended and unintended receiver scenarios with proper choice of the priors on the initial conditions. Utilizing this framework, we illustrate the privacy potential of chaotic DS/CDMA systems via some special cases.

Finally, a summary of the main contributions of this dissertation is given in Chapter 6, along with a representative collection of potentially interesting directions for future research that are suggested by this work.

# Chapter 2

# A Class of Pseudochaotic DS/CDMA Systems

In this dissertation, we consider a class of DS/SS-based CDMA systems for communication over noisy channels, where the spreading sequences for all users are generated by iterating distinct initial conditions through the same chaotic map. This chapter describes the main components of these systems that contribute to the communication reliablity and privacy – the DS/SS transmitter, its pseudochaotic spreading sequences, and the noisy channel model.

The outline of this chapter is as follows. In Section 2.1, we first introduce the model of the pseudochaotic DS/CDMA transmitter and the channel model that are the focus of this dissertation. In Section 2.2, we present the class of chaotic sequences utilized in obtaining the spreading sequences of interest and study their properties that affect communication privacy. In Section 2.3, we develop digital realization methods of spreading sequences from a class of chaotic maps that, for all practical purposes, allow the resulting pseudochaotic DS/SS systems to be evaluated via the analytical framework that we develop for their chaotic counterparts.

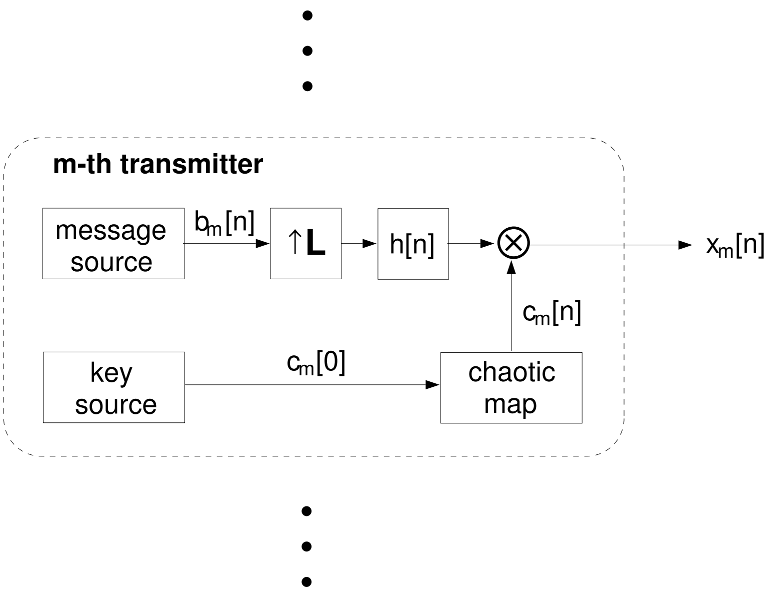


Figure 2.1: Block diagram of a chaotic DS/CDMA transmitter.

## 2.1 System Model

In this section we present the class of pseudochaotic DS/CDMA systems and channel models that are of interest in this dissertation.

A system model for the $m$-th pseudochaotic transmitter is shown in Fig. 2.1, where $m = 1, \ldots, M$ with $M$ representing the number of active transmitters in the system. The message stream $b_m[n] \in \left\{+\sqrt{\mathcal{E}_b}, -\sqrt{\mathcal{E}_b}\right\}$ is a sequence of statistically independent and identically distributed (IID) binary-valued symbols with equally likely symbol values, and $c_m[n]$ is the spreading sequence obtained by iterating an initial condition $c_m[0]$ through an 1D pseudochaotic map. The message stream $b_m[n]$ is upsampled by an integer factor of $L$, such that the output $b_{m,u}[n]$ of the upsampler is given by

$$b_{m,u}[n] = \begin{cases} b_m\left[\frac{n}{L}\right], & n = \ldots, -L, 0, L, 2L, \ldots \\ 0, & \text{otherwise} \end{cases} .$$

This output $b_{m,u}[n]$ is processed by a linear time-invariant (LTI) pulse-shaping filter

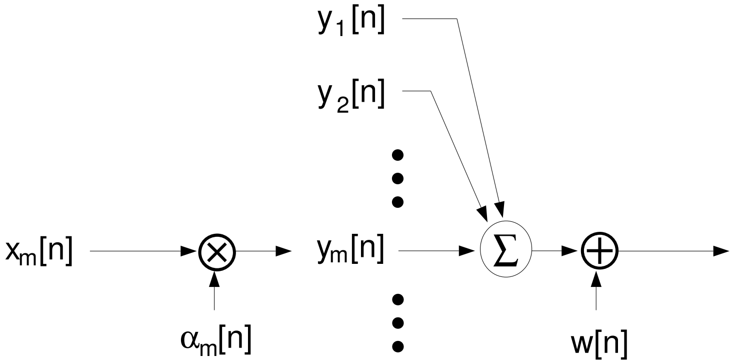


Figure 2.2: A discrete-time baseband model for a time-selective fading channel

$h[n]$, whose output is

$$b_{m,h}[n] = \frac{A}{\sqrt{L}} b_m \left[ \left\lfloor \frac{n}{L} \right\rfloor \right] \,, \tag{2.1}$$

where $A \overset{\triangle}{=} 1/\sqrt{E\left[c_m^2[n]\right]}$ guarantees that $\mathcal{E}_b$ equals the transmitted energy per bit and the floor function $\lfloor x \rfloor$ denotes the greatest integer less than or equal to $x$. The transmitted signal of $m$-th user is thus given by

$$x_m[n] = c_m[n] \sum_j b_m[k] \; h[n - kL] \,. \tag{2.2}$$

Besides replacing binary-valued LFSR spreading sequences with chaotic sequences, the system in Fig. 2.1 is effectively identical to a conventional DS/CDMA system with spreading gain $L$.

The channels of interest in this dissertation are modeled via a cascade of a bank of multiplicative components and an additive component, as shown in Fig. 2.2. Each multiplicative coefficient $\alpha_m[n]$ captures the effect of fading for each user. The additive component $w[n]$ represents the combined effect of a large number of independent noise sources at the receiver. Thus we assume that, via the central limit theorem, $w[n]$ follows Gaussian distribution and possess flat spectra. The intended and unintended users' received signal at time $n$ is of the form

$$y[n] = \sum_{m=1}^{M} \alpha_m[n] x_m[n] + w[n]\,, \tag{2.3}$$

where the fading coefficients $\alpha_m[n]$ are statistically independent in $m$ and $w[n]$ is an IID, zero-mean, complex-valued, circularly-symmetric stationary white Gaussian noise sequence with power $N_o/2$ per dimension.

The model (2.3) can represent many channels of interest with proper choice of the characterization of $\alpha_m[n]$. With $\alpha_m[n]$ an IID process, it naturally captures time-selective flat (frequency-nonselective) fading channels (with $n$ denoting the time index). Slow (time-nonselective) flat fading and AWGN channels are captured with $\alpha_m[n] = \alpha_m$, $\forall n$. While this channel model does not directly reflect frequency-selective fading scenarios, we remark that it can also capture these scenarios with an orthogonal frequency division multiplexing (OFDM) front-end at the transmitter. In this case, $x_m[n]$ may be viewed as the output of the $n$-th subcarrier in the OFDM system, whereby a frequency-selective channel is effectively transformed into a number of frequency-nonselective channels. We assume that, apart from $c_{m'}[0]$, the unintended receiver for $m'$-th transmitter has the same information as the intended receiver, including the knowledge of $\alpha_{m'}[n]$.

## 2.2 Sequences Generated from a Class of Piecewise-Linear Chaotic Maps

In this section we define the chaotic maps and sequences of interest, and present some of their attributes that affect the receiver performance and privacy behaviors. We then develop useful representations for these chaotic maps and sequences in Section 2.2.1, and examine the associated sequence power characteristics that are integral in the intended receiver $\Pr(\epsilon)$ analysis in Section 2.2.2. Methods for digital implementation of these chaotic sequences, and their ramifications are discussed in Section 2.3.

The chaotic spreading sequences we exploit in this work are generated via the recursion

$$c[n] = F(c[n-1])\,, \tag{2.4}$$

initialized with some initial condition $c[0] \in I \overset{\triangle}{=} [-1,\, 1]$. We assume that the map $F$ belongs to the class of piecewise-linear $P \times Q$ equipartition maps defined as follows:

**Definition 1.** *The map $F : I \to I$ is a piecewise-linear $P \times Q$ equipartition map if it satisfies the following conditions:*

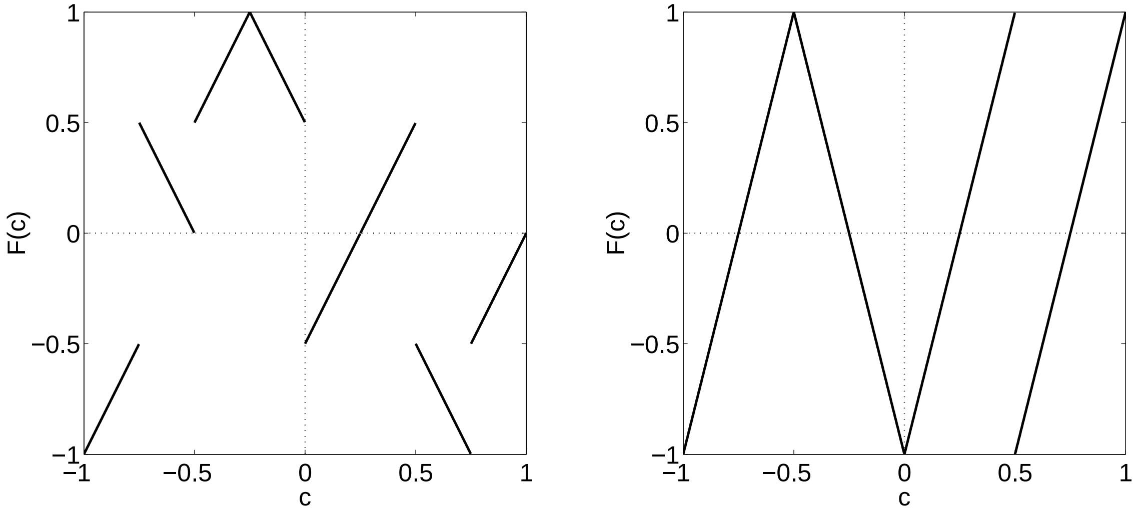
*(i) There exist partitions $-1 = a_0 < a_1 < \cdots < a_P = 1$ and $-1 = b_0 < b_1 < \cdots < b_Q = 1$ of $I$, where $P$ and $Q$ are positive integers with $P > Q$, such that, for each $i \in \{1, \ldots, P\}$, the restriction of $F$ to $I_i = I_i^P \overset{\triangle}{=} [a_{i-1}, a_i)$, $F|I_i$, is onto $[b_{j-1}, b_j)$, for some $j \in \{1, \ldots, Q\}$.*

*(ii) $F(\cdot)$ is surjective, i.e., for any $j \in \{1, \ldots, Q\}$, there exists an $i \in \{1, \ldots, P\}$ for which $F|I_i$ is onto $[b_{j-1}, b_j)$.*

*(iii) $F(\cdot)$ is piecewise linear, i.e., $F|I_i$ is affine for all $i$.*

*(iv) $F(\cdot)$ is equipartitioned, i.e., the sets of numbers $\{a_0,\, \ldots,\, a_P\}$ and $\{b_0,\, \ldots,\, b_Q\}$ are both uniformly spaced on $I$.*

For convenience, we refer to the class of maps of Defn. 1 with fixed $P$ and $Q$ as $P \times Q$ partition maps, and the subclass of Defn. 1 corresponding to $Q = 1$ as $P$-partition maps. Fig. 2.3 shows representative examples of $P \times Q$ partition maps and $P$-partition maps.



(a) a $P \times Q$ partition map with $P = 8, Q = 4$ (b) a $P$-partition map with $P = 4$

Figure 2.3: Example $P \times Q$ partition map and $P$-partition map.

The class of $P$-partition maps and the sequences they generate have a number of important properties. First, these maps have uniform invariant densities and are fully stretching, *i.e.*, $F|I_i$ is onto for all $i$. Moreover, they are exact and ergodic transformations that possess the Markov property [19, 20] in the sense of the definitions in App. A.1.[1] Exactness ensures complete loss of memory of initial conditions with repeated iterations of the map, and is directly related to the growth rate of sequence prediction error and the sensitive dependence on initial conditions. This sensitivity is captured by the Lyapunov exponent of the map, $\lambda = \log(P) > 0$, and thus depends *only* on the numbers of partitions $P$. Remarkably, however, as we show in Section 3.2, distinct maps with the same $P$, possessing the same sensitivity to initial conditions, can provide vastly different uncoded $\Pr(\epsilon)$ advantages to intended receivers. As $P$-partition maps are especially amenable to analysis, we employ them to illustrate

[1] The Markov property is particularly attractive in the context of multiuser CDMA systems, as there are readily available methods for analyzing the correlation and spectral characteristics of Markov sequences [19].

some of the key relationships between maps and the degree of privacy of the associated chaotic spread spectrum systems. These relationships are then exploited to select maps from the richer class of maps of Defn. 1 so as to achieve a required level of uncoded $\Pr(\epsilon)$ advantage offered to intended users. The subset of $P \times Q$ partition maps selected in the process also corresponds to exact Markov (and hence ergodic) maps, with uniform invariant densities and Lyapunov exponents $\lambda = \log(P/Q) > 0$.

### 2.2.1 Representations of Chaotic Sequences

We next develop certain important representations for $L$-point sequences

$$\mathbf{c}^L \triangleq \begin{bmatrix} c[0] & c[1] & \cdots & c[L-1] \end{bmatrix}^{\mathrm{T}} \tag{2.5}$$

generated by a given $P \times Q$ partition map. First, we note that $\mathbf{c}^L$ is fully determined by the initial condition $c[0]$, or, alternatively, by $c[L-1]$ and the set of partition indexes within which the iterates $\{c[n]; 0 \leq n < L\}$ fall; given this information one can reconstruct $\mathbf{c}^L$. Furthermore, we note that given any $c \in [-1,\, 1]$, we have $c \in I_i$ for a unique $i \in \{1,\, 2,\, \cdots,\, P\}$ and $F(c) \in [b_{j-1}, b_j)$ for a unique $j \in \{1, \ldots, Q\}$. For convenience, we define

$$s = s(c) \triangleq 2i - P - 1 \tag{2.6a}$$

and

$$q_s = q_s(s(c)) \triangleq 2j - Q - 1\,. \tag{2.6b}$$

The identifier functions in (2.6) are odd-symmetric, *e.g.*,

$$s(-c) = -s(c),\; c \in I. \tag{2.7}$$

Using (2.6), the mapping $F(\cdot)$ can be described as follows

$$y = F_s(x) = \frac{\zeta_s}{Q}\left(P \cdot x + \zeta_s \cdot q_s - s\right) , \tag{2.8}$$

where $\zeta_s$ denotes the sign of the slope of the piecewise-linear map on its restriction to the partition associated with the index $s = s(x)$. Similarly, the inverse map is given by

$$x = F_s^{-1}(y) = \zeta_s \left(\frac{Q \cdot y - q_s + \zeta_s \cdot s}{P}\right) . \tag{2.9}$$

Letting $s[n] = s(c[n])$, we have

$$c[n+1] = F(c[n]) = F_{s[n]}(c[n]) \;\Leftrightarrow\; c[n] = F_{s[n]}^{-1}(c[n+1]) \, , \tag{2.10}$$

and, hence, the following equivalent representations for $\mathbf{c}^L$

$$\mathbf{c}^L \quad \Leftrightarrow \quad c[0] \quad \Leftrightarrow \quad \{\mathbf{s}^{L-1}, \, c[L-1]\} \, , \tag{2.11}$$

where $\mathbf{s}^n \triangleq \begin{bmatrix} s[0] & s[1] & \cdots & s[n-1] \end{bmatrix}^{\mathrm{T}}$ is often referred to as the $n$-point itinerary of $c[0]$.

The pair of vectors

$$\zeta = \zeta^P \triangleq \begin{bmatrix} \zeta_{-P+1} & \zeta_{-P+3} & \cdots & \zeta_{P-1} \end{bmatrix}^{\mathrm{T}} , \tag{2.12}$$

comprising the ordered signs of the slopes of $F(\cdot)$ over the $P$ partitions, and

$$\mathbf{q} = \mathbf{q}^P \triangleq \begin{bmatrix} q_{-P+1} & q_{-P+3} & \cdots & q_{P-1} \end{bmatrix}^{\mathrm{T}} , \tag{2.13}$$

comprising the ordered range intervals associated with the $P$ partitions, completely characterize a $P \times Q$ partition map. For instance, the case $(P = 2, Q = 1)$ with $\zeta = \begin{bmatrix} 1 & -1 \end{bmatrix}^{\mathrm{T}}$ and $\mathbf{q} = \begin{bmatrix} 0 & 0 \end{bmatrix}^{\mathrm{T}}$ corresponds to the tent map

$$F_{\mathrm{T}}(c) = 1 - 2|c| \,, \tag{2.14}$$

while the case $\{\zeta_s = 1, \ \forall s\}$, $\{q_s = 0, \ \forall s\}$ results in the class of $r$-adic maps, with $(P = 2, Q = 1)$ corresponding to the dyadic map

$$F_{\mathrm{D}}(c) = 2(c+1) \mod 2 - 1 \ . \tag{2.15}$$

We remark that this characterization is not unique; any $P_0 \times Q_0$ partition map can be also viewed as a $(M \cdot P_0) \times (M \cdot Q_0)$ partition map for any positive integer $M$, by appropriately expanding the pair $\left(\zeta^{P_0}, \mathbf{q}^{P_0}\right)$ to $\left(\zeta^{M \cdot P_0}, \mathbf{q}^{M \cdot P_0}\right)$. For example, the tent map (2.14) can be also viewed as a $4 \times 2$ partition map with $\zeta = \begin{bmatrix} 1 & 1 & -1 & -1 \end{bmatrix}^{\mathrm{T}}$ and $\mathbf{q} = \begin{bmatrix} -1 & 1 & 1 & -1 \end{bmatrix}^{\mathrm{T}}$.

Any $P$-partition map $F(\cdot)$ and its inverse have the following concise descriptions:

$$y = F_s(x) = \zeta_s(P \cdot x - s) \,, \tag{2.16a}$$

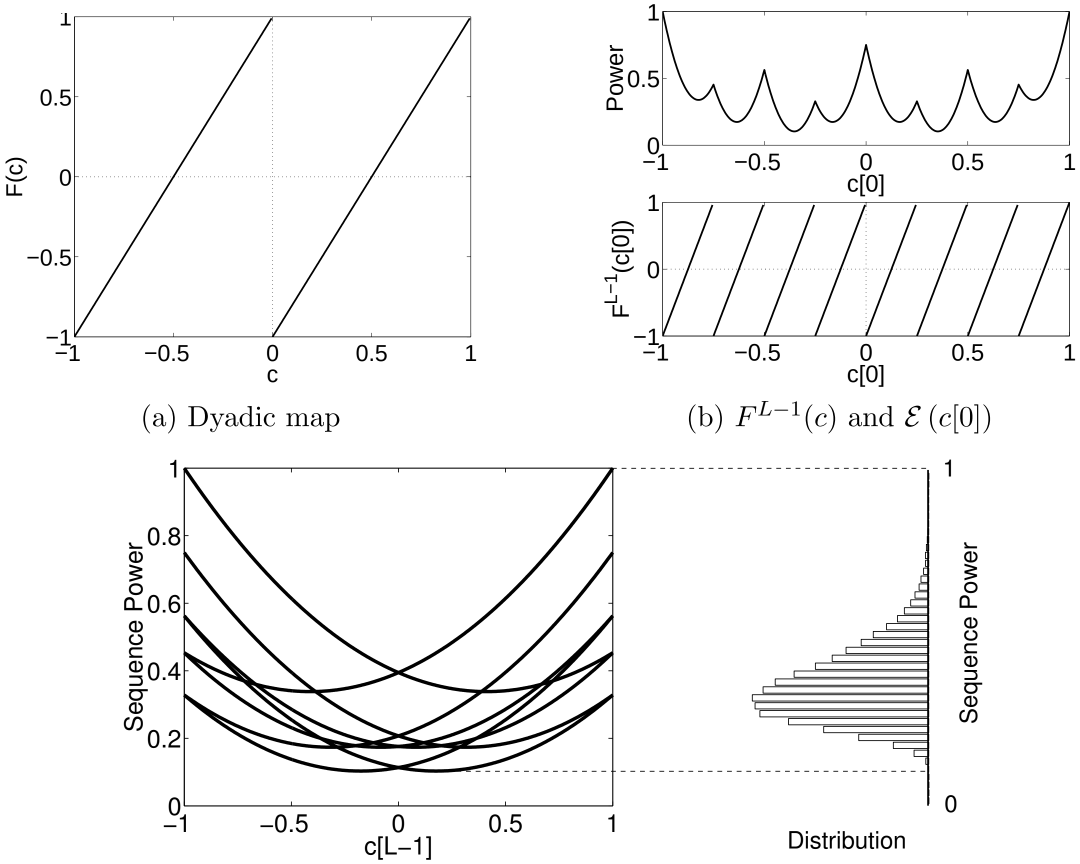
and

$$x = F_s^{-1}(y) = \frac{\zeta_s \cdot y + s}{P}. \tag{2.16b}$$

As (2.16) reveals, any map within this class is fully characterized by the vector (2.12).

### 2.2.2 Sequence Power Characteristics

We next focus on the probability density function (PDF) of the power of length-$L$ sequences, and, in particular, its relation to features of the chaotic map. These PDFs



(a) Dyadic map

(b) $F^{L-1}(c)$ and $\mathcal{E}\left(c[0]\right)$

(c) $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ and $\mathcal{E}\left(\mathbf{c}^{L}\right)$ distribution

Figure 2.4: Dyadic map and its sequence power characteristics for $L = 4$.

play a key role in the probability of error performance of intended receivers.

Due to (2.11), the power of a length-$L$ chaotic vector $\mathbf{c}^L$ can be viewed as a function of the vector $\mathbf{c}^L$, the initial condition $c[0]$, or, alternatively, $\{\mathbf{s}^{L-1},\, c[L-1]\}$. Hence, with a slight abuse of notation, we have

$$\mathcal{E}\left(\mathbf{c}^L\right) = \mathcal{E}\left(c[0]\right) = \mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right) = \frac{1}{L}\sum_{n=0}^{L-1} c^2[n] \ . \tag{2.17}$$

Fig. 2.4 shows the dyadic map, its $(L-1)$-fold composition, $F^{L-1}(c)$, and the power of $\mathbf{c}^L$, first vs. $c[0]$ in Fig. 2.4 (b), and then vs. $c[L-1]$ for all possible $\mathbf{s}^{L-1}$ in

Fig. 2.4 (c). Each quadratic segment of $\mathcal{E}\left(c[0]\right)$ and $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ corresponds to a unique itinerary vector $\mathbf{s}^{L-1}$. We remark that the curvatures of the $\mathcal{E}\left(c[0]\right)$ curves grow exponentially with $L$, while those of $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ remain bounded as $L \to \infty$.

All $P$-partition maps with the same number of partitions $P$ have the same power PDF. For any pair of distinct $P$-partition maps $F(\cdot)$ and $G(\cdot)$ with the same $P$, using (2.16a) we can readily verify that[2]

$$F_{s(c)}(c) = \pm G_{s(c)}(c)\,.$$

Moreover, using (2.7) we can readily show that

$$F_{s(-c)}(-c) = \pm F_{s(c)}(c).$$

Consequently, for any pair of sequences generated by propagating the same initial condition through two distinct $P$-partition maps $F(\cdot)$ and $G(\cdot)$ with the same $P$, we have

$$\begin{bmatrix} c & F(c) & F^2(c) & \cdots & F^{L-1}(c) \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} c & \pm G(c) & \pm G^2(c) & \cdots & \pm G^{L-1}(c) \end{bmatrix}^{\mathrm{T}}, \tag{2.18}$$

showing, indeed, that the PDF of $\mathcal{E}\left(\mathbf{c}^L\right)$ depends only on the number of partitions, $P$, and not on the sign vector $\zeta$ associated with the particular map. In addition, all $P$-partition maps have the same average sequence power; $E\left[\mathcal{E}\left(\mathbf{c}^L\right)\right] = 1/3$, where $E\left[\cdot\right]$ denotes expectation. Thus, for the sequences from these maps, $A = \sqrt{3}$ in (2.1).

Finally, the minimum sequence power, $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$, is also of interest as it

[2] We employ the notation $y = \pm x$ to denote $y = +x$ or $-x$.

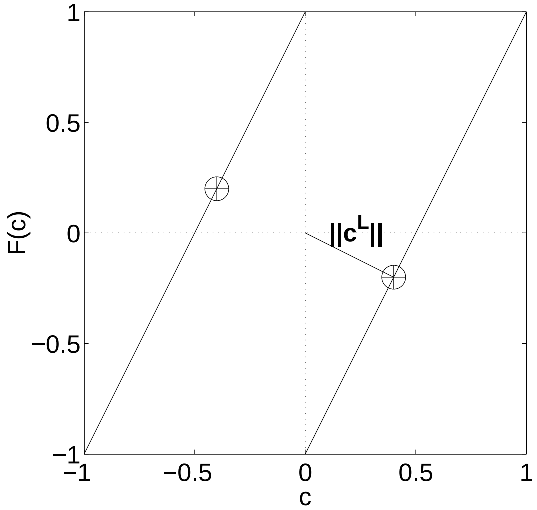


Figure 2.5: Sequences with minimum sequence power for dyadic map and $L = 2$. $\oplus$ marks correspond to the sequences with minimum $\left\|\mathbf{c}^L\right\|$.

greatly affects the intended receiver $\Pr(\epsilon)$. Since $\mathcal{E}\left(\mathbf{c}^L\right) = \left\|\mathbf{c}^L\right\|^2/L = \left\|\mathbf{c}^L - \mathbf{0}\right\|^2/L$, where $\|\cdot\|$ denotes $\mathcal{L}_2$-norm, $\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right)$ is attained by the sequences with $\min\left\|\mathbf{c}^L\right\|$, *i.e.*, those that are closest to the $L$-dimensional origin. This is graphically illustrated in Fig. 2.5 for the dyadic map. Since $P$-partition maps with odd $P$ pass through the origin, $\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right) = 0$ for these maps. $P$-partition maps with even $P$ do not pass through the origin and, hence, exhibit a nonzero $\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right)$. As $L \to \infty$, these $\min\left\|\mathbf{c}^L\right\|$ sequences rapidly approach fixed or period-2 trajectories with sample values from $\left\{+\frac{1}{P+1}, -\frac{1}{P+1}\right\}$. Consequently,

$$\lim_{L\to\infty}\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right) = \left(\frac{1}{P+1}\right)^2, \quad P \text{ even}\,. \tag{2.19}$$

As a result, over all $P$-partition maps, $\min\mathcal{E}\left(\mathbf{c}^L\right)$ is maximum for $P = 2$, corresponding to the tent map and the dyadic map.

## 2.3 Digital Realization of Sequences from $P \times Q$ Partition Maps

In this section, we examine some of the issues that arise in digital realizations of sequences from $P \times Q$ partition maps, and develop implementation methods for a class of these maps that address these issues. Digital realization of chaotic systems is necessary to ensure that the number of bits representing $c[0]$ is finite, allowing efficient digital transmission of the key. Quantization of a real-valued initial condition for analog circuit implementations does not ensure reliable communication, since the chaotic sequence generated by the receiver with quantized initial condition exponentially diverges from the actual spreading sequence used in modulation. Digital realization also avoids a potential problem in analog implementation, where even infinitisimal inconsistency in the physical emulations of a given map for a pair of transmitter and receiver results in different spreading sequences for the pair with the same $c[0]$. These digital implementations are dynamical systems over finite-cardinality domains, and can thus be viewed as finite state machine realizations of $P \times Q$ partition maps. As each digitized sequence from such a dynamical system is equivalent to a series of output states from a finite state machine, it is inherently periodic (thereby not chaotic), and hence, it cannot, in a strict sense, exhibit sensitive dependence on initial conditions in the long term [21]. If properly designed, however, digitized sequences with enormous periods can be generated that retain, in some sense, many of the important properties of the chaotic trajectories of interest. We demonstrate such design methods, first for the class of $r$-adic maps, then for a class of odd $P \times Q$ partition maps.

Brute-force digital realizations of piecewise-linear chaotic maps can yield systems with undesirable dynamics. This can be illustrated by considering digital realizations of $r$-adic maps

$$\tilde{F}(x) = r\,x \mod 1\,,\ x \in [0,1]\,,$$

where $x \mod a$ denotes the nonnegative remainder of $x/a$. Given a numerical precision depth of $B$ bits, a straightforward realization method exploiting the maximum number of quantization levels can be effectively viewed as a mapping of the form

$$G(x) \overset{\triangle}{=} r\,x \mod 2^B\,, \tag{2.20}$$

where $x \in \left\{0, 1, 2, \ldots, 2^B - 1\right\}$. Propagating any initial condition $x$ through (2.20) yields a fixed point of the map after a finite number of iterations. For instance, in the case $r = 2$, the maximum possible number of iterations before reaching a fixed point is $B + 1$. Evidently, this type of brute-force realization in general does not preserve the invariant density, exactness, broadband characteristics, and sensitivity to initial conditions of the original map.

Certain key properties of chaotic sequences can, in some sense, be preserved via properly constructed digitized realizations. In particular, consider $r$-adic map implementations of the form

$$G(x) = r\,x \mod q\,, \tag{2.21}$$

where $x \in \mathcal{S}_Q \overset{\triangle}{=} \{0,\ 1,\ \cdots\ ,\ q-1\}$ and $q$ is a suitably chosen prime such that $q < 2^B$. An attractive attribute of implementations of the type (2.21) is that, under modulo $q$ addition and multiplication, the integer set $\{0,\ 1,\ \cdots\ ,\ q-1\}$ forms a Galois Field of

| $B$ | dyadic map | 3-adic map | $2^B$ |
|---:|---:|---:|---:|
| 8 | 227 | 233 | 256 |
| 12 | 4093 | 4073 | 4096 |
| 16 | 65371 | 65419 | 65536 |
| 24 | 16776989 | 16777183 | 16777216 |
| 32 | 4294967291 | 4294967188 | 4294967296 |
| 48 | 281474976710597 | 281474976710597 | 281474976710656 |
| 64 | 18446744073709551557 | 18446744073709551557 | 18446744073709551616 |

Table 2.1: The largest prime $q$, $q < 2^B$, such that nonzero sequences from (2.21) have period $q-1$, for $r = 2$ (dyadic map) and $r = 3$ (3-adic map).

order $q$, GF($q$). As a result, if the prime $q$ is chosen such that $r$ is a primitive element in GF($q$), then (2.21) yields $q-1$ maximal-length sequences $G^{(n)}(x)$ with period $q-1$, for all initial conditions except for $x = 0$ [22].

Implementations of the form (2.21) with $r$ a primitive element of GF($q$) have several attractive properties. First, the sequences arising from nonzero initial conditions are exact and ergodic, and possess uniform invariant probability mass functions (PMFs) on their restriction on $\mathcal{S}_{Q'} \overset{\triangle}{=} \{1, 2, \cdots, q-1\}$. Furthermore, from the unintended receiver's point of view, these sequences can retain the sensitive dependence on initial conditions of the original chaotic map, in the sense that the combined effect of sufficient quantization depth and channel noise can render the space spanned by these digitized sequences effectively indistinguishable from the space spanned by the real-valued chaotic trajectories. Consequently, the performance of intended and unintended receivers in the context of DS/SS systems exploiting such pseudochaotic sequences can be evaluated via analysis techniques that are developed for their chaotic counterparts. Thus, in the following chapters of this dissertation, we investigate the receiver Pr($\epsilon$) performance characteristics in the context of original chaotic DS/SS systems.

Table 2.1 shows the largest prime $q$ such that $r$ is a primitive element of $\mathrm{GF}(q)$, as a function of the precision depth $B$ for $r$-adic maps with $r = 2, 3$. As the table reveals, $q$ is very close to $2^B$ for all $B$ values in the figure, demonstrating that indeed this type of implementation can provide digitized sequences with enormous periods for sufficiently large $B$. We note that, while empirical methods for finding a suitable $q$ may be sufficient, as one such $q$ may suffice in designing a chaotic DS/SS system, algorithms for systematically generating such $q$'s as a function of the precision depth and $r$ are important in their own right and warrant further investigation.

An important class of odd-symmetric $P \times Q$ partition map-based digital sequences can be generated from systematic modifications of their $r$-adic counterparts described above. In particular, we consider odd $P \times Q$ partition maps $H$ that arise as a composition of a masking map $M$ and an $r$-adic map $G$ in the form of (2.21) with a suitably chosen prime $q$, *i.e.*, $H \overset{\triangle}{=} M \circ G$. For a class of masking maps in the following theorem, this composition generates maximal-length sequences $H^{(n)}(x)$ with least period $q - 1$ for all nonzero initial conditions $x \in \mathcal{S}_{Q'}$:

**Theorem 1.** *Let the following conditions hold for* $G : \mathcal{S}_Q \to \mathcal{S}_Q$ *and* $M : \mathcal{S}_Q \to \mathcal{S}_Q$, *where* $\mathcal{S}_Q = \{0, 1, \cdots, q-1\}$.

*(i)* $G(\cdot)$ *is maximal length for all nonzero initial conditions, i.e., given the quantization depth* $q$, $q - 1$ *is the smallest* $n$ *for which* $G^{(n)}(x) = x, x \in \mathcal{S}_{Q'}$, *where* $\mathcal{S}_{Q'} = \{1, 2, \cdots, q-1\}$.

*(ii)* $G(\cdot)$ *is odd, i.e.,* $G(x) = q - G(q - x)$ *for all* $x \in \mathcal{S}_{Q'}$.

*(iii)* $M(\cdot)$ *is odd, i.e.,* $M(x) = q - M(q - x)$ *for all* $x \in \mathcal{S}_{Q'}$.

*(iv) For each* $x \in \mathcal{S}_{Q'}$, *either* $M(x) = x$ *or* $M(x) = q - x$.

*(v) the number of elements in* $\mathcal{S}_{Q'}$ *for which* $M(x) = q - x$ *is a multiple of* 4.

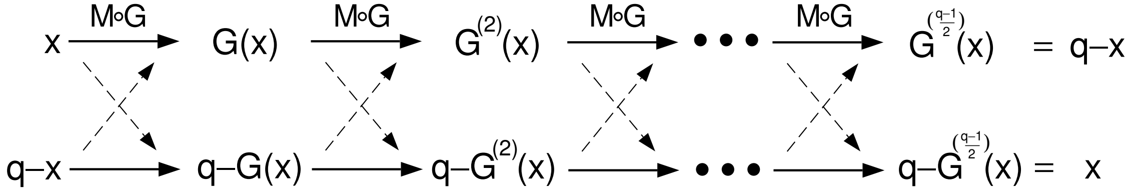


Figure 2.6: Finite states representation of $(M \circ G)^{(n)}(x)$. Solid arrows correspond to $M(x) = x$ (2.23a) and dashed arrows correspond to $M(x) = q - x$ (2.23b), for $x \in \mathcal{S}_{Q'}$.

*Then,* $H(x) = (M \circ G)(x)$ *is odd and maximal length for all* $x \in \mathcal{S}_{Q'}$.

*Proof.* First, $H(\cdot)$ is odd since it is the composition of two odd maps. Next we prove that $H(\cdot)$ is maximal length. From condition (ii), we have

$$G^{(n)}(q - x) = q - G^{(n)}(x)\,. \tag{2.22}$$

From conditions (iii) and (iv) and (2.22) we have, for all $x \in \mathcal{S}_{Q'}$ and integer $n \geq 0$,

$$M(G^{(n)}(x)) = G^{(n)}(x) \text{ if and only if } M(q - G^{(n)}(x)) = q - G^{(n)}(x)\,, \tag{2.23a}$$

and

$$M(G^{(n)}(x)) = q - G^{(n)}(x) \text{ if and only if } M(q - G^{(n)}(x)) = G^{(n)}(x)\,. \tag{2.23b}$$

The maximal-length condition (i) and (2.23) imply that $G^{(\frac{q-1}{2})}(x) = q - x$, and in general, $G^{(\frac{q-1}{2}+n)}(x) = q - G^{(n)}(x)$. The effect of the masking operation $M$ on the finite state machine realization of $G$ is illustrated in Fig. 2.6. In this figure, each arrow represents an application of the mapping $(M \circ G)(\cdot)$. Specifically, solid arrows correspond to the case $M(G^{(n)}(x)) = G^{(n)}(x)$, and dashed arrows correspond to the case $M(G^{(n)}(x)) = q - G^{(n)}(x)$, for $x \in \mathcal{S}_{Q'}$. As can be deduced from the figure, for

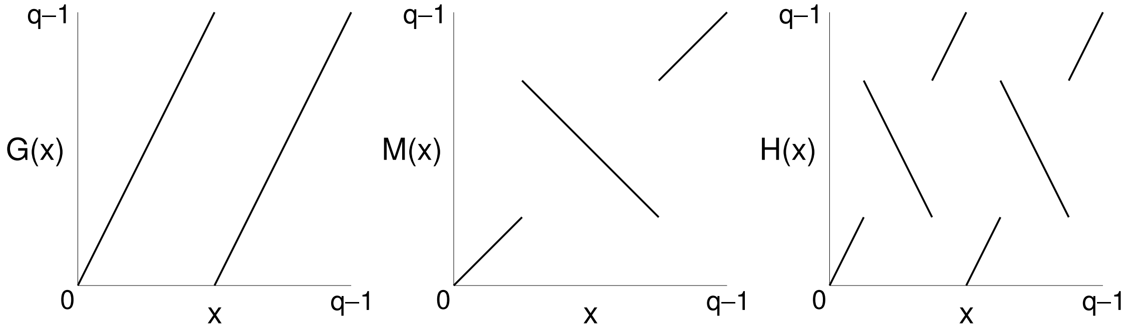


Figure 2.7: An example masking operation on an $r$-adic map. $G(x)$ is the dyadic map, $M(x)$ is a masking map satisfying the conditions in Theorem 1, and $H(x) = M \circ G(x)$ is the output map of masking.

$H^{(n)}(x) = (M \circ G)^{(n)}(x)$ to be maximal length, the number of $n \in \{1,\ 2,\ \cdots,\ \frac{q-1}{2}\}$ for which $M(G^{(n)}(x)) = q - G^{(n)}(x)$ (dashed arrows) need be an even number. Due to the relationships in (2.23a) and (2.23b), the same holds for $n \in \{\frac{q-1}{2}+1,\ \frac{q-1}{2}+2,\ \cdots,\ q-1\}$, thus this sufficient condition is equivalent to the condition (v). Therefore $H(x)$ is maximal length for all $x \in \mathcal{S}_{Q'}$. □

The class of maps $H(\cdot) = (M \circ G)(\cdot)$ in Theorem 1, where $G(\cdot)$ is an $r$-adic map of the form (2.21) that generates maximal-length sequences, retains many important attributes of the digitized $r$-adic maps $G(\cdot)$, in addition to the least period $q-1$ and odd symmetry. In particular, the sequences $H^{(n)}(x)$, $x \in \mathcal{S}_{Q'}$ are exact and ergodic, and possess uniform invariant densities. As Fig. 2.7 suggests, the composition of a suitably designed masking map with an $r$-adic map can be used to construct a wide range of potentially useful odd $P \times Q$ partition maps.

## Chapter 3

# Analysis and Design of Pseudochaotic DS/SS Systems: AWGN Channels

In this chapter, we focus on developing algorithmic design methods for pseudochaotic DS/SS systems with the desired level of communication privacy in the case of single-user communications over AWGN channels. This instructive special case captures many of the key performance and design issues that arise in the context of private and reliable multiuser communication over fading channels. The block diagram of the single-user chaotic DS/SS transmitter, a specialization from the general model in Fig. 2.1 and shown previously in Fig. 1.2, is repeated in Fig. 3.1 for convenience, with the redundant subscripts suppressed. In this case, the transmitted signal at time $n$ in (2.2) simplifies to

$$x[n] = x\left[n; c, b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\right] = \frac{A}{\sqrt{L}} F^n(c)\; b\left[\left\lfloor\frac{n}{L}\right\rfloor\right] \,, \tag{3.1}$$

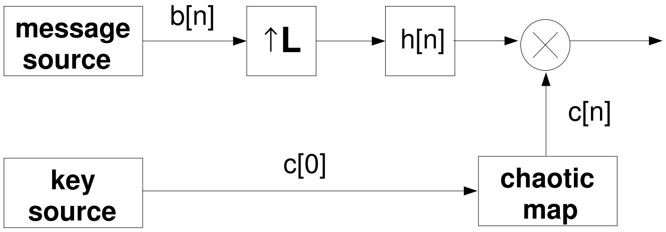


Figure 3.1: Block diagram of a chaotic DS/SS modulator.

and the intended and unintended users' received signal (2.3) reduces to

$$\begin{aligned} y[n] &= x[n] + w[n] \\ &= \frac{A}{\sqrt{L}} F^n(c)\; b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] + w[n]\,. \end{aligned} \tag{3.2}$$

In this chapter, we initially focus on the class of chaotic DS/SS systems based on $P$-partition maps in Chapter 2, and characterize the single-user communication privacy for the signal (3.2). We deduce the relationships between the level of privacy and various system parameters. These relationships are then exploited to establish systematic methods for designing DS/SS systems based on $P \times Q$ partition maps that meet a required privacy strength.

We first investigate the $\Pr(\epsilon)$ performance for the intended receiver in Section 3.1. Specifically, we develop $\Pr(\epsilon)$ expressions and bounds, and infer connections between $\Pr(\epsilon)$ performance and various system parameters. As we show, the intended receiver of the pseudochaotic DS/SS transmission with suitably chosen chaotic maps has effectively identical $\Pr(\epsilon)$ performance as that of conventional DS/SS systems for spreading gains of practical interest.

In designing chaotic DS/SS with attractive privacy benefits, it is important to understand how the behavior of a primary privacy metric, *i.e.*, the unintended receiver $\Pr(\epsilon)$, depends on the controllables, *i.e.*, system parameters. In Section 3.2

we develop bounds and approximations to the unintended receiver $\Pr(\epsilon)$, and identify the features of chaotic maps that affect the associated receiver $\Pr(\epsilon)$. As we show, such relationships between unintended receiver performance and chaotic map features naturally suggest a subclass of $P$-partition maps with attractive privacy benefits. For this class of maps, we demonstrate that, at high signal-to-noise ratio (SNR), the unintended receiver $\Pr(\epsilon)$ curves decay at a rate of $1/\sqrt{\text{SNR}}$, in sharp contrast to the exponential decay rate exhibited by the intended receiver $\Pr(\epsilon)$.

To be able to establish private communication over a wide array of scenarios with different privacy requirements, it is desirable to have systematic system design methods, the associated privacy of which can be efficiently quantified based on a set of system parameters. Toward this goal, in Section 3.3 we build on our investigation in Section 3.2 to develop iterative design methods of DS/SS systems based on $P \times Q$ partition maps that systematically degrade the unintended receiver $\Pr(\epsilon)$ while maintaining intended user performance. For a subset of these systems, we obtain expressions for predicting the relations between the unintended receiver $\Pr(\epsilon)$ and system parameters.

An important factor that must be considered in constructing operational pseudochaotic DS/SS systems on digital platforms is the impact such numerical implementations of chaotic spreading sequences have on communication privacy. In Section 3.4, we deduce the range of digital implementation parameters for which the unintended receiver performance for suitably constructed pseudochaotic DS/SS accurately approximates that for the underlying chaotic DS/SS systems. In the process we show that the class of pseudochaotic DS/SS we develop can provide attractive privacy benefits to intended receivers under a wide range of system parameters of practical interest.

## 3.1 Intended Receiver Performance

In the following we develop numerically efficient methods for evaluating the $\Pr(\epsilon)$ performance of intended receivers for DS/SS communication with $P$-partition maps in AWGN, and determine the relationship between system and map parameters and the $\Pr(\epsilon)$ of these receivers.

From the viewpoint of an intended receiver that knows the initial condition, chaotic spreading is equivalent to linearly modulating the message bit stream on a *known* time-varying shaping waveform. Consequently, the minimum $\Pr(\epsilon)$ receiver is a symbol-by-symbol detector consisting of a time-varying matched filter followed by sampling and a threshold detector. The (instantaneous) received bit SNR associated with a specific spreading vector $\mathbf{c}^L$ is given by

$$\gamma_b = A^2 \frac{\mathcal{E}_b}{N_o} \mathcal{E}\left(\mathbf{c}^L\right) = \frac{A^2}{L} \cdot \frac{\mathcal{E}_b}{N_o} \sum_{n=0}^{L-1} c^2[n] \ , \tag{3.3}$$

where we set $A = \sqrt{3}$ for all $P$-partition maps. As $c[n]$ is an ergodic sequence for almost all initial conditions [20],

$$\Pr(\epsilon) = E\left[\mathcal{Q}\left(\sqrt{2\gamma_b}\right)\right] = \int \mathcal{Q}\left(\sqrt{\frac{6\,\mathcal{E}_b\,\mathcal{E}\left(c\right)}{N_o}}\right) p_{c[0]}(c)\, dc\,, \tag{3.4}$$

where $\mathcal{Q}\left(\nu\right) = 1 - \mathcal{F}(\nu)$, where $\mathcal{F}(\cdot)$ denotes the cumulative distribution function of the standard Gaussian PDF, *i.e.*,

$$\mathcal{Q}\left(\nu\right) = \frac{1}{\sqrt{2\pi}} \int_{\nu}^{\infty} e^{-\frac{t^2}{2}} dt\,, \tag{3.5}$$

and where $p_{c[0]}(\cdot)$ denotes the invariant density, which, for any $P$-partition map, is uniform in $[-1,\, 1]$. We remark that the integral (3.4) has no closed form solution. Furthermore, the number of intervals required for numerical integration grows exponentially with $L$, as Fig. 2.4 (b) suggests. These integrals are characterized by exponentially decreasing widths and integrands with curvatures exponentially increasing in $L$, leading to numerically sensitive computation algorithms of (3.4).

An alternative expression to (3.4) can be obtained by replacing $\mathcal{E}\left(c[0]\right)$ with $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$ and using the fact that $c[L-1]$ is uniformly distributed on $I$,

$$\begin{aligned} \Pr(\epsilon) &= E\left[E\left[\mathcal{Q}\left(\sqrt{\frac{6\,\mathcal{E}_b\,\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)}{N_o}}\right)\middle|\,\mathbf{s}^{L-1}\right]\right] \\ &= \frac{1}{2P^{L-1}}\sum_{i=1}^{P^{L-1}}\int_{-1}^{+1}\mathcal{Q}\left(\sqrt{\frac{6\,\mathcal{E}_b\,\mathcal{E}\left(\mathbf{s}_i, c\right)}{N_o}}\right)dc\,. \end{aligned} \tag{3.6}$$

Although (3.6) requires computation of a number of integrals that grows exponentially with $L$, unlike (3.4), it suggests well-behaved algorithms for numerical computation of the intended receiver $\Pr(\epsilon)$, as each $\mathcal{E}\left(\mathbf{s}^{L-1} = \mathbf{s}_i, c[L-1]\right)$ curve in (3.6) has bounded curvature for all $L$. Furthermore, (3.6) suggests computationally efficient approximations based on equivalence classes of itineraries with similar $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$'s. In particular, we can define equivalence classes, according to which, any two itineraries $\mathbf{s}_1$ and $\mathbf{s}_2$, whose ordered elements are permutations of each other, are viewed as members of the same class. We select a random set of class representatives by choosing exactly one random sample itinerary $\mathbf{s}_e$ from each equivalence class. The contribution of a class representative on $\Pr(\epsilon)$ is then scaled by the number of distinct itineraries in the associated equivalence class. It can be shown that, for the case $P = 2$, each set of $\mathcal{E}\left(\mathbf{s}^{L-1}, c[L-1]\right)$'s conditioned on itineraries of an equivalence class forms a dense subset of the sequence power PDF with little overlap with other sets, and, hence,

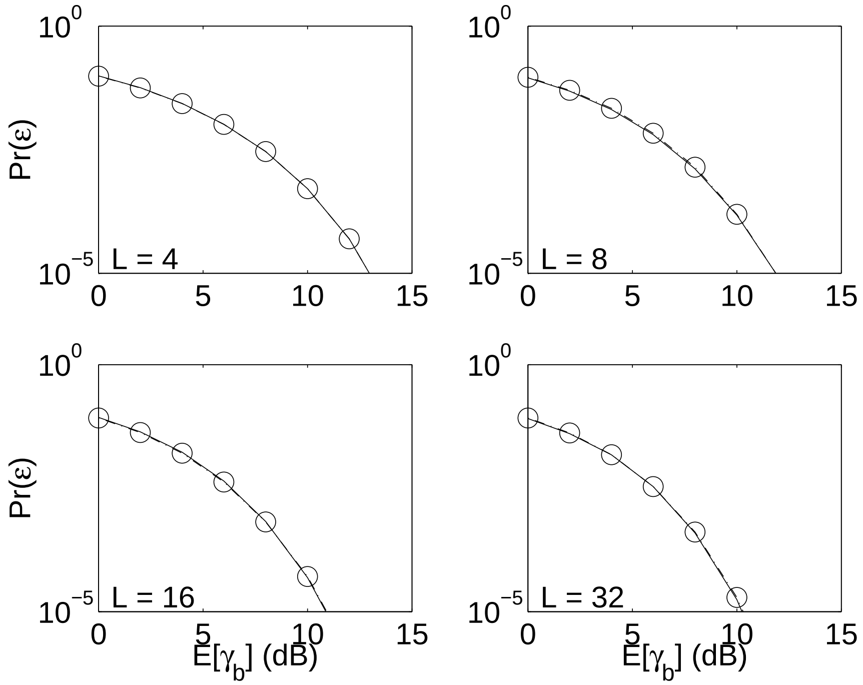


Figure 3.2: Accuracy of itinerary distribution approximation of intended receiver $\Pr(\epsilon)$ for $P = 2$. Solid curves represent analytically computed $\Pr(\epsilon)$ expression (3.6), and dashed curves with circles represent analytically computed $\Pr(\epsilon)$ approximation (3.7).

members of an equivalence class yield similar conditional $\Pr(\epsilon)$ characteristics. As demonstrated in Fig. 3.2, for $P = 2$, this approximation yields an accurate estimate of $\Pr(\epsilon)$, which is given by

$$\Pr(\epsilon) \approx \frac{1}{2^L} \sum_{e=0}^{L-1} \binom{L-1}{e} \int_{-1}^{+1} \mathcal{Q}\left(\sqrt{\frac{2\mathcal{E}_b\, \mathcal{E}\left(\mathbf{s}_e, c\right)}{N_o}}\right) dc\,, \tag{3.7}$$

where $e$ corresponds to the number of $-1$'s (or $+1$'s) in an itinerary $\mathbf{s}^{L-1}$. While extensions of this approximation to higher $P$ as well as other types of equivalence classes certainly merit further investigation, they are outside the scope of this dissertation.

Upper and lower bounds that are independent of $L$ can serve as figures of merit for assessing the asymptotic $\Pr(\epsilon)$ characteristics of intended receivers. Specifically, we have

$$\mathcal{Q}\left(\sqrt{2\overline{\gamma}_b}\right) \leq \Pr(\epsilon) \leq \mathcal{Q}\left(\sqrt{\frac{6\,\mathcal{E}_b \min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)}{N_o}}\right) , \tag{3.8}$$

where $\overline{\gamma}_b = E\left[\gamma_b\right] = \mathcal{E}_b/N_o$ is the average bit SNR. The lower bound in (3.8) is obtained using Jensen's inequality [23] and the fact that $\mathcal{Q}\left(\cdot\right)$ is convex, and corresponds to the optimum $\Pr(\epsilon)$ for antipodal signaling using binary-valued PN spreading sequences in AWGN, while the upper bound is due to $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right) \leq \mathcal{E}\left(\mathbf{c}^L\right)$. For DS/SS systems using $P$-partition maps with odd $P$, the upper bound in (3.8) reduces to 1/2, since $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right) = 0$. For DS/SS systems using maps with even $P$, $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$ rapidly converges to its limiting value (2.19) as $L$ increases. Consequently, over a wide range of spreading gains, the upper bound in (3.8) is well approximated by its limiting value

$$\lim_{L\to\infty} \Pr(\epsilon) \leq \mathcal{Q}\left(\frac{\sqrt{6\,\overline{\gamma}_b}}{P+1}\right), \quad P \text{ even}\,. \tag{3.9}$$

The spreading gain, $L$, the number of map partitions, $P$, and $\overline{\gamma}_b$ are the only parameters affecting the intended receiver $\Pr(\epsilon)$, as, due to (2.18), the codeword power PDF is independent of the sign vector $\zeta$. Figs. 3.3 and 3.4 show typical $\Pr(\epsilon)$ curves vs. SNR as functions of $L$ and $P$. As Fig. 3.3 reveals, the $\Pr(\epsilon)$ is a decreasing function of $L$, converging to the lower bound in (3.8) as $L \to \infty$. The curves on Fig. 3.4 are consistent with the upper bound in (3.8). Specifically, the $\Pr(\epsilon)$ for any odd-$P$ map does not decay exponentially with SNR, as $\min \mathcal{E}\left(\mathbf{c}^L\right) = 0$.[1] This is reminiscent of $\Pr(\epsilon)$ performance over fading channels. Indeed, chaotic spreading can in some sense be viewed as inducing a known (strongly dependent) fading process on a bit stream modulated on a rectangular spreading code. In contrast to the odd $P$ cases,

[1] Using an argument similar to the one used in Section 3.2.3, we can show that the intended receiver $\Pr(\epsilon)$ for any DS/SS with spreading sequences from $P$-partition maps with odd $P$, decays at best as $1/\sqrt{\overline{\gamma}_b}$.

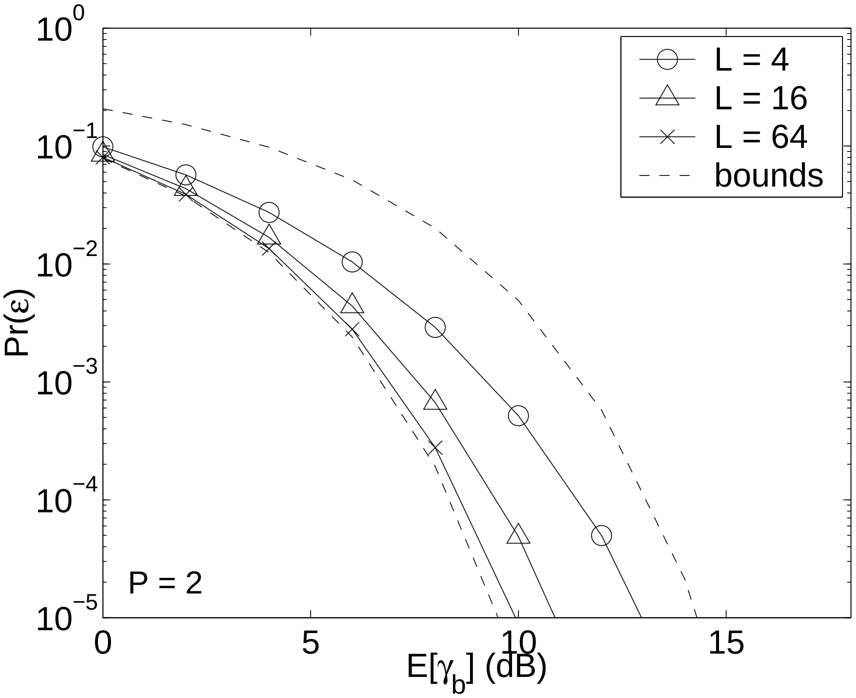


Figure 3.3: Intended receiver $\Pr(\epsilon)$ performance vs. SNR for various spreading gain $L$. Solid curves indicate analytically computed $\Pr(\epsilon)$'s and dashed curves indicate the lower and upper bounds for a given number of partitions.

the intended receiver $\Pr(\epsilon)$ for any even-$P$ map decays exponentially with SNR, as $\min \mathcal{E}\left(\mathbf{c}^L\right) > 0$. Furthermore, the tent and dyadic map-based systems ($P = 2$) have the best $\Pr(\epsilon)$ performance, consistent with the fact that they provide the spreading sequences with the largest $\min \mathcal{E}\left(\mathbf{c}^L\right)$. However, this property does not necessarily render these maps the most attractive for achieving privacy, as it does not take into account the $\Pr(\epsilon)$ trends of unintended receivers.

## 3.2 Unintended Receiver Performance

In this section we characterize the unintended receiver $\Pr(\epsilon)$ for DS/SS signaling with a class of $P \times Q$ partition maps and determine the system attributes that affect the unintended receiver $\Pr(\epsilon)$. In particular, we develop computationally viable methods

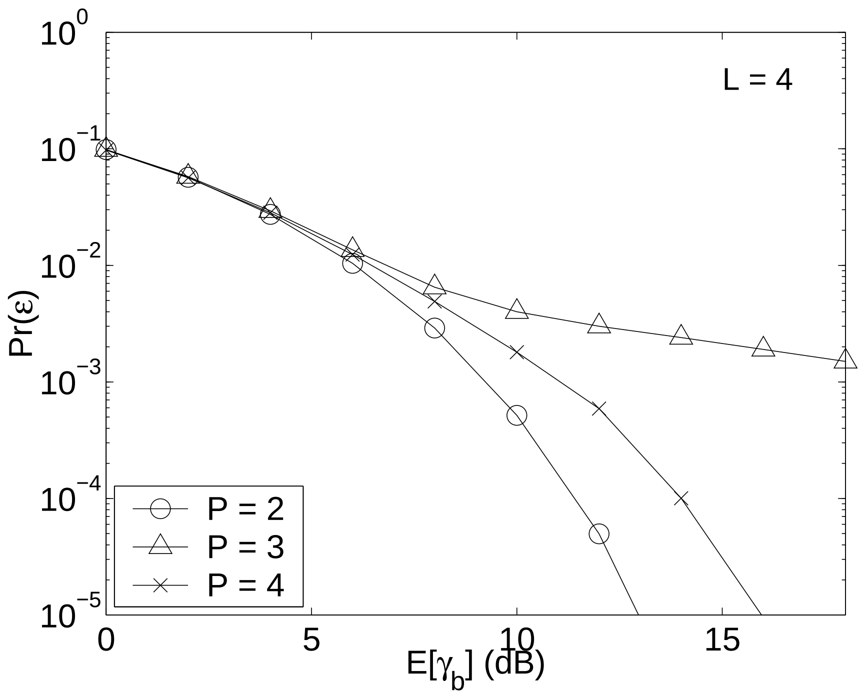


Figure 3.4: Intended receiver $\Pr(\epsilon)$ performance vs. SNR for various number of partitions $P$.

for evaluating the unintended receiver $\Pr(\epsilon)$ associated with $P$-partition map-based chaotic spreading, and identify the major factors that dictate the $\Pr(\epsilon)$ performance. In the process, we formulate a class of maps that provide the strongest privacy benefits among all $P$-partition maps. For this class of maps, we establish a lower bound on the asymptotic decaying rate of unintended receiver $\Pr(\epsilon)$ vs. SNR. Finally, we exploit the factors affecting the unintended receiver $\Pr(\epsilon)$ to develop computationally efficient simulation-based approximations to the $\Pr(\epsilon)$ for a class of $P \times Q$ partition maps. We assume that the unintended receiver has complete knowledge of the modulation scheme including the chaotic map, but does not know the initial condition $c[0]$.

### 3.2.1 Performance Evaluation for $P$-partition Maps

In the following we develop numerically efficient lower and upper bounds on the $\Pr(\epsilon)$ performance of the optimum maximum-likelihood (ML) sequence detector given the noisy observation (3.2) but not $c[0]$.

As the unintended receiver does not know the key, $c[0]$, it faces a composite hypothesis testing problem; under each (message sequence) hypothesis the observed sequence is a signal term in AWGN, whereby the signal term is a random vector with statistical characterization determined by the message hypothesis and the set of valid chaotic spreading sequences. In particular, we assume that

$$\mathbf{y} = \mathbf{y}^{NL} = \begin{bmatrix} y[0] & y[1] & \cdots & y[NL-1] \end{bmatrix}^{\mathrm{T}} \tag{3.10}$$

is observed, corresponding to a sequence of $N$ transmitted bits in (3.2), represented as

$$\mathbf{b} \triangleq \begin{bmatrix} b[0] & b[1] & \cdots & b[N-1] \end{bmatrix}^{\mathrm{T}} . \tag{3.11}$$

Then the maximum likelihood detector is given by

$$\begin{aligned} \hat{\mathbf{b}}_{\mathrm{ML}}(\mathbf{y}) &= \arg\max_{\mathbf{b}} \int p_{\mathbf{y}|\mathbf{b},c}(\mathbf{y}|\mathbf{b},c) p_{c[0]}(c)\, dc \\ &= \arg\max_{\mathbf{b}} \int \exp\left\{ \frac{1}{N_o} \sum_{n=0}^{NL-1} \left( 2\sqrt{\frac{3}{L}}\, y[n] F^n(c)\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] \right.\right. \\ &\qquad\qquad \left.\left. - \frac{3\,\mathcal{E}_b}{L} \left(F^n(c)\right)^2 \right) \right\} p_{c[0]}(c)\, dc. \end{aligned} \tag{3.12}$$

One can readily verify that, if $F$ is an odd map, $\mathbf{y}$ from (3.10) has the same statistical characterization under hypotheses $\mathbf{b} = \mathbf{b}_o$ and $\mathbf{b} = -\mathbf{b}_o$, and, hence, $p_{\mathbf{y}|\mathbf{b}}(\mathbf{y}|\mathbf{b}_o) = p_{\mathbf{y}|\mathbf{b}}(\mathbf{y}|-\mathbf{b}_o)$. As a result, even as $\overline{\gamma}_b \to \infty$, the optimal detector is

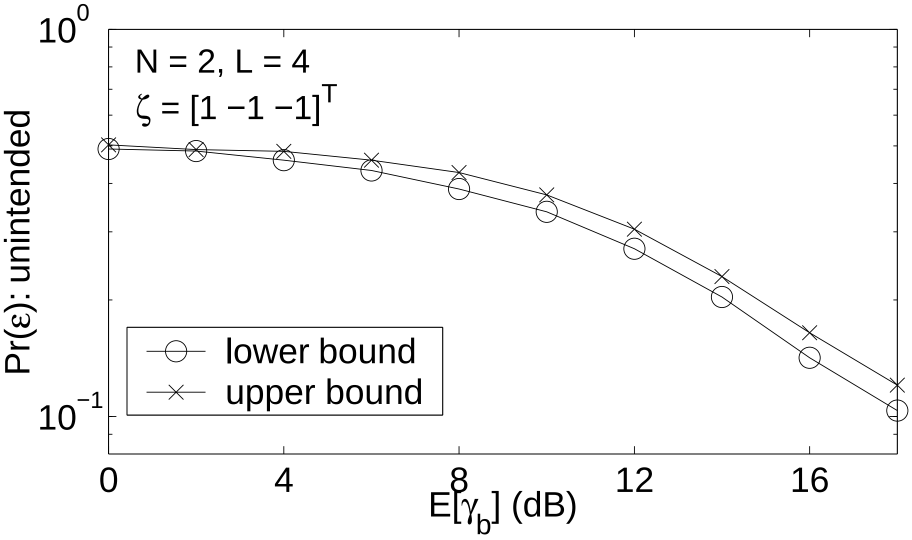


Figure 3.5: Upper and lower bounds for the unintended receiver performance.

unable to distinguish between the correct hypothesis and its antipodal. We therefore assume that there are only $N-1$ information bits to be distinguished, *i.e.*, each pair $\pm\mathbf{b}_o$ are merged into a single hypothesis, resulting in $2^{N-1}$ possible hypotheses, carrying $N-1$ information bits. For consistency, we apply this approach to intended and unintended receivers and all chaotic DS/SS systems, regardless of the chaotic map symmetry.

Direct implementation of (3.12) is impractical except for small values of $N$, $P$ and $L$, as each of the $2^{N-1}$ likelihoods requires $P^{NL}$ integral computations. As an alternative to exact $\Pr(\epsilon)$ evaluation, we develop lower and upper bounds that reflect the $\Pr(\epsilon)$ trends as a function of SNR and spreading gain. First, a numerically computable lower bound is obtained by simulating the optimum receiver in the case that, in addition to $\mathbf{y}$, the receiver has side information available in the form of the set $\{+c[NL-1], -c[NL-1]\}$. Associated with each member of this set is a finite set of possible initial conditions $\{c_m[0], m = 1, 2, \ldots, P^{NL-1}\}$, effectively transforming the uniform PDF of $c[0]$ to a posterior probability mass function (PMF) of $2P^{NL-1}$

impulses. The associated ML detector is given by

$$\begin{aligned}\hat{\mathbf{b}}_{\text{LB}}(\mathbf{y}) &= \arg\max_{\mathbf{b}} \sum_{m=1}^{2P^{NL-1}} \exp\left\{ \frac{1}{N_o} \sum_{n=0}^{NL-1} \left( 2\sqrt{\frac{3}{L}}\, y[n] F^n(c_{(m)}[0]) b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] \right.\right. \\ &\qquad \left.\left. - \frac{3\,\mathcal{E}_b}{L} \left(F^n(c_{(m)}[0])\right)^2 \right) \right\}. \qquad (3.13)\end{aligned}$$

A useful upper bound on the unintended receiver $\Pr(\epsilon)$ can be obtained by considering the performance of the following suboptimal generalized likelihood ratio test (GLRT) detector:

$$\begin{aligned}\hat{\mathbf{b}}_{\text{GLRT}}(\mathbf{y}) &= \arg\max_{\mathbf{b}} \max_{c[0]|\mathbf{b}} p_{\mathbf{y}|\mathbf{b},c[0]}(\mathbf{y}|\mathbf{b}, c) \\ &= \arg\min_{\mathbf{b}} \sum_{n=0}^{NL-1} \left( y[n] - \sqrt{\frac{3}{L}}\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] \hat{c}\left[n|NL-1, \mathbf{b}\right] \right)^2, \qquad (3.14)\end{aligned}$$

where $\hat{c}[n|k, \mathbf{b}_o]$ denotes the ML estimate of $c[n]$ based on $y[0], y[1], \cdots, y[k]$, given $\mathbf{b} = \mathbf{b}_o$. Accurate approximations of these estimates can be computed via extensions of the linear-complexity algorithm in [24], as elaborated in App. B.1. As Fig. 3.5 demonstrates for a typical $P$-partition map, the gap between the $\Pr(\epsilon)$ bounds based on (3.13) and (3.14) remains small over a wide range of SNR levels, revealing that these bounds can predict the $\Pr(\epsilon)$ trends of unintended receivers in practical settings.

### 3.2.2 Performance Dependence on System Parameters

In this section we utilize the $\Pr(\epsilon)$ metrics developed in Section 3.2.1 to deduce the dependence of the unintended receiver $\Pr(\epsilon)$ on system parameters.

Unlike the intended receiver case, in addition to the spreading gain and the number of map partitions, the unintended receiver $\Pr(\epsilon)$ is greatly affected by the

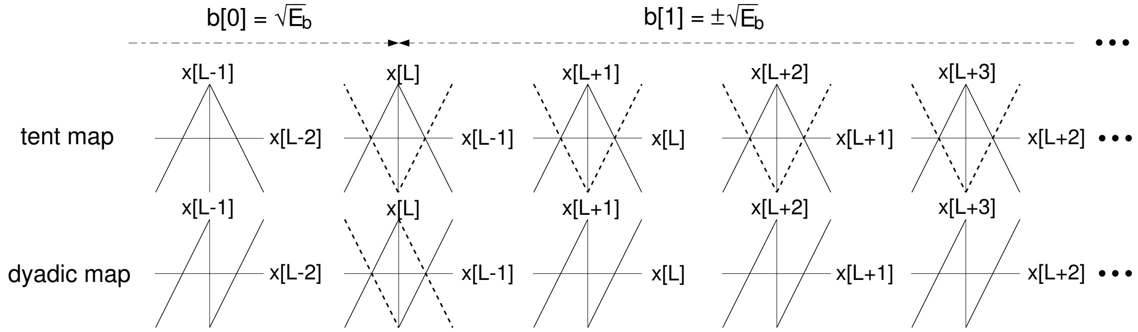


Figure 3.6: Pairwise signal trajectories for tent and dyadic map-based SS systems, in the cases $b[1] = b[0] = \sqrt{\mathcal{E}_b}$ (solid) and $b[1] = -b[0] = -\sqrt{\mathcal{E}_b}$ (dashed).

map slope signs $\zeta$ in (2.12). This can be illustrated by considering a vector $\mathbf{b}$ with $N = 2$, where it is known that $b[0] = \sqrt{\mathcal{E}_b}$. For convenience, we denote by $x[n]$ the signal-component samples, obtained by letting $w[n] = 0$ in (3.2), and consider the pairwise relation between successive signal samples for tent and dyadic map-based SS systems. Fig. 3.6 shows the associated signal pair trajectories when $b[1] = \sqrt{\mathcal{E}_b}$ (solid) and $b[1] = -\sqrt{\mathcal{E}_b}$ (dashed). As the figure reveals, unlike the tent map case where the two hypotheses are distinguishable throughout transmission of $b[1]$, in the dyadic map case, only the boundary pair $\{x[L-1], x[L]\}$ provides information for distinguishing between the two hypotheses. This effect is readily seen to be true for any odd map regardless of the number of partitions. A major consequence of this effect, combined with the sensitive dependence on initial conditions of chaotic trajectories, is that only a small number of symbols $x[n]$ around the codeword boundaries dominate the unintended receiver $\Pr(\epsilon)$, and this number does not grow with spreading gain. Thus, in general, odd maps are more attractive in terms of privacy potential than maps of even or no symmetry.

The optimal unintended receiver $\Pr(\epsilon)$ can vary among distinct odd $P$-partition maps. Since the optimal decision rules for systems utilizing odd maps are dominated by the pairs of observations at the bit transitions, insight can be gained by study-

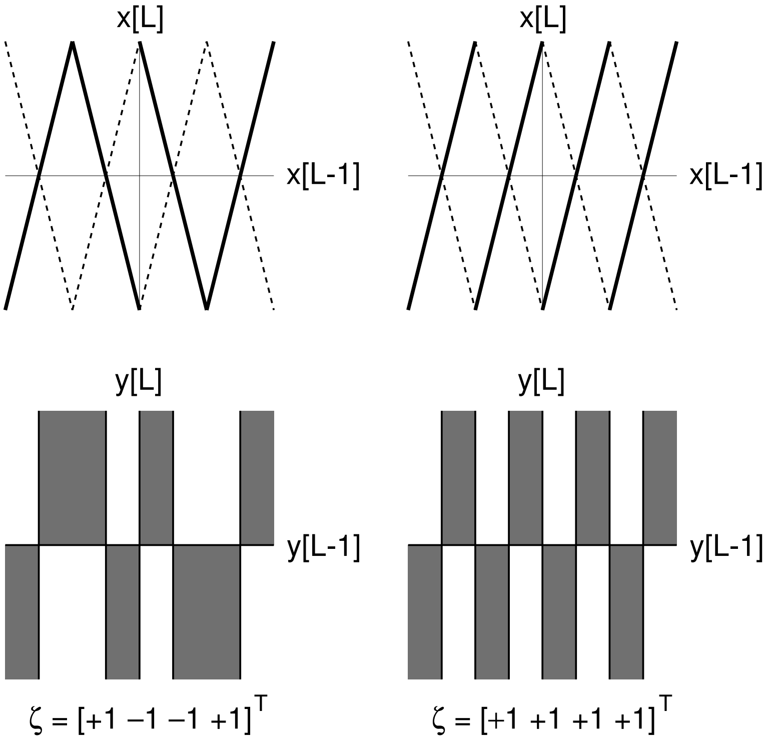


Figure 3.7: Upper graphs: valid signal trajectories ($x[L-1]$, $x[L]$) for two odd 4-partition maps, under hypotheses $b[0]=b[1]$ (solid), and $b[0] = -b[1]$ (dashed). Lower graphs: associated decision regions based on ($y[L-1]$, $y[L]$).

ing the decision regions of simplified rules that are solely based on such observation pairs. Such decision regions for two 4-partition odd maps are shown in Fig. 3.7. As the figure reveals, the $r$-adic map leads to a finer partition of strips of alternating decision regions and, thus, lower noise immunity, suggesting a higher unintended receiver $\Pr(\epsilon)$ than the other odd map in the figure. It is straightforward to verify that, among all odd $P$-partition maps, the $r$-adic map yields the finest partitioning of decision regions. Furthermore, between any two $r$-adic maps, the one with larger $P$ results in a larger number of thinner strips of alternating decision regions, and hence, higher unintended receiver $\Pr(\epsilon)$.

Fig. 3.8 depicts the unintended receiver $\Pr(\epsilon)$ as a function of the spreading gain, $L$, for several 4-partition maps. As the figure reveals, for all maps, $\Pr(\epsilon)$ is

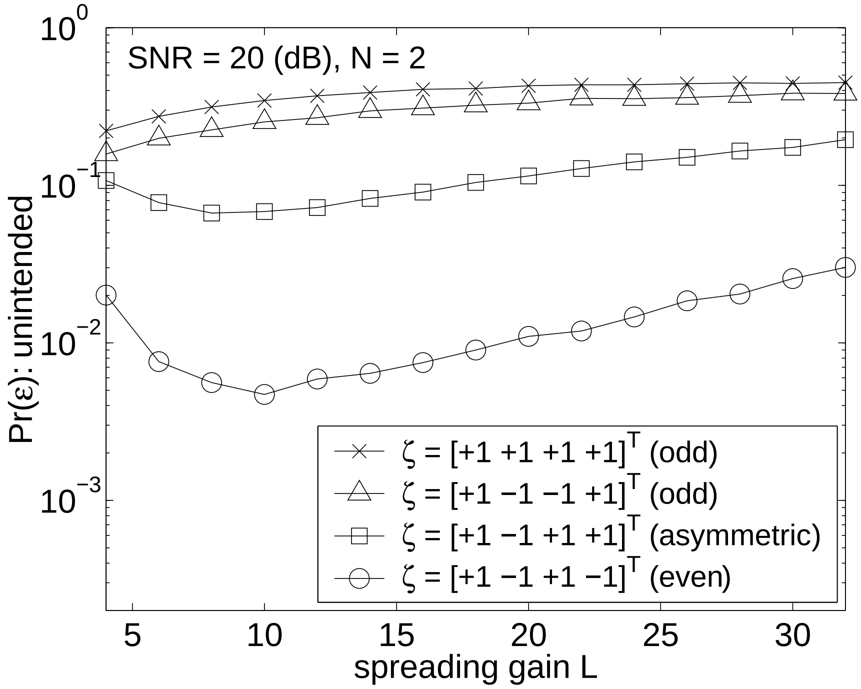


Figure 3.8: Numerically computed upper bounds on the unintended receiver $\Pr(\epsilon)$ vs. spreading gain for several SS systems employing 4-partition maps.

an eventually increasing function of $L$, with $\lim_{L\to\infty}\Pr(\epsilon) = 0.5$. For the odd maps in the figure, the unintended receiver $\Pr(\epsilon)$ is a strictly increasing function of the spreading gain; this is expected, as, for these maps, discrimination is effectively based on boundary signal pairs, and the energy per signal pair decreases with increasing $L$. On the other hand, for the asymmetric and the even map in the figure there is an $L$–range over which the $\Pr(\epsilon)$ performance improves with $L$. This is due to the fact that for these maps discrimination is based on *all* signal pairs throughout the interval (see Fig. 3.6), and is thus affected by both the chip and the codeword energy. In particular, as $L$ increases, the variance in $\mathcal{E}\left(\mathbf{c}^L\right)$ becomes smaller and thus the probability of transmitting a low-power codeword, which dictates the $\Pr(\epsilon)$, decreases.[2] As, however, higher spreading gains also imply lower energy per chip, the

[2] Each sequence $c[n]$ generated from any $P$-partition map has identically distributed PDFs with

unintended receiver performance eventually degrades with increasing $L$. The figure also shows that odd maps outperform even and non-symmetric maps in terms of $\Pr(\epsilon)$. Among all $P$-partition odd maps, $r$-adic maps are the most attractive as they result in the worst-case $\Pr(\epsilon)$ performance for unintended receivers. These observations are consistent with our preceding analysis revealing that odd maps lead, in general, to higher unintended receiver $\Pr(\epsilon)$, and that among odd maps with the same number of partitions, $r$-adic maps yield the least favorable decision regions. Thus, among all $P$-partition maps, $r$-adic maps provide the highest $\Pr(\epsilon)$ advantages to intended users. Digitized maximal-length sequences from $r$-adic maps that retain key properties of the underlying true chaotic trajectories can be readily generated via the design methods developed in Section 2.3. Interestingly, $r$-adic maps have been extensively studied in the context of intended receiver performance in multiuser DS/CDMA systems, and have been shown to possess attractive auto- and cross-correlation properties and broadband spectra [8–10].

Fig. 3.9 depicts the $\Pr(\epsilon)$ of intended and unintended receivers vs. SNR for various $r$-adic maps. Also shown in the figure is the lower bound on $\Pr(\epsilon)$ from (3.8). As the number of partitions $P(= r)$ is increased, the $\Pr(\epsilon)$ attainable by intended receivers increases with respect to the lower bound from (3.8), as discussed in Sec. 3.1. This degradation is offset, however, by a more significant increase in the unintended receiver $\Pr(\epsilon)$, as higher $r$ implies higher sensitivity to initial conditions and lower quality chaotic sequence estimates. At higher spreading gains, the $\Pr(\epsilon)$ gap becomes even larger as the intended receiver $\Pr(\epsilon)$ converges to the lower bound in (3.8) while the unintended receiver $\Pr(\epsilon)$ degrades with $L$. Thus varying the slope $r$ among $r$-adic maps provides a method for trading intended receiver $\Pr(\epsilon)$ performance for greater

respect to $n$ and, hence, the law of large numbers applies to $\mathcal{E}\left(\mathbf{c}^L\right)$.

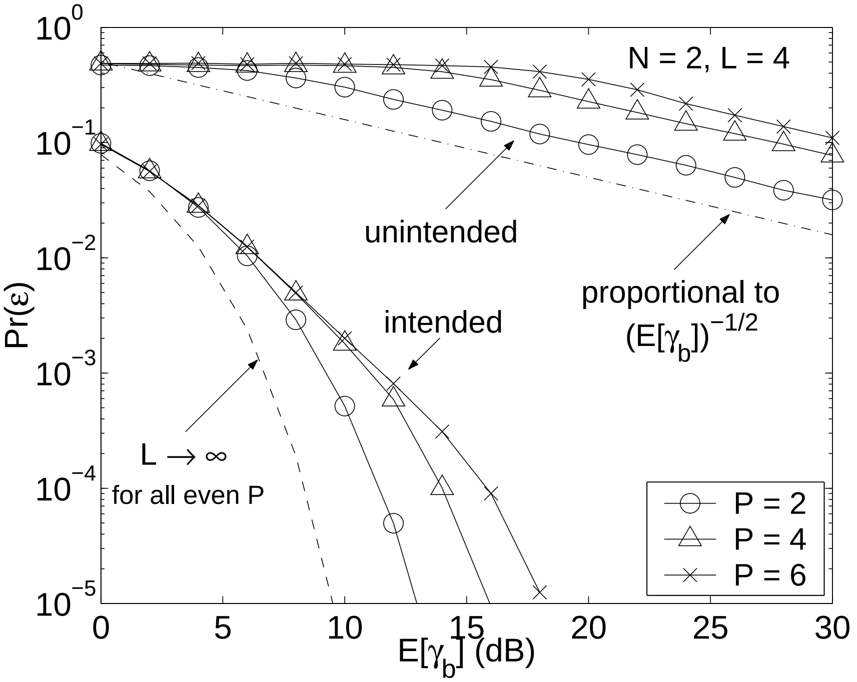


Figure 3.9: Analytically computed intended receiver $\Pr(\epsilon)$'s vs. numerically computed upper bounds on $\Pr(\epsilon)$'s of unintended receivers, for $r$-adic map based SS systems. Dashed curve corresponds to the lower bound on the intended receiver $\Pr(\epsilon)$ (3.8).

privacy benefits.

An important characteristic of unintended receiver $\Pr(\epsilon)$ inferable from Fig. 3.9 is that, at high $\overline{\gamma}_b$, the unintended receiver $\Pr(\epsilon)$ curves for $r$-adic map-based DS/SS systems decay at a constant rate. Specifically, the figure suggests that the decaying rate is $1/\sqrt{\overline{\gamma}_b}$ (the same as the slope of dash-dot line). In the next section we verify this decaying rate for the class of odd $P$-partition maps that includes all $r$-adic maps.

### 3.2.3 Asymptotic Decaying Rate of $\Pr(\epsilon)$ for Odd $P$-partition Maps

In this section we utilize the results developed in App. B.2 to show that the unintended receiver $\Pr(\epsilon)$ for DS/SS with spreading sequences generated by odd $P$-partition maps can be bounded from below by a function that decays at a rate of $1/\sqrt{\overline{\gamma}_b}$ at high $\overline{\gamma}_b$.

We develop a lower bound on the $\Pr(\epsilon)$ of detecting a fixed but arbitrary differentially encoded symbol given observation of $y[n]$ in (3.2). In particular, we assume that an IID sequence $i[n] = \pm 1$ is differentially encoded into the sequence $b[n] = i[n]\, b[n-1]$ used in (3.2). We focus on detection of $i[D]$, for some $1 \leq D \leq N-1$, based on observation of $\mathbf{y}$ in (3.10). We denote via $\mathbf{x}(c, \mathbf{b})$ the $NL$-dimensional signal vector that is transmitted, given an initial condition $c$ and a vector $\mathbf{b}$ in (3.11); *viz.*,

$$\mathbf{x} \;=\; \mathbf{x}^{NL} \;=\; \mathbf{x}(c, \mathbf{b}) \;\stackrel{\triangle}{=}\; \begin{bmatrix} x[0] & x[1] & \cdots & x[NL-1] \end{bmatrix}^{\mathrm{T}} , \qquad (3.15)$$

where $x[n]$ is as in (3.1) and $\mathbf{b}$ and $b[n]$ are related via (3.11). Letting $\mathcal{S}_\imath^{(D)} = \{\mathbf{b};\; b[D]b[D-1]/\mathcal{E}_b = \imath\}$, for $\imath = \pm 1$, the optimal detector for the $D$th symbol sets is

$$\hat{i}[D] \;=\; \arg\max_{\imath \in \{-1,\,1\}} \Pr\left(\mathbf{b} \in \mathcal{S}_\imath^{(D)} | \mathbf{y}\right) .$$

To obtain a lower bound on the $\Pr(\epsilon)$, we consider a detector that is provided with the remaining $N-2$ information symbols $\{i[n];\, 1 \leq n \leq N-1,\, i \neq D\}$ as well as some additional side information that depends on whether or not $c[0]$ belongs in the set $I_o \stackrel{\triangle}{=} \bigcup_{c \in \mathcal{C}^{(D)}} I(c)$, where $I(c) \stackrel{\triangle}{=} (c, c+\Delta)$, $\Delta \stackrel{\triangle}{=} 2\, P^{-(NL-1)}$, and $\mathcal{C}^{(D)}$ is the preimage of $\{0\}$ under $F^{DL-1}$. Specifically, when $c[0] \notin I_o$, the value of $i[D]$ is declared to the receiver; when $c[0] \in I_o$, the receiver is only told that the initial condition is from the set $\{\pm \underline{c}[0] + \delta\}$, where $\underline{c}[0]$ denotes the unique $c \in \mathcal{C}^{(D)}$ for which $c[0] \in (c, c+\Delta)$, and $\delta \stackrel{\triangle}{=} \delta(c[0]) = c[0] - \underline{c}[0]$. As App. B.2 shows, the optimal receiver given this side information is inferior to the optimal detector in the context of binary signaling in AWGN with codewords $\mathbf{x}_{i[D]}$ and $\mathbf{x}_{-i[D]}$, where $\mathbf{x}_{i[D]}$ is the transmitted vector in (3.15), and where $\mathbf{x}_{-i[D]}$ is the vector closest in Euclidean distance to $\mathbf{x}_{i[D]}$

among those associated with the antipodal hypothesis, and corresponds to using the spreading sequence generated from the initial condition $-\underline{c}[0] + \delta$. Consequently,

$$\Pr(\epsilon | c[0] \in I_o) \geq \mathcal{Q}\left(\sqrt{\tilde{\gamma}(\delta)}\right) \tag{3.16}$$

where

$$\tilde{\gamma}(\delta) = \frac{\|\mathbf{x}_1 - \mathbf{x}_{-1}\|^2}{2N_o} = \frac{2\,\|\mathbf{r}\|^2}{N_o} = \delta^2 \frac{6\,\mathcal{E}_b(P^{2DL}-1)}{L(P^2-1)\,N_o} = C\overline{\gamma}_b\delta^2\ , \tag{3.17}$$

with $C = \frac{6(P^{2DL}-1)}{(P^2-1)}$. Conditioned on $c[0] \in I(\underline{c}[0])$ (and thus on $c[0] \in I_o$), $\delta$ is uniformly distributed in $(0, \Delta)$, which, using (3.17), also implies that $0 < \tilde{\gamma}(\delta) < \gamma_{\max} = C\Delta^2\overline{\gamma}_b$. To show that $\Pr(\epsilon)$ cannot decay faster than $1/\sqrt{\overline{\gamma}_b}$, we pick an arbitrary $\gamma_o \in (0,\ C\,\Delta^2\,\overline{\gamma}_b)$; we remark that $\gamma_o$ *can* remain fixed as $\overline{\gamma}_b$ increases. Hence, using (3.16), we have

$$\begin{aligned}
\Pr(\epsilon) &\geq \Pr(c[0] \in I_o)\ \Pr(\epsilon | c[0] \in I_o) \\
&\geq \Pr\left(c[0] \in I_o\right) \int_0^\infty \mathcal{Q}\left(\sqrt{\gamma}\right) p_{\tilde{\gamma}}\left(\gamma\right) d\gamma \\
&\geq P^{(D-N)L}\,\mathcal{Q}\left(\sqrt{\gamma_o}\right) \int_0^{\gamma_o} p_{\tilde{\gamma}}\left(\gamma\right) d\gamma & \text{(3.18a)} \\
&= P^{(D-N)L}\,\mathcal{Q}\left(\sqrt{\gamma_o}\right) \Pr\left(\delta < \sqrt{\frac{\gamma_0}{\overline{\gamma}_b\,C}}\ \middle|\ c[0] \in I_o\right) \\
&= P^{(D-N)L}\,\mathcal{Q}\left(\sqrt{\gamma_o}\right) \frac{P^{NL-1}}{2} \sqrt{\frac{\gamma_o L(P^2-1)}{6(P^{2DL}-1)}}\,\frac{1}{\sqrt{\overline{\gamma}_b}}\,, & \text{(3.18b)}
\end{aligned}$$

where (3.18a) is due to the fact the $\mathcal{Q}\left(\sqrt{\gamma}\right)$ is a nonnegative decreasing function of $\gamma$, and where (3.18b) is the desired bound.

### 3.2.4 Performance Evaluation for Odd $P \times Q$ Partition Maps

The major factors that affect the unintended receiver performance, as observed in Section 3.2.2, can be exploited to develop a set of efficient $\Pr(\epsilon)$ metrics for a class of $P\times Q$ partition maps with attractive privacy characteristics. In particular, the dominance of the pairs of observations at codeword transitions $\{y[DL-1], y[DL]\}$, $D = 1, 2, \cdots$ on the unintended receiver $\Pr(\epsilon)$ for odd-symmetric maps allows the development of unintended receiver $\Pr(\epsilon)$ predictors for odd $P \times Q$ partition maps. These metrics are computationally more efficient than their counterparts in Section 3.2.1, which do not have straightforward extensions for the $P \times Q$ partition maps with $Q \geq 2$.

We develop efficient simulation based methods that predict the $\Pr(\epsilon)$ trends as functions of SNR, spreading gain $L$, and the $P \times Q$ partition map descriptors $\zeta$ in (2.12) and $\mathbf{q}$ in (2.13). These metrics are more accurate than the upper bounds in Section 3.2.1. First, a lower bound on $\Pr(\epsilon)$ is obtained by assuming that the unintended receiver knows that the initial condition is from the set $\{c[m];\ m = 0, 1, \ldots, M_o - 1\}$ for some $M_o$ significantly larger than the observation interval $NL$. In particular, the unintended receiver $\Pr(\epsilon)$ is bounded by that of the optimum receiver in the case that, in addition to the observation $\mathbf{y}$ in (3.10), the receiver is given $b[0]$ and $\{i[n];\ 1 \leq n \leq N-1,\, n \neq D\}$ as well as $c[0] \in \{c[m];\ m = 0, 1, \ldots, M_o - 1\}$. This effectively transforms the uniform PDF of $c[0]$ to a posterior PMF of $M_o$ impulses. The associated ML detector is given by

$$\hat{i}_{\mathrm{LB}}(\mathbf{y}) = \arg\max_{i\in\pm1} \sum_{m=0}^{M_o-1} \exp\left\{ \frac{1}{N_o} \sum_{n=0}^{NL-1} \left( \frac{2A}{\sqrt{L}}\, y[n] F^n(c[m])\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] - \frac{A^2 \mathcal{E}_b}{L} \left(F^n(c[m])\right)^2 \right) \right\}, \qquad (3.19)$$

where $i = b[D-1]b[D]$. The computational complexity of (3.19), while lower than that of the lower bound (3.13) in Section 3.2.1 for suitably chosen $M_o$, still grows exponentially with observation length $NL$. Computationally viable approximations to (3.19) can be obtained by replacing $\mathbf{y}$ with a windowed observation around the codeword boundary

$$\mathbf{y}_w \triangleq \begin{bmatrix} y[DL-w] & y[DL-w+1] & \cdots & y[DL+w-1] \end{bmatrix}^{\mathrm{T}},\ 1 \le w \le (N-1)L\,.$$

These approximations can prove accurate even when $w = 1$, due to the dominance of the pairs of observations at the bit transitions on the $\Pr(\epsilon)$, and the sensitive dependence of the chaotic map on initial conditions. Efficient upper bounds on the unintended receiver $\Pr(\epsilon)$ for odd $P \times Q$ partition maps can be similarly obtained by considering the optimum detector of $i[D]$ given the windowed observation $\mathbf{y_1}$ (transition from $b[D-1]$ to $b[D]$). For a class of odd $P \times Q$ partition maps whose map segments lie only on those of an $r$-adic map $\{c, F(c)\}$ or its antipodal $\{c, -F(c)\}$, this detector is also the minimum distance detector for the simpler binary-signaling-in-AWGN problem, with sets of constellation points

$$\hat{\mathbf{c}}_{i,j} \ \triangleq\ \begin{bmatrix} \frac{2(j-1)-(P-1)}{P} & \frac{i(-1)^j(Q-2j+1)}{Q} \end{bmatrix}^{\mathrm{T}},\ i \in \pm 1,\ k = 1, 2, \ldots, P\ .$$

Consequently, this detector takes the following form.

$$\hat{i}_{\mathrm{UB}}(\mathbf{y}) \ =\ \arg\min_i \min_j \left\| \mathbf{y_1} - \sqrt{\frac{A^2\,\mathcal{E}_b}{L}}\,\hat{\mathbf{c}}_{i,j} \right\|^2 . \qquad (3.20)$$

As Fig. 3.10 reveals, the approximation to (3.19) with $w = 1$ nearly coincides with the upper bound (3.20) and rapidly converges as $w$ increases, suggesting that these approximations in conjunction with the upper bound (3.20) predict the $\Pr(\epsilon)$ trends of

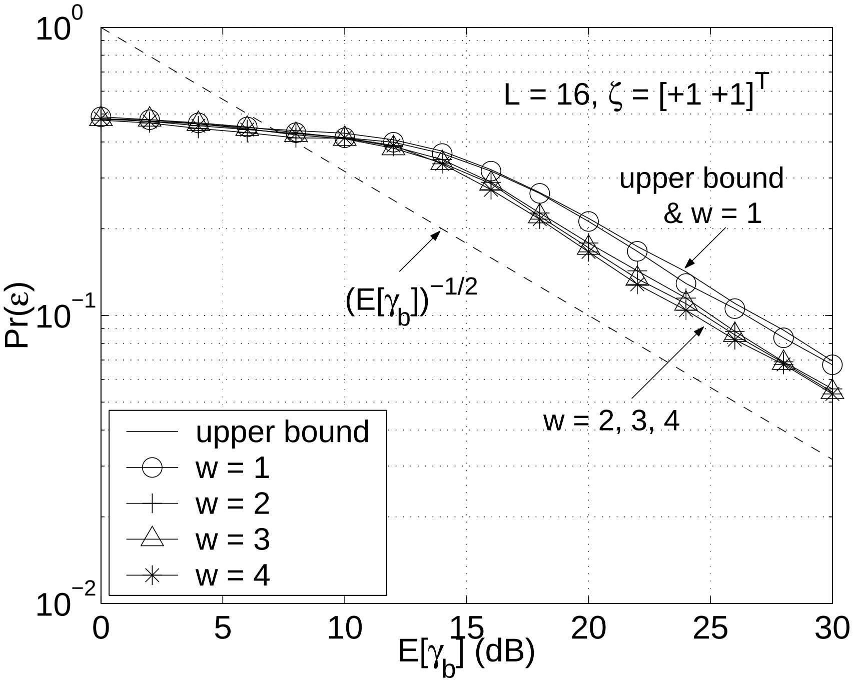


Figure 3.10: Simulated upper bound and approximation to lower bound on the unintended receiver $\Pr(\epsilon)$ via (3.19) for dyadic map and various values of $w$ ($M_o = 4092$).

unintended receivers. We remark that the constellation set for (3.20) can be modified to accommodate richer classes of odd $P \times Q$ partition maps.

Fig. 3.10, in addition to Fig. 3.9, empirically substantiates our finding in Section 3.2.3 that the unintended receiver $\Pr(\epsilon)$ for DS/SS with odd $P$-partition maps cannot not decay faster than $1/\sqrt{\overline{\gamma}_b}$ at high $\overline{\gamma}_b$. In contrast, the intended receiver $\Pr(\epsilon)$ for these systems (with $P$ even) decays exponentially with $\overline{\gamma}_b$. Thus the knowledge of the initial seed in the chaotic DS/SS systems we consider yields significant uncoded $\Pr(\epsilon)$ advantages to intended users. This is in contrast to conventional DS/SS employing binary-valued spreading sequences generated via LFSRs, where an unintended receiver without knowledge of the initial seed can obtain a consistent estimate even at very low $\overline{\gamma}_b$, provided a long enough segment of the sequence is observed [17, 18].

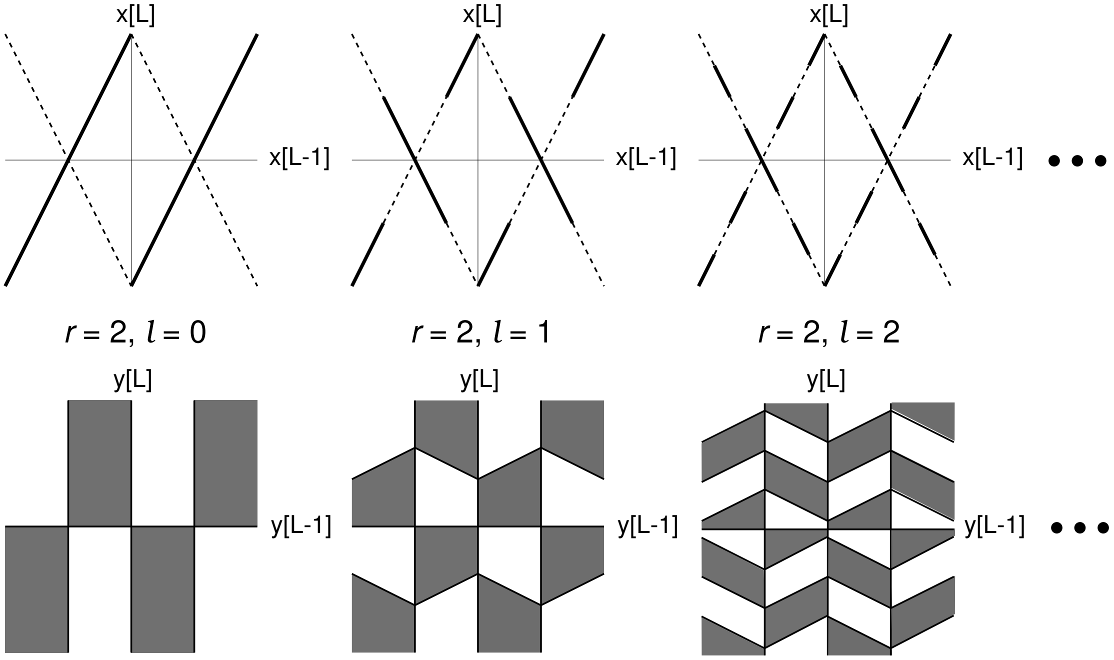


Figure 3.11: Upper graphs: signal trajectories for nested maps based on dyadic map, under hypotheses $b[0] = b[1]$ (solid), and $b[0] = -b[1]$ (dashed). Lower graphs: associated decision regions.

## 3.3 Iterative Constructions of $P \times Q$ Partition Map-based DS/SS

Based on the analysis in Sec. 3.2, suggesting that odd symmetry and fine decision-region partitioning are attractive attributes, we can construct recursive algorithms for generating sequences of maps from the richer class of $P \times Q$ partition maps with monotonically increasing unintended receiver $\Pr(\epsilon)$, while keeping the intended receiver $\Pr(\epsilon)$ unaffected. Such an algorithm that preserves the ratio $P/Q$ and, hence, the Lyapunov exponent, is illustrated in Fig. 3.11. The algorithm is initialized with an $r$-adic map, *e.g.*, the dyadic map. At each recursion step, a new $P \times Q$ partition map is constructed via modifications of the map constructed in the preceding recursion step. In particular, certain piecewise linear segments are swapped with their antipodal versions, to create a map of twice as large $P$ and $Q$, whereby odd symmetry is preserved and the partitioning of the unintended-receiver decision regions is made finer. Specifically, the algorithm results in a sequence of $P_\ell \times Q_\ell$ partition maps $F_\ell(\cdot)$ by means of the following steps:

(1) *Initialization* ($\ell = 0$): $F_0(\cdot)$ is an $r$-adic map for some $r$ ($P_0 = 2r$ , $Q_0 = 2$).

(2) *Recursion* (step $\ell$): construct a $P_\ell \times Q_\ell$ partition map $F_\ell(\cdot)$ from $P_{\ell-1} \times Q_{\ell-1}$ partition map $F_{\ell-1}(\cdot)$, as follows:

- (2a) set $P_\ell = 2 \cdot P_{\ell-1}$ and $Q_\ell = 2 \cdot Q_{\ell-1}$;
- (2b) view $F_{\ell-1}(\cdot)$ as a $P_\ell \times Q_\ell$ partition map with (equi-spaced in $I$) partitions points $\{a_1^{(\ell)}, a_2^{(\ell)}, \cdots , a_{P_\ell}^{(\ell)}\}$ and $\{b_1^{(\ell)}, b_2^{(\ell)}, \cdots , b_{Q_\ell}^{(\ell)}\}$;
- (2c) letting $m_i^{(\ell)}$ denote the mid-point of $I_i^{(\ell)} = \left[a_{i-1}^{(\ell)}, a_i^{(\ell)}\right)$, *i.e.*, $m_i^{(\ell)} \triangleq \frac{a_{i-1}^{(\ell)}+a_i^{(\ell)}}{2}$ , $i \in \{1, \ldots , P_\ell\}$, sequentially define $F_\ell(\cdot)$ on $I = \cup_{1 \leq i \leq P_\ell} I_i^{(\ell)}$ as follows:
  - (2c-i) *Initialization*: $F_\ell | I_1^{(\ell)} \triangleq F_{\ell-1} | I_1^{(\ell)}$; set $i = 2$;
  - (2c-ii) *$i$-th Interval*: for all $c \in I_i^{(\ell)}$,
    if $\left|F_\ell(m_{i-1}^{(\ell)}) + F_{\ell-1}(m_i^{(\ell)})\right| > \left|F_\ell(m_{i-1}^{(\ell)}) - F_{\ell-1}(m_i^{(\ell)})\right|$ ,
    then $F_\ell \triangleq -F_{\ell-1}$ , else $F_\ell \triangleq F_{\ell-1}$;
  - (2c-iii) if $i \leq P_\ell$, increment $i$ by 1 and go to step (2c-ii); else, go to step (3);

(3) increment $\ell$ by 1 and go to step (2).

Throughout, we use $F_{r,\ell}(\cdot)$ to denote the map constructed by applying $\ell$ steps of the above "nested" recursion on a particular $r$-adic map. We remark that this algorithm can be extended to initializations with any $P$-partition map. However, for a fixed $P_0$, the choice of the initializing $P$-partition map does not affect the intended and unintended receiver $\Pr(\epsilon)$ for the subsequently generated nested maps of $\ell \geq 1$. This

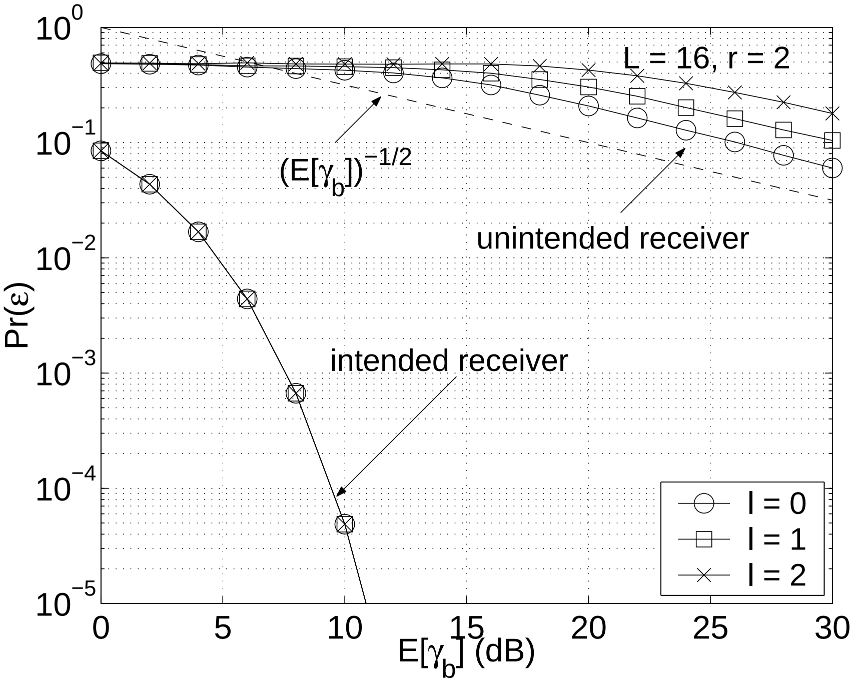


Figure 3.12: Intended receiver $\Pr(\epsilon)$ vs. simulation-based upper bounds (3.20) on unintended receiver $\Pr(\epsilon)$, for nested maps based on dyadic map.

is because the recursions initialized with any $P$-partition map with $P = r$ generate $\pm F_{r,\ell}(\cdot)$ for $\ell \geq 2$. Since, among all possible initializing $P$-partition maps with $P = r$, the $r$-adic map offers the strongest privacy, in this dissertation we focus on the nested recursions initialized with an $r$-adic map.

The nested maps $F_{r,\ell}(\cdot)$ designed by this algorithm have several important properties. First, they are odd $P \times Q$ partition mappings, and, hence, the unintended receiver $\Pr(\epsilon)$ can be readily evaluated via the methods in Section 3.2.4. Moreover, $E\left[\mathcal{E}\left(\mathbf{c}^L\right)\right] = 1/3$ for all nested maps, thus $A = \sqrt{3}$ in (3.2). In fact, since $|F^k_{r,\ell}(c[0])| = |F^k_{r,\ell'}(c[0])|$ for all $r$, $\ell$, $\ell'$, $k$ and $c[0]$, the recursion preserves the PDF of spreading codeword power and, hence, the intended receiver $\Pr(\epsilon)$. Also, all constructed maps have (unique) uniform invariant densities, exhibit the same sensitive dependence on initial conditions as the initializing $r$-adic map, $F_{r,0}(\cdot)$, and can be made exact with suitable realizations. Furthermore, since for any nested map there exists a corresponding initializing $r$-adic map with lower unintended receiver $\Pr(\epsilon)$, the $1/\sqrt{\overline{\gamma}_b}$ lower bound on the asymptotic decaying rate of $\Pr(\epsilon)$, developed in Section 3.2.3 for $r$-adic maps, holds for all nested maps. Finally, digitized maximal-length sequences from any nested map that retain key properties of the underlying chaotic trajectories can be efficiently generated by exploiting Theorem 1 in Section 2.3.[3]

In general, the associated unintended receiver $\Pr(\epsilon)$ depends on the received SNR, the map parameters $r$ and $\ell$, and the spreading gain $L$. These trends are reflected in Fig. 3.12, showing that the unintended receiver $\Pr(\epsilon)$ degrades monotonically with the number of recursion steps, while the intended receiver $\Pr(\epsilon)$ is unaffected. The figure also verifies that the unintended receiver $\Pr(\epsilon)$ curves for nested maps at high $\overline{\gamma}_b$ indeed decay at the rate of $1/\sqrt{\overline{\gamma}_b}$. Thus each of these curves at sufficiently high $\overline{\gamma}_b$ can be modeled as $1/\sqrt{\mathcal{K}(L,r,\ell)\overline{\gamma}_b}$, where $\mathcal{K}$ is some constant that depends only on $\{L,r,\ell\}$. The physical-layer privacy potential of these chaotic DS/SS systems is readily apparent from the figure, in terms of the $\Pr(\epsilon)$ gap between intended and unintended receivers.

### 3.3.1 Closed-Form $\Pr(\epsilon)$ Prediction for a Class of Nested Maps

In this section, we investigate the dependence of the unintended receiver $\Pr(\epsilon)$ performance on the system parameters for the nested maps, and quantify the dependence in closed form for a class of nested maps. Specifically, we consider the $1/\sqrt{\mathcal{K}(L,r,\ell)\overline{\gamma}_b}$ model of unintended receiver $\Pr(\epsilon)$, and determine the relationship between $\mathcal{K}$ and the system parameters $\{L,r,\ell\}$ for a subclass of nested maps.

The dependence of $\mathcal{K}$ on $L$ can be readily deduced for moderate and large

[3] We note that $H(x)$ in Fig. 2.7 is the nested map $F_{2,1}(\cdot)$

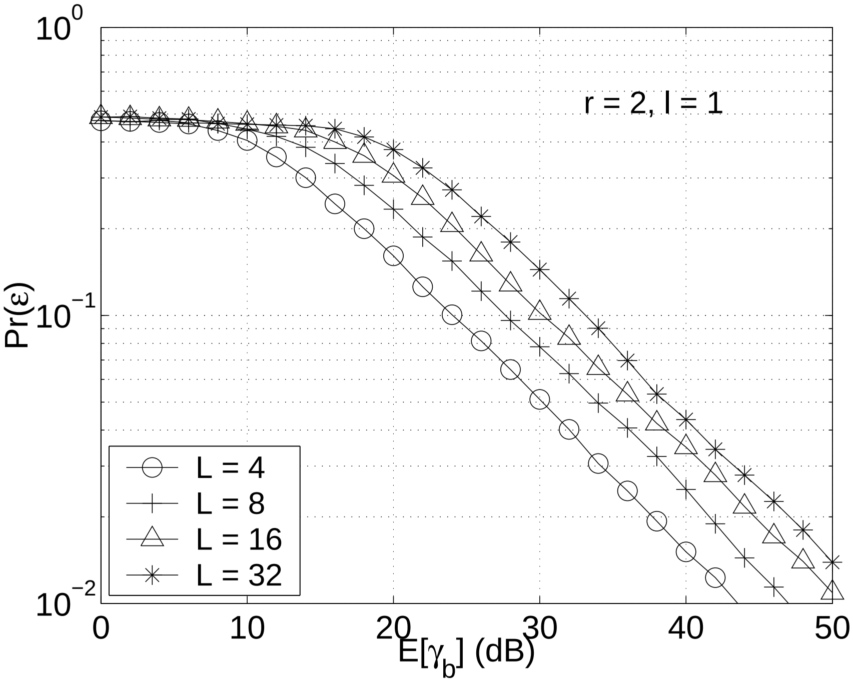


Figure 3.13: Simulation-based upper bounds on the unintended receiver $\Pr(\epsilon)$ vs. SNR for nested map-based DS/SS with various spreading gains.

$L$ values. As Fig. 3.13 shows for nested maps, doubling $L$ increases the $\overline{\gamma}_b$ required for a target $\Pr(\epsilon)$ by 3 dB; this is expected, since the average chip energy $\mathcal{E}_c \triangleq (\mathcal{E}_b/L)E\left[c^2[n]\right]$ is reduced by a factor of two and the unintended receiver $\Pr(\epsilon)$ for these maps is effectively dictated by a small number of chip observations (around bit transitions) that does not grow with $L$.

The dependence of the unintended receiver $\Pr(\epsilon)$ on the parameters $\{r, \ell\}$ can be accurately predicted for certain subsequences of nested maps. A sequence of such maps $G_\ell(\cdot)$ is shown in Fig. 3.14. These maps can be generated by first generating sequences of nested maps $F_{r,\ell}(\cdot)$, each initialized with different $r$-adic map, then selecting one map from each sequence of nested maps that satisfy the constraint $r = 2^\ell$, *i.e.*,

$$G_\ell(\cdot) \triangleq F_{2^\ell,\ell}(\cdot)\,. \tag{3.21}$$

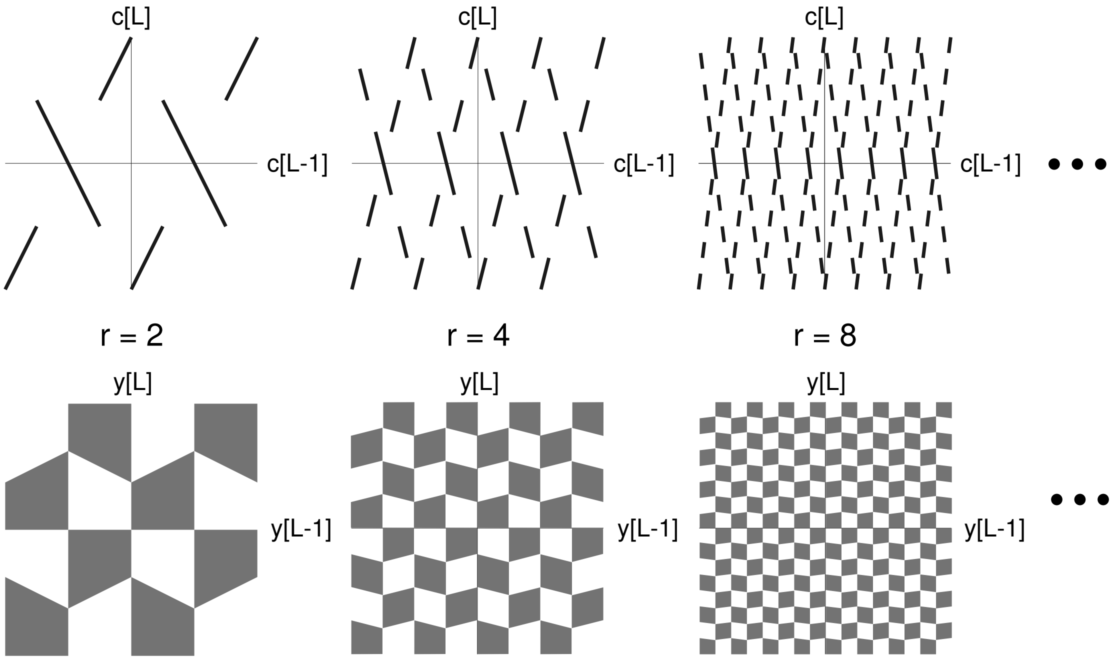


Figure 3.14: Upper graphs: signal trajectories for sequence of nested maps with $r = 2^\ell$ under hypotheses $i[1] = +1$. Lower graphs: associated decision regions.

As shown in Fig. 3.14, for these maps the decision regions for pairs of observations at bit transitions can be modeled as diamond-shaped regions of the same size. From the figure, the gap between the $\overline{\gamma}_b$ required by $G_\ell(\cdot)$ and $G_{\ell+1}(\cdot)$ for a target $\Pr(\epsilon)$ at a given $L$ can be predicted to be 6 dB, since the side lengths of each decision region for $G_{\ell+1}(\cdot)$ is half of those for $G_\ell(\cdot)$. Fig. 3.15 verifies these assertions for the maps of (3.21). Indeed, increasing $\ell$ by one increases the $\overline{\gamma}_b$ required for a target $\Pr(\epsilon)$ by approximately 6 dB. The estimate of 6 dB shift, while pessimistic for $\ell = 1$, becomes increasingly accurate for higher $\ell$, as the modeling of decision regions as diamonds becomes more accurate. Finally, by exploiting the empirical observation that $\mathcal{K}(16, 2, 1) \approx 1/16$, we may obtain an expression approximately predicting the

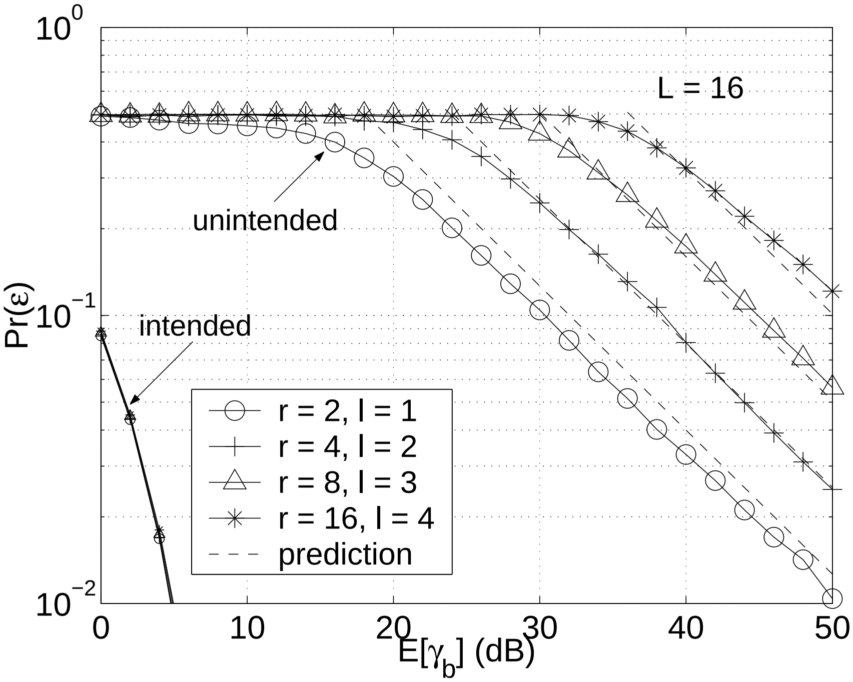


Figure 3.15: Intended receiver $\Pr(\epsilon)$ vs. simulation-based upper bounds and prediction (3.22) on unintended receiver $\Pr(\epsilon)$ for nested maps $F_{r,\ell}(\cdot)$.

unintended receiver $\Pr(\epsilon)$ for the subclass of maps in (3.21) at high $\overline{\gamma}_b$:

$$\Pr(\epsilon) \approx 2^{\ell-1}\sqrt{\frac{L}{\overline{\gamma}_b}}\,. \tag{3.22}$$

This predictor, while less accurate than the $\Pr(\epsilon)$ analysis based on Monte-Carlo simulations of (3.14), can furnish rule-of-thumb curves for system design purposes. As shown in Figs. 3.13 and 3.15, this class of nested map-based DS/SS systems allows systematic selection of the system parameters $\{L, r, \ell\}$ such that the unintended receiver $\Pr(\epsilon)$ is lower bounded by the target $\Pr(\epsilon)$ subject to a maximum SNR constraint. We note that, although Figs. 3.13 and 3.15 suggest that arbitrary improvement in secrecy is possible by indefinitely increasing $\{r, \ell\}$, as we show in the following section, the finite precision depth of practical systems limits the extent of these improvements.

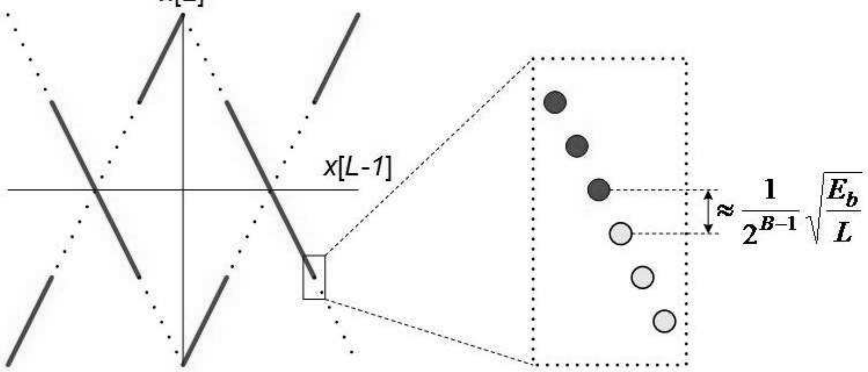


Figure 3.16: Left-hand side: Signal trajectories $\{x[L-1], x[L]\}$ for the $B$-bit implementation of the nested maps $F_{2,1}$, under hypotheses $b[0] = b[1]$ (solid), and $b[0] = -b[1]$ (dotted). Right-hand side: Close-up view of a part of the mapping, showing several circles representing the constellation points, under hypotheses $b[0] = b[1]$ (dark) and $b[0] = -b[1]$ (light).

## 3.4 Privacy via Pseudochaotic DS/SS

In the following we explore some of the implementation-induced limitations on the privacy benefits provided with chaotic DS/CDMA systems. In particular, we compare the unintended receiver performance trends corresponding to the sequences from nested maps, generated via the algorithms in Section 2.3, to those corresponding to the associated true chaotic spreading sequences. In the process, we determine the ranges of SNR and nested recursion depths, for which the privacy benefits of the pseudochaotic DS/SS closely approximate those of the associated true chaotic DS/SS.

Conditioned on a finite precision depth, there is a bit SNR range $(\overline{\gamma}_{\text{min}}, \overline{\gamma}_{\text{max}})$, over which the $\Pr(\epsilon)$ of the unintended receiver for the pseudochaotic DS/SS closely approximates that for the underlying true chaotic DS/SS. In particular, the unintended receiver $\Pr(\epsilon)$ in this SNR range decays as $1/\sqrt{\text{SNR}}$. For SNR higher than $\overline{\gamma}_{\text{max}}$, however, the decaying rate of the unintended receiver $\Pr(\epsilon)$ for pseudochaotic DS/SS does not decay at the rate of $1/\sqrt{\text{SNR}}$ associated with true chaotic DS/SS.

Instead, the unintended receiver $\Pr(\epsilon)$ decays at an exponential rate. This is because a pseudochaotic map, implemented as a finite state machine using $B$-bit state description, can be described by the graph that consists of a finite number of points that approximate the continuous affine segments of the associated true chaotic map. For odd-symmetric maps, the projection of the set of modulated pseudochaotic trajectories on the two-dimensional space formed by the pairs of symbols at codeword boundaries dominates the unintended receiver $\Pr(\epsilon)$. Thus, the $2 \times 1$ vectors that compose the graphs of the projected pseudochaotic mapping at codeword boundaries can be effectively employed as the set of vectors for decision rules based on the windowed observation $\mathbf{y}_1$, as in Section 3.2.4. For convenience, we refer to these $2 \times 1$ vectors as constellation points. The precision depth $B$ affects $\overline{\gamma}_{\max}$ via the minimum distance between two neighboring constellation points associated with antipodal hypotheses, since this distance begins to dominate the receiver performance as the average noise power level becomes sufficiently small, *i.e.*, $\overline{\gamma}_b$ reaches $\overline{\gamma}_{\max}$. Fig. 3.16 shows the mapping $\{x[L-1], x[L]\}$ and a close-up view of some constellation points that compose the mapping, where the signal

$$x[n] \;=\; \sqrt{\frac{3}{L}}\, c[n] b \left[ \left\lfloor \frac{n}{L} \right\rfloor \right]$$

is from (3.1), with $c[n]$ generated from the $B$-bit implementation of the nested map $F_{2,1}$ via the methods in Section 2.3. As the figure illustrates, for the nested map-based DS/SS implemented on a $B$-bit precision platform with spreading gain $L$, the distance between two neighboring constellation points is determined by $B$ and $L$ and is approximately $\sqrt{\mathcal{E}_b}/2^{B-1}\sqrt{L}$ (the number of amplitude levels is close to $2^B$). In addition, the nested map parameters $r$ and $\ell$ determine the layout of the decision regions and, hence, the number of constellation points near decision region boundaries.

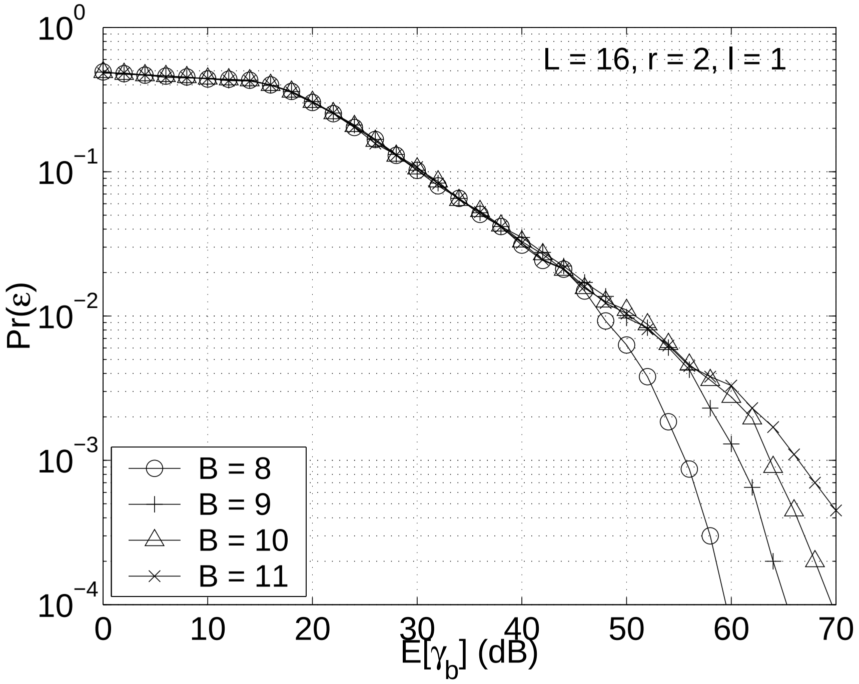


Figure 3.17: Unintended receiver $\Pr(\epsilon)$ via (3.19) for the nested map $F_{2,1}$ as a function of $\overline{\gamma}_b$ for various values of bit precision depth $B$.

Thus $\overline{\gamma}_{\max}$ can be modeled as some function of $r$ and $\ell$ times the average SNR in certain proportion to the distance between neighboring constellation points. From these observations, we can find the relationship between the bit precision depth $B$ and $\overline{\gamma}_{\max}$ by considering the effect of $B$ on the $\overline{\gamma}_b = \mathcal{E}_b/N_o$ such that the standard deviation of the noise term, $\sqrt{N_o/2}$, is approximately half of the distance between two neighboring constellation points. The $\overline{\gamma}_b$ satisfying $\sqrt{N_o/2} \approx \sqrt{\mathcal{E}_b}/2^B\sqrt{L}$ is given by

$$\overline{\gamma}_b \;\approx\; L\,2^{2B-1}\;. \tag{3.23}$$

This relationship (3.23) indicates that increasing $B$ by one increases $\overline{\gamma}_{\max}$ by approximately 6 dB. This is empirically verified for the class of nested maps and illustrated in Fig. 3.17, which shows the unintended receiver $\Pr(\epsilon)$ performance for a nested map implemented with several values of $B$. Fig. 3.17 also suggests that the DS/SS based on a suitably designed pseudochaotic nested map can effectively provide the same privacy benefits as the chaotic DS/SS over virtually all SNR levels of practical interest. Indeed, exploiting the observation from Fig. 3.17 that $\overline{\gamma}_{\max} \approx 62$ dB for 10-bit realization of the DS/SS with $F_{2,1}$ and $L = 16$, and that $\overline{\gamma}_{\max}$ increases approximately by 6 dB with each increment of $B$ by one, we can predict that, for the nested map $F_{2,1}$ realized with 64-bit precision and the spreading gain $L = 16$, $\overline{\gamma}_{\max} \approx 386$ dB.

The finite precision also affects the extent to which we can increase the nested recursion parameters $r$ or $\ell$ for degrading the unintended receiver performance. Since a nested map $F_{r,\ell}$ has $r\,2^{\ell+1}$ affine segments, it can be represented by a $B$-bit digital implementation of a nested map composed of approximately $2^B$ constellation points, where $B$ satisfies

$$B \;\geq\; \log_2 r + \ell + 1 \;. \tag{3.24}$$

Equality in (3.24) holds for the case of a single constellation point representing each affine segment of the map, and indicates the limit on the number of nested recursion steps that can be taken for privacy enhancement. For the subsequence of nested maps $G_\ell(\cdot) = F_{2^\ell,\ell}(\cdot)$ of (3.21) in Section 3.3.1, (3.24) implies that each step of the subsequence increases the minimum $B$ needed for describing the new map by two, *i.e.*, $B \geq 2\,\ell + 1$. This is consistent with the change in the associated decision regions as shown in Fig. 3.14, where every step of the recursion yields a map with four times as many decision regions than the old map. Thus the minimum number of constellation points for describing the map increases by four, and the minimum $B$ increases by two.

Based on (3.24), we can also determine the maximum recursion step $\ell$ of the nested maps $F_{r,\ell}$ conditioned on $r$ and $B$. Fig. 3.18 depicts the unintended receiver $\Pr(\epsilon)$ vs. SNR for the nested maps $F_{2,\ell}$ realized with 8-bit precision. The figure shows

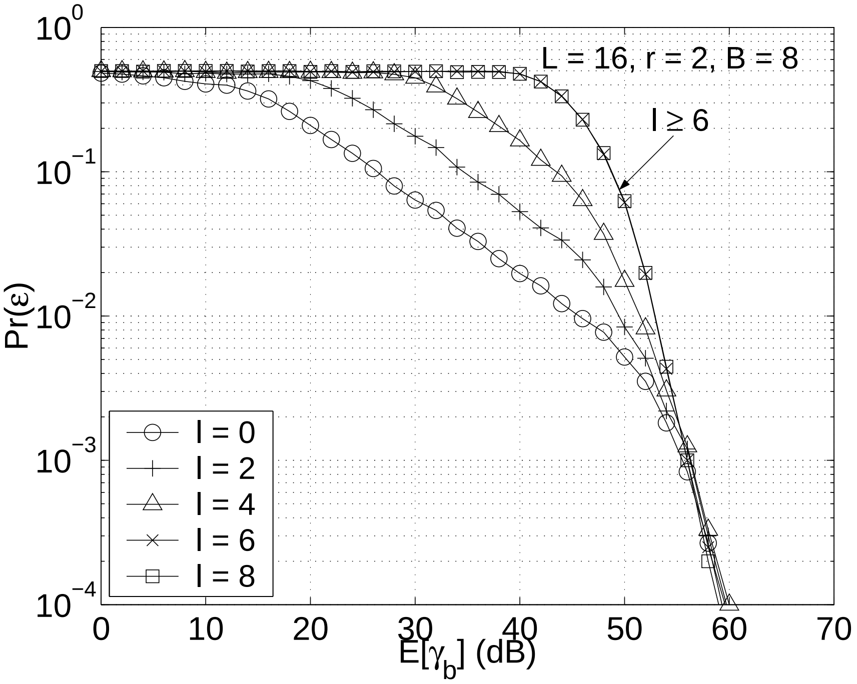


Figure 3.18: Unintended receiver $\Pr(\epsilon)$ via (3.19) as a function of $\overline{\gamma}_b$ for various nested maps with $r = 2$ and $B = 8$.

that increasing the nested recursion step $\ell$ beyond $B - \log_2 r - 1 = B - 2$ does not provide monotonic degradation of the unintended receiver performance, confirming that (3.24) specifies the maximum range of $\ell$ for degrading the unintended receiver $\Pr(\epsilon)$ for SNR smaller than $\overline{\gamma}_{\max}$. Thus, with sufficient bit precision depth, the class of pseudochaotic DS/SS with nested maps can meet a required level of privacy for an enormous range of SNR; for instance, on a 64-bit platform with $L = 16$, $F_{2,62}$ can be implemented such that the unintended receiver $\Pr(\epsilon) \approx 1/2$ for a maximum $\overline{\gamma}_b$ of approximately 370 dB.

# Chapter 4

# Analysis and Design of Pseudochaotic DS/SS Systems: Fading Channels

In this chapter, we characterize the privacy provided by the class of pseudochaotic DS/SS systems of Chapter 3 in the setting of single-user communication over fading channels. Signal fading due to the Doppler effect and multipath propagation result in time-varying signal distortions, which affect receiver design and system performance. As typical wireless channels are easily accessible, communication over such channels is especially vulnerable to interception and unintended demodulation of signals. Thus it is of utmost practical interest to design chaotic DS/SS systems and assess their potential in providing private and reliable communication over fading channels.

The random variations of the channel gain in a fading channel have ramifications on receiver performance that may differentiate the privacy characteristics in fading from those in AWGN. In particular, the intended receiver $\Pr(\epsilon)$ exhibits a slower decaying rate in a wide array of fading channels than in AWGN channels. Hence it is important in designing pseudochaotic DS/SS systems to ensure that the $\Pr(\epsilon)$ decaying rate of the intended receiver is significantly faster than that of the unintended receiver. In addition, in some types of fading channels, the presence of imperfect channel estimates at the receiver can lead to nonzero $\Pr(\epsilon)$ even in noiseless channels, *i.e.*, error floors. Therefore it is of great interest to make certain that, for such channels, the error floor of unintended receivers is much higher than that of the intended users for the same level of channel estimates quality. Moreover, receivers can employ diversity techniques, whereby multiple independently fading copies of the signal are combined to combat the effects of fading and, hence, improve the $\Pr(\epsilon)$ performance. The most commonly exploited types of independently fading signals arise from temporal, spectral, or spatial variations in fading, and result in temporal, spectral, or spatial diversity, respectively. The number of such independently fading copies, or the degree of diversity, that a receiver can exploit is typically limited by associated hardware cost and system constraints, *e.g.*, acceptible processing delays, bandwidth, and physical size [25]. The degrees of receiver antenna diversity that can be exploited, in particular, is limited only by the practical constraints on the receiver and not by the communication system. This is in contrast to many other types of diversity including temporal, spectral, and transmitter antenna diversity, where the degrees of diversity available to the receiver is limited by the constraints on the transmitter and channel and not by those on the receivers. Thus it is possible in certain scenarios that unintended receivers have an advantage in available material resources and can exploit a larger number of receiver antenna elements than intended ones. It is therefore important to design private communication systems such that an unintended receiver can reap only marginal benefits with receiver antenna diversity techniques.

In this chapter we extend and validate our analysis and design of the pseudo-chaotic DS/SS systems in Chapter 3 for private and reliable communication over fading channels. In particular, we consider the impact of channel estimation error and diversity reception on the receiver $\Pr(\epsilon)$ performance. In Section 4.1, we describe a system model for the fading channels of interest. For the channels considered, in Section 4.2 we examine the applicability of the chaotic map design methods developed in Chapter 3. We develop computationally efficient metrics for the intended receiver $\Pr(\epsilon)$ in Section 4.3, and for the unintended receiver $\Pr(\epsilon)$ in Section 4.4. We show that, for the case of slow flat fading, the $\Pr(\epsilon)$ of the optimal unintended receiver with $K$ degrees of spatial diversity decays as $1/\sqrt{\mathrm{SNR}}$ at high SNR, in contrast to the $1/(\mathrm{SNR})^K$ decay rate exhibited by the intended receiver $\Pr(\epsilon)$. Based on the analysis in Section 4.3 and Section 4.4, in Section 4.5 we investigate the impact of diversity gains and imperfect channel estimation on privacy.

## 4.1 System Model

In this section we describe the class of single-user pseudochaotic DS/SS systems that are of interest in this chapter. We assume that the pseudochaotic DS/SS transmitter remains the same as in Chapter 3, *i.e.*, the transmitted signal $x[n]$ is as in (3.1).

We consider the fading channel model in Section 2.1 modified for single-user communication with diversity reception, where the intended and unintended users' received signal is

$$\begin{aligned} y_k[n] &= \alpha_k[n]x[n] + w_k[n] \\ &= \frac{A}{\sqrt{L}}\alpha_k[n]c[n]b\left[\left\lfloor\frac{n}{L}\right\rfloor\right] + w_k[n]\,,\ 1 \le k \le K\,, \end{aligned} \tag{4.1}$$

where the $w_k[n]$'s are IID in $k$ and $n$, zero-mean, complex-valued, circularly-symmetric stationary white Gaussian sequences with power $N_o/2$ per dimension. We consider Rayleigh fading that models the signal propagation with a large number of independent scatterers and no dominant direct line-of-sight component [26]. Specifically, we assume that the fading coefficients $\alpha_k[n]$'s are independent of $w_k[n]$'s and are independent in $k$, zero-mean, complex-valued, circularly-symmetric stationary Gaussian sequence with variance 1/2 for real and imaginary parts, corresponding to $E\left[|\alpha_k[n]|^2\right] = 1$ for all $n$ and $k$. Then the fading envelope

$$a_k[n] \overset{\triangle}{=} |\alpha_k[n]| = \sqrt{(\mathrm{Re}\{\alpha_k[n]\})^2 + (\mathrm{Im}\{\alpha_k[n]\})^2}\,,$$

where $\mathrm{Re}\{z\}$ and $\mathrm{Im}\{z\}$ denote the real and imaginary parts of a complex number $z$, follows the Rayleigh PDF with $E\left[a_k^2[n]\right] = 1$;

$$p_{a_k[n]}(a) = 2\,a\,e^{-a^2}\;,\;\; a \geq 0\,.$$

With proper choice of $K$ and the statistical characterization of $\alpha_k[n]$ with respect to $n$, the model in (4.1) captures several fading channel models of interest:

(1) *Slow flat fading*: Set $\alpha_k[n] = \alpha_k$ for all $n$.

(2) *Fast flat fading*: Set $\alpha_k[n]$ IID in $n$. Spread spectrum receivers naturally exploit the available degrees of temporal diversity in time-selective (fast) fading channels.

(3) *Frequency-selective fading with OFDM front end*: Set $\alpha_k[n]$ as the output of the OFDM system associated with the $n$-th subcarrier band. OFDM front end can effectively transform a frequency-selective channel with some degrees of spectral diversity into a number of frequency-nonselective channels, where $\alpha_k[n]$ is IID in $n$.

For all the cases listed above, setting $K = 1$ corresponds to the single receiver antenna scenario, and $\alpha_k[n]$ with $K > 1$ captures the availability of multiple degree of receiver antenna diversity. For this case, we assume that there is a sufficient spatial separation between any pair of antenna elements such that $\alpha_k[n]$'s are independent in $k$.

We assume that the receiver is given the estimates, $\hat{\alpha}_k[n]$, of the fading coefficients $\alpha_k[n]$. The channel estimates $\hat{\alpha}_k[n]$ are assumed to be obtained from the transmission of pilot signals. Specifically, the received pilot signal is of the form

$$y_{p,k}[n] = \sqrt{\mathcal{E}_p}\,\alpha_k[n] + v_k[n]\,, \tag{4.2}$$

where $\mathcal{E}_p$ denotes the pilot signal power and $v_k[n]$'s are independent in $k$, zero-mean, complex-valued, circularly-symmetric stationary Gaussian random variables with variance $\sigma_v^2/2$ per dimension and independent of $\alpha_j[n]$'s for all $1 \le j \le K$. For the case of slow flat fading channels, $\alpha_k[n] = \alpha_k$ and $v_k[n] = v_k$ for all $n$, while for the fast fading channels, $\alpha_k[n]$ and $v_k[n]$ are IID with respect to $n$. The linear minimum mean-square error (MMSE) estimate $\hat{\alpha}_k[n]$ of $\alpha_k[n]$ based on the measurement (4.2) satisfies

$$\begin{aligned} \hat{\alpha}_k[n] &= \alpha_k[n] - \epsilon_k[n] && \text{(4.3a)} \\ &= \frac{\overline{\gamma}_p}{\overline{\gamma}_p + 1}\alpha_k[n] + \frac{\overline{\gamma}_p}{\sqrt{\mathcal{E}_p}\left(\overline{\gamma}_p + 1\right)}v_k[n]\,, && \text{(4.3b)} \end{aligned}$$

where the estimation error $\epsilon_k[n]$ is uncorrelated with $\hat{\alpha}_k[n]$ and

$$\overline{\gamma}_p \triangleq \frac{\mathcal{E}_p}{\sigma_v^2} \tag{4.4}$$

represents the quality of the pilot channel. Utilizing (4.3a), (4.1) can be expressed as

$$y_k[n] = \frac{A}{\sqrt{L}}\,\hat{\alpha}_k[n]c[n]b\left[\left\lfloor\frac{n}{L}\right\rfloor\right] + \frac{A}{\sqrt{L}}\,\epsilon_k[n]c[n]b\left[\left\lfloor\frac{n}{L}\right\rfloor\right] + w_k[n]\,, \tag{4.5}$$

where $\epsilon_k[n]$ in the second term on the right-hand side of (4.5) is a zero-mean Gaussian random variable that is IID with respect to $k$ (and $n$ for fast fading channels).

The receiver antenna diversity setting is of particular interest in the context of privacy, since an asymmetry in the number of antenna elements used by intended and unintended receivers can easily exist. In particular, an unintended receiver may be capable of exploiting larger number of antenna elements, in an effort to detect the information-bearing sequence. This is possible because the degrees of receiver antenna diversity available is limited only by material resource constraints on the receiver and not by the system specifications. Also, receiver antenna diversity settings are often exploited in the fading channels that preclude usage of other forms of diversity. Furthermore, the associated average SNR improvement at the output of receiver antenna diversity combiner is much larger than that associated with temporal or spectral diversity. Thus examination of the receiver antenna diversity helps furnish the extent, in the context of the chaotic DS/SS signaling in this dissertation, of the receiver $\Pr(\epsilon)$ enhancement due to exploiting multiple uncorrelated observations of the same signal. In addition, our findings for slow flat fading channels, coupled with those for AWGN channels in Chapter 3, can provide upper and lower bounds on the unintended receiver performance in other types of fading channels with various types of diversity, and can provide insights regarding the privacy characteristics of chaotic DS/SS over these channels.

## 4.2 Design of Chaotic DS/SS for Fading Channels

In the following we show that the methods for constructing chaotic DS/SS systems that provide privacy over AWGN channels in Chapter 3 remain attractive for providing private communication over the fading channels of interest.

For the class of chaotic DS/SS systems based on $P$-partition maps and on the $P \times Q$ partition maps constructed via the nested recursions in Section 3.3, many of the important relationships between the receiver $\Pr(\epsilon)$ performance and the map parameters hold over both AWGN and fading channels. In particular, the ordering of maps in terms of the associated intended receiver $\Pr(\epsilon)$ is the same for all the channels we consider. This is due to dependence of the intended receiver $\Pr(\epsilon)$ on codeword power PDF.

In fact, for the class of $P \times Q$ partition maps (and hence $P$-partition maps), the *ordering* of maps in terms of the associated privacy benefits they provide is the same for both AWGN and fading channels. In both types of channels, among all $P$-partition maps, $r$-adic maps result in the worst unintended receiver $\Pr(\epsilon)$, and applying the nested recursion algorithms of Section 3.3 monotonically degrades the unintended receiver $\Pr(\epsilon)$ while preserving the intended receiver $\Pr(\epsilon)$. This is because the channel gain $\alpha_k[n]$ in (4.1), while changing the actual privacy characteristics, does not affect the ordering of maps in terms of the associated unintended receiver $\Pr(\epsilon)$. Specifically, for odd map-based DS/SS, the observation pairs $\{y_k[DL-1], y_k[DL]\}$, $D = 1, 2, \cdots$ dominate the optimal decision rules for unintended receivers, for all channels of interest. In particular, only a small number of observations at the boundary between two modulated codewords affect the unintended receiver $\Pr(\epsilon)$. The number of observations sufficient for accurate characterization of the unintended receiver performance depends only on the Lyapunov exponent, and does not grow with

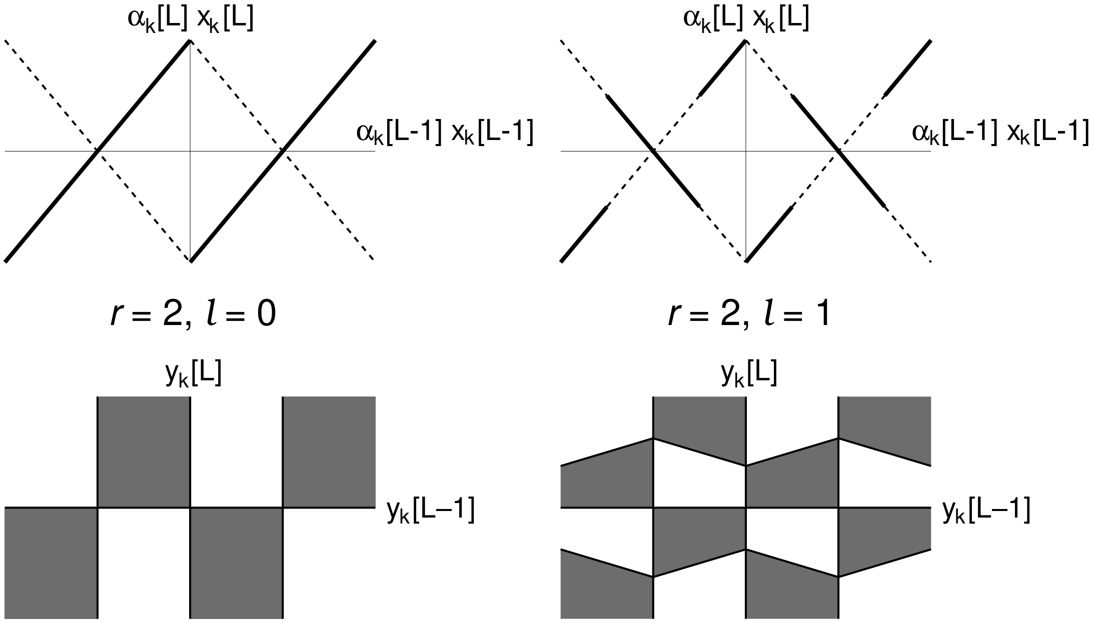


Figure 4.1: The effect of fading on the decision region partitioning of the nested maps $F_{2,0}(\cdot)$ and $F_{2,1}(\cdot)$.

the spreading gain. Most importantly, fading does not affect the *ordering* of maps in terms of the fineness of decision region partitioning, as illustrated in Fig. 4.1. As the figure shows, fading of the form $\alpha_k[n]$ amounts to scaling the axes of the mapping of the received signal components with channel gain but without additive noise, *i.e.*, $\{\alpha_k[n-1]x[n-1], \alpha_k[n]x[n]\}$ and, hence, those of the associated decision regions. Thus, regardless of the channel, $r$-adic maps yield the least favorable decision regions among all $P$-partition maps with the same number of partitions, and increasing the step $\ell$ of the nested recursion implies finer partitioning of decision regions regardless of the channel.

## 4.3 Intended Receiver Performance

In this section we develop methods for evaluating the $\Pr(\epsilon)$ performance of intended receivers for DS/SS communication with nested maps $F_{r,\ell}(\cdot)$ in flat Rayleigh fading. We assume that the intended receivers employ a $K$-element antenna array and possess estimates of the fading coefficients. We first consider slow flat fading channels in Section 4.3.1, then consider fast flat fading channels in Section 4.3.2.

### 4.3.1 Slow Flat Fading

In the following we focus on the evaluation of intended receiver $\Pr(\epsilon)$ in slow flat Rayleigh fading channels, and examine the impact of the availability of multiple independently fading observations of the signal and the quality of channel fading coefficients estimates on the receiver performance.

The optimal (minimum $\Pr(\epsilon)$) detector of the transmitted bit sequence $\mathbf{b}$ in (3.11) for slow fading channels, given the knowledge of $c[0]$ and estimates of $\alpha_k$, utilizes the entire observation set, unlike in Chapter 3. Specifically, assuming that $\mathbf{x}^{NL}$ of the form (3.15) is transmitted and the channel estimates $\hat{\alpha}_k$, $1 \leq k \leq K$, are derived via (4.3) from pilots with quality $\overline{\gamma}_p$ in (4.4) at the receiver, the maximum likelihood (ML) detector of $\mathbf{b}$ based on observations

$$\mathcal{Y} \ = \ \mathcal{Y}^{K,NL} \ \overset{\triangle}{=} \ \{y_k[n];\ k = 1, 2, \cdots, K \text{ and } n = 0, 1, \cdots, NL - 1\} \tag{4.6}$$

is, as shown in App. C.2, given by

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathcal{Y}, c[0]) = \arg\max_{\mathbf{b}} \Bigg\{ & \frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)} \\ & \cdot \sum_{n=0}^{NL-2}\sum_{l=n+1}^{NL-1} F^n(c)F^l(c)\,\mathrm{sgn}\left(b\left[\left\lfloor\frac{n}{L}\right\rfloor\right] b\left[\left\lfloor\frac{l}{L}\right\rfloor\right]\right)\sum_{k=1}^{K}\mathrm{Re}\{y_k^*[n]y_k[l]\} \\ & + \sqrt{\frac{3}{L}}\sum_{n=0}^{NL-1}F^n(c)\,b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\sum_{k=1}^{K}\mathrm{Re}\left\{\hat{\alpha}_k^* y_k[n]\right\}\Bigg\}\,,\end{aligned} \tag{4.7}$$

where the signum function $\mathrm{sgn}(\cdot)$ is defined as

$$\mathrm{sgn}(x) \triangleq \begin{cases} -1\,, & x < 0 \\ 1\,, & x > 0 \end{cases}\,, \tag{4.8}$$

and $\alpha^*$ denotes the complex conjugate of $\alpha$. For the special case of perfect channel estimates ($\overline{\gamma}_p \to \infty$), (4.7) reduces to a simple extension of its counterpart in Chapter 3, *i.e.*, a symbol-by-symbol detector consisting of a time-varying matched filter followed by sampling and a threshold detector. Specifically, the ML detector of the transmitted bit $b[0]$ based on $\mathcal{Y}$ is given by

$$\hat{b}_{\mathrm{ML}}(\mathcal{Y}, c[0]) = \mathrm{sgn}\left(\sum_{n=0}^{L-1} c[n]\,\mathrm{Re}\left\{y[n]\right\}\right)\,, \tag{4.9}$$

where

$$y[n] = \sum_{k=1}^{K} \alpha_k^*\, y_k[n] \tag{4.10}$$

is the signal at the output of the maximal-ratio combiner (MRC) [1, 25, 26] for a $K$-element receiver antenna array with channel gains $\alpha_k$.

The performance characteristics of the optimal intended receiver in slow flat fading, while dependent on the fading of signal amplitudes, are not fundamentally altered by noisy channel estimates. Specifically, the $\Pr(\epsilon)$ of the intended receiver with imperfect channel estimates exhibits trends similar to those in the perfect channel estimation case over the entire range of channel estimation quality values $\overline{\gamma}_p$. In fact, as $\overline{\gamma}_b \to \infty$, the $\Pr(\epsilon)$ curves of the intended receiver in (4.7) with noisy channel estimates converge to the curve that is a 3dB shifted (in SNR) version of the $\Pr(\epsilon)$ associated with perfect channel estimates. This is because, as $\overline{\gamma}_b$ increases, the first term in (4.7), which is independent of $\hat{\alpha}_k$, eventually dominates the decision statistics for all finite $\overline{\gamma}_p$. The 3dB shift arises since the first term in (4.7) is a correlation detector of all the differentials among $b\left[\left\lfloor \frac{n}{L} \right\rfloor\right]$'s based on the observations $y_k[n]y_k[l],\ n \neq l$ with approximately twice the noise variance of the observation $y_k[n]$ for perfect channel estimation case. This is reminiscent of the difference in the performance behavior of differential phase shift keying (DPSK) from its ordinary phase shift keying (PSK) counterpart. Thus, the $\Pr(\epsilon)$ of the detector in (4.7) does not exhibit an error floor, *i.e.*, $\lim_{\overline{\gamma}_b \to \infty} \Pr(\epsilon) = 0$.

The $\Pr(\epsilon)$ trends of the intended receiver, with any level of channel estimate quality $\overline{\gamma}_p$, is fundamentally affected by diversity combining. In particular, in the context of perfect channel estimates and $K$-element receiver antenna diversity, the average SNR per bit at the output of the ML detector (4.9) is a factor of $K$ greater than the average bit SNR per channel (antenna element) [25]. The (instantaneous) SNR per bit at the output of (4.9) associated with a specific spreading vector $\mathbf{c}^L$ is given by

$$\gamma_O \;=\; \gamma_O\left(\mu, \mathbf{c}^L\right) \;=\; 3\,\mu\,\overline{\gamma}_b\,\mathcal{E}\left(\mathbf{c}^L\right)\,, \tag{4.11}$$

where

$$\mu \;\triangleq\; \sum_{k=1}^{K} |\alpha_k|^2\,. \tag{4.12}$$

Thus the average output SNR is

$$\overline{\gamma}_O \overset{\triangle}{=} E\left[\gamma_O\right] = K\,\overline{\gamma}_b\,. \tag{4.13}$$

The $\Pr(\epsilon)$ evaluation metrics for intended receivers with perfect channel estimates in slow flat fading can be established by straightforward extensions of those for AWGN channels in Chapter 3. These metrics can be useful in illustrating the $\Pr(\epsilon)$ behavior for all $\overline{\gamma}_p$, especially in the high SNR range, due to the dominance of the first term in (4.7). Concise forms of these metrics can be obtained by utilizing the bit error probability conditioned on $\mathbf{c}^L$, derived in App. C.3. As shown in the appendix, $\gamma_O$ in (4.11) is a chi-square-distributed random variable with $2K$ degrees of freedom. Consequently, the $\Pr(\epsilon)$ expression (3.6) extends to the following form

$$\begin{aligned}\Pr(\epsilon) &= E\left[E\left[E\left[\mathcal{Q}\left(\sqrt{2\gamma_O\left(\mu,\{\mathbf{s}^{L-1},c[L-1]\}\right)}\right)\middle|\,\mathbf{s}^{L-1}\right]\middle|\,c[L-1]\right]\right]\\ &= \frac{1}{2\,r^{L-1}}\sum_{i=1}^{r^{L-1}}\int_{-1}^{+1}\mathrm{Pc}\big(K,\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\}\right)\big)\,dc\,,\end{aligned} \tag{4.14}$$

where

$$\begin{aligned}\mathrm{Pc}\big(K,\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\}\right)\big) &\overset{\triangle}{=} \Pr(\epsilon|\mathbf{c}^L)\\ &= \left[\frac{1}{2}\left(1-\sqrt{\frac{\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\}\right)}{1+\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\}\right)}}\right)\right]^K\\ &\quad\cdot\sum_{k=0}^{K-1}\binom{K-1+k}{k}\left[\frac{1}{2}\left(1+\sqrt{\frac{\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\}\right)}{1+\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\},\right)}}\right)\right]^k\,,\end{aligned} \tag{4.15}$$

and $\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\}\right)$ is the average bit SNR per channel conditioned on $\mathbf{c}^L$, *i.e.*,

$$\overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_i,c\}\right) = \overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right) = 3\,\overline{\gamma}_b\mathcal{E}\left(\mathbf{s}_i,c\right)\ .$$

Similarly, the approximation (3.7) for $r = 2$ extends to

$$\Pr(\epsilon) \ \approx\ \frac{1}{2^L}\sum_{e=0}^{L-1}\binom{L-1}{e}\int_{-1}^{+1}\mathrm{Pc}\big(K, \overline{\gamma}_{b|\mathbf{c}^L}\left(\{\mathbf{s}_e, c\}\right)\big)\, dc\,. \tag{4.16}$$

Upper and lower bounds on $\Pr(\epsilon)$ can be obtained via the same techniques employed in Sec. 3.1. Specifically, the lower bound is given by

$$\Pr(\epsilon) \ \geq\ \mathrm{Pc}\big(K, E\left[\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)\right]\big) \ =\ \mathrm{Pc}(K, \overline{\gamma}_b)\ , \tag{4.17}$$

while the upper bound is given by

$$\Pr(\epsilon) \ \leq\ \mathrm{Pc}\bigg(K, 3\,\overline{\gamma}_b \min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right)\bigg)\ , \tag{4.18a}$$

and is well approximated by

$$\lim_{L\to\infty}\Pr(\epsilon) \ \leq\ \mathrm{Pc}\bigg(K, \frac{3\,\overline{\gamma}_b}{(P+1)^2}\bigg)\ . \tag{4.18b}$$

For slow flat fading channels, another computationally efficient metric of intended receiver $\Pr(\epsilon)$ can be obtained by applying the Gaussian approximation on $\overline{\gamma}_{b|\mathbf{c}^L}$;

$$3\,\frac{\mathcal{E}_b}{N_o}\,\mathcal{E}\left(\mathbf{c}^L\right) \ \overset{L\to\infty}{\longrightarrow}\ \mathcal{N}(m, \sigma^2)\,, \tag{4.19}$$

where $\mathcal{N}(m, \sigma^2)$ denotes, with some abuse of notation, a real-valued Gaussian random variable with mean $m$ and variance $\sigma^2$, and where the convergence is in the cumulative sense. For nested maps $F_{r,\ell}(\cdot)$ with even $r$, $\min_{\mathbf{c}^L}\mathcal{E}\left(\mathbf{c}^L\right)$ is nonzero as shown in Section 2.2.2. Furthermore, for sufficiently large $L$, the sequence power $\mathcal{E}\left(\mathbf{c}^L\right)$ can be modeled as a Gaussian random variable that does not take values below some finite $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$, *i.e.*, $p_{\mathcal{E}(\mathbf{c}^L)}(e) = 0$ for $e \leq \min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$. This Gaussian approximation arises from the application of the Lindeberg-Feller central limit theorem [27,28]; given $s_n^2 = \sum_{n=0}^{L-1} \text{var}(c^2[n])$ (where $\text{var}(\nu)$ denotes the variance of $\nu$), $\overline{\gamma}_{b|\mathbf{c}^L}$ satisfies the Lindeberg condition;

$$\lim_{L\to\infty} \frac{1}{L} \sum_{n=0}^{L-1} E\left[ \frac{\left(c^2[n] - E\left[c^2[n]\right]\right)^2}{s_n^2} \,\middle|\, \left|c^2[n] - E\left[c^2[n]\right]\right| > \epsilon s_n \right] = 0$$

for all $\epsilon > 0$. The Gaussian approximation leads to the following approximation of the $\Pr(\epsilon)$:

$$\begin{aligned} \Pr(\epsilon) &= E\left[E\left[\mathcal{Q}\left(\sqrt{\gamma_O}\right)|\overline{\gamma}_{b|\mathbf{c}^L}\right]\right] \\ &\approx \int_0^\infty \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{-\frac{(\gamma - m)^2}{2\sigma^2}\right\} \text{Pc}(K, \gamma)\; d\gamma\,, \end{aligned} \tag{4.20}$$

where $m = \mathcal{E}_b/N_o$ and

$$\sigma^2 = 9\left(\frac{\mathcal{E}_b}{N_o}\right)^2 \left[\frac{1}{L} E\left[c^4[n]\right] + \frac{2}{L^2} \sum_{l=1}^{L-1} (L - l)\, E\left[c^2[n]c^2[n+l]\right]\right] - m^2\,.$$

The correlation metrics $E\left[c^2[n]c^2[n+l]\right]$ can be computed through efficient methods provided in [19]. Fig. 4.2 compares the intended receiver $\Pr(\epsilon)$ approximated via (4.20) with the analytic solutions via (4.14) and (4.16). As the figure shows, numerical integration of (4.20) results in an accurate approximation of the intended receiver performance. This is because the effect of the missing tail of the clipped Gaussian distribution on $\Pr(\epsilon)$ is largely suppressed in the fading channels of interest. This is a direct consequence of the distribution of $\mu$ in (4.12), which determines the statistical characteristics of $\gamma_O$ in (4.11). Specifically, as shown in App. C.3, $\mu$ is a chi-square-

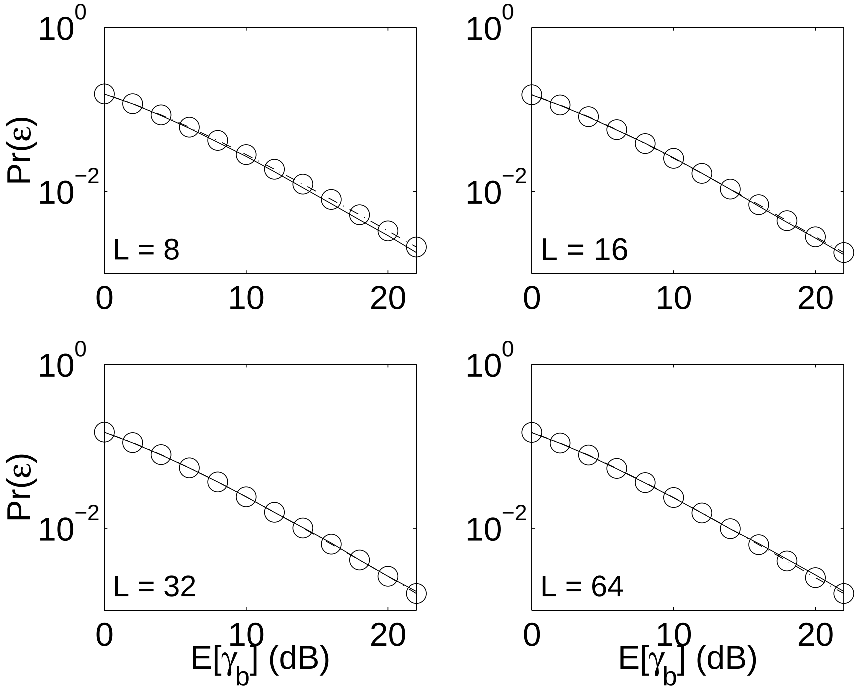


Figure 4.2: Accuracy of Gaussian approximation of intended receiver $\Pr(\epsilon)$ for dyadic map, $K = 1$, and $\overline{\gamma}_p \to \infty$. Solid curves indicate analytically computed $\Pr(\epsilon)$ ((4.14) for $L = 8$ and 16, (4.16) for $L = 32$ and 64), and dash-dot curves with circles represent analytically computed $\Pr(\epsilon)$ approximation (4.20).

distributed random variable with $2K$ degrees of freedom. Hence $\mu$ has a sizable portion of its PDF in the closed interval $[0, \mu']$ for any $\mu' > 0$, and dominates the intended receiver $\Pr(\epsilon)$ performance over $\mathbf{c}^L$.

Fig. 4.3 shows the intended receiver $\Pr(\epsilon)$ performance as a function of SNR for various levels of channel estimate quality $\overline{\gamma}_p$. The figure suggests that the $\Pr(\epsilon)$ in the case of perfect channel estimates at the receiver ($\overline{\gamma}_p \to \infty$) can serve as a metric for determining the high SNR performance characteristics in the presence of noisy channel estimates at the receiver. Indeed, Fig. 4.3 verifies our preceding analysis that the $\Pr(\epsilon)$ curves of the intended receiver with imperfect channel estimates asymptotically converge, as $\overline{\gamma}_b$ increases, to the curve that is 3 dB shifted in SNR from the $\Pr(\epsilon)$ associated with perfect channel estimates. This shifted curve, as the figure shows,

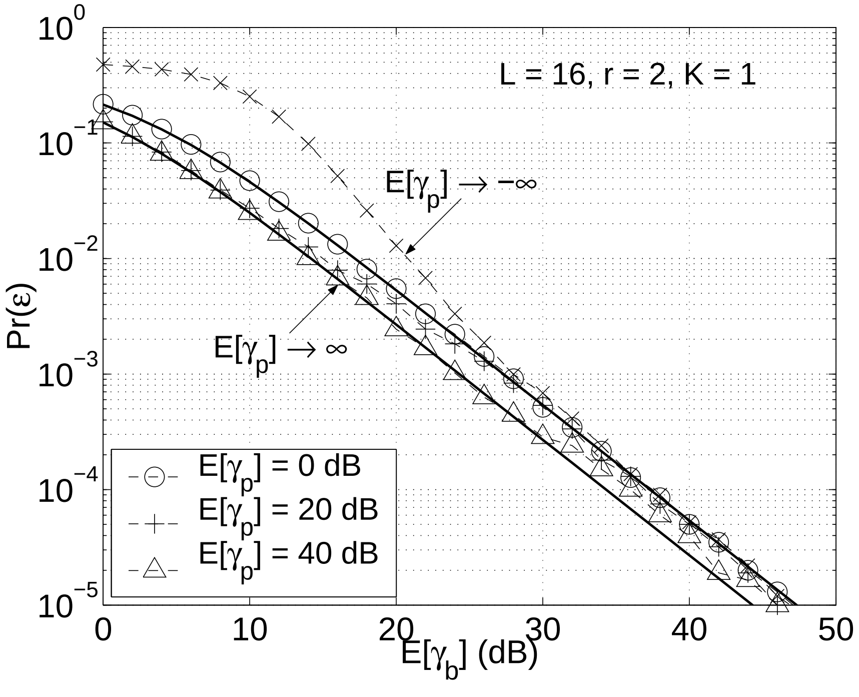


Figure 4.3: Intended receiver $\Pr(\epsilon)$ performance vs. $\overline{\gamma}_b$ for various level of pilot quality $\overline{\gamma}_p$. Dashed curves with markers represent simulated $\Pr(\epsilon)$ associated with imperfect channel estimation (4.7). Lower solid curve represents analytically computed $\Pr(\epsilon)$ (4.14) for perfect channel estimation and upper solid curve represents 3 dB shifted copy of the lower curve.

provides an upper bound to the $\Pr(\epsilon)$ curves for all $\overline{\gamma}_p \geq 0$ dB, and an accurate approximation for a wide range of $\overline{\gamma}_b$ and $\overline{\gamma}_p$.

Fig. 4.4 shows the intended receiver $\Pr(\epsilon)$ curves vs. SNR as functions of the number of receiver antenna elements $K$ in the case that perfect channel estimates are available at the receiver. As the figure reveals, for DS/SS based on nested maps $F_{r,\ell}(\cdot)$, with $r$ an even number, the intended receiver can achieve full diversity. Specifically, the $\Pr(\epsilon)$ of an intended receiver exploiting $K$ independently fading observations of the same signal decays as $1/\overline{\gamma}_b^K$ for high $\overline{\gamma}_b$. This is because $\min_{\mathbf{c}^L} \mathcal{E}\left(\mathbf{c}^L\right)$ is bounded away from zero for the spreading sequences from nested maps. In general, intended receivers can achieve full diversity irrespective of the channel estimation quality, since

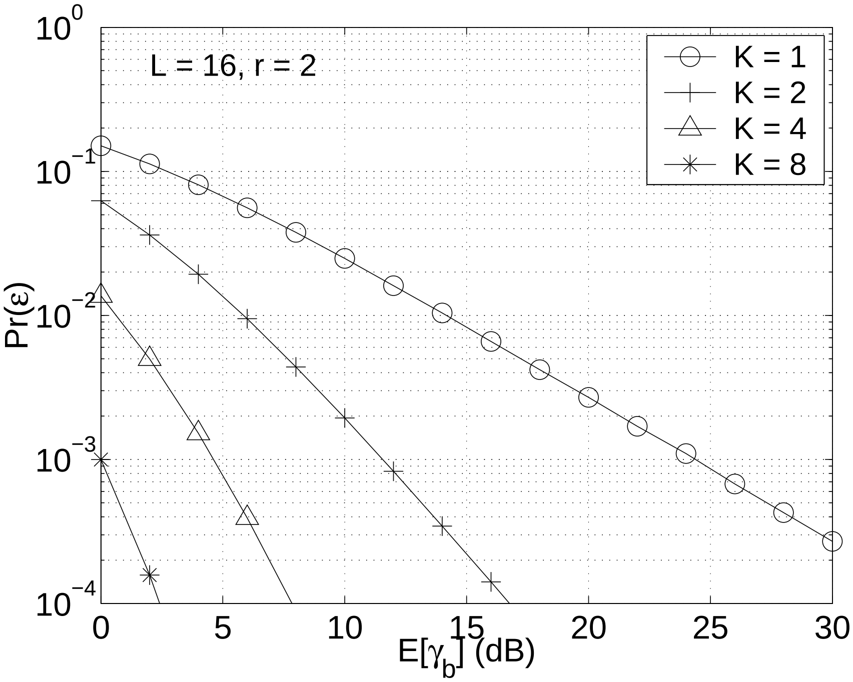


Figure 4.4: Analytically computed intended receiver $\Pr(\epsilon)$ (4.14) vs. $\overline{\gamma}_b$ for various number of receiver antenna elements $K$ and perfect channel estimation.

the asymptotic behavior of $\Pr(\epsilon)$ at high SNR is the same for all $\overline{\gamma}_p$. We remark that, with suitable extensions of the $\Pr(\epsilon)$ evaluation techniques developed in this section, we can show that the intended receivers can achieve full diversity benefits over channels with other commonly used forms of diversity.

### 4.3.2 Fast Flat Fading

In this section we focus on the evaluation of the intended receiver $\Pr(\epsilon)$ in fast flat Rayleigh fading channels, and examine the impact of diversity combining and fading channel estimate quality on the receiver performance.

The time selectivity of fading coefficients has pronounced effects on the intended receiver structure and its performance in the context of partial channel state information at the receiver. Specifically, in contrast to the slow fading case considered in Section 4.3.1, the optimal intended receiver in fast flat fading with channel estimates $\hat{\alpha}_k$ is a symbol-by-symbol detector for any channel estimate quality $\overline{\gamma}_p$. Assuming that $\mathbf{x}^{NL}$ of the form (3.15) is transmitted and the channel estimates $\hat{\alpha}_k[n]$, $1 \leq k \leq K$ and $0 \leq n \leq NL - 1$, are derived via (4.3), the maximum likelihood detector of the transmitted bit $b[0]$ based on observations $\mathcal{Y}$ in (4.6) is, as shown in App. C.4, given by

$$\hat{b}_{\mathrm{ML}}(\mathcal{Y}, c[0]) = \mathrm{sgn}\left(\sum_{n=0}^{L-1} \frac{c[n]\,\mathrm{Re}\left\{y[n]\right\}}{\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\,c^2[n]+1}\right), \tag{4.21}$$

where

$$y[n] \;=\; \sum_{k=1}^{K} \hat{\alpha}_k^*[n]\,y_k[n] \tag{4.22}$$

is the output of the MRC. The (instantaneous) SNR, $\gamma_O$, at the output of the detector (4.21) in this case can be obtained by using (4.22) and (4.5) to expand the decision statistic

$$U \;\triangleq\; \sum_{n=0}^{L-1} \frac{c[n]\,\mathrm{Re}\left\{y[n]\right\}}{\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\,c^2[n]+1}$$

and taking the ratio of $E\left[U\right]^2$ and the variance of $U$. Thus we have

$$\gamma_O \;=\; \frac{\left(\sum_{n=0}^{L-1} \frac{c^2[n]\mu[n]}{\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\,c^2[n]+1}\right)^2}{\frac{1}{\overline{\gamma}_p+1}\sum_{n=0}^{L-1} \frac{c^4[n]\mu[n]}{\left(\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\,c^2[n]+1\right)^2} + \frac{L}{3\overline{\gamma}_b}\sum_{n=0}^{L-1} \frac{c^2[n]\mu[n]}{\left(\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\,c^2[n]+1\right)^2}}, \tag{4.23}$$

where

$$\mu[n] \;\triangleq\; \sum_{k=1}^{K} \left|\hat{\alpha}_k[n]\right|^2 . \tag{4.24}$$

The asymptotic behavior of $\gamma_O$ as $\overline{\gamma}_b \rightarrow \infty$ suggests that the intended receiver $\Pr(\epsilon)$

in fast fading exhibits an error floor for finite $\overline{\gamma}_p$. In particular,

$$\lim_{\overline{\gamma}_b \to \infty} \gamma_O = \left(\overline{\gamma}_p + 1\right) \sum_{n=0}^{L-1} \mu[n] \,. \tag{4.25a}$$

We can take expectation of (4.25a) and interchange the expectation and the limit using the Lebesque dominated convergence theorem [23], obtaining

$$\lim_{\overline{\gamma}_b \to \infty} \overline{\gamma}_O = K\, L\, \overline{\gamma}_p \,. \tag{4.25b}$$

As a result, in contrast to the slow fading case, the $\Pr(\epsilon)$ performance of the intended receiver in fast fading with noisy channel estimates cannot be adequately characterized by its counterpart with perfect channel estimates. The asymptotic behavior of $\gamma_O$, however, also suggests that the level of the error floor decreases as the number of antenna array elements and the spreading gain increase. The form of (4.25) also implies that diversity combining remains an attractive avenue for improving the $\Pr(\epsilon)$ performance over fast fading channels. This observation is further reinforced by the behavior of $\overline{\gamma}_O$ in the limiting case of $\overline{\gamma}_p \to \infty$;

$$\lim_{\overline{\gamma}_p \to \infty} \overline{\gamma}_O = K\, \overline{\gamma}_b \,,$$

which, in conjunction to (4.25), suggests that the independence of channel gain with respect to receiver antenna elements leads to a $K$-fold increase in SNR for the general scenario of imperfect channel estimates at the receiver, as in Section 4.3.1.

While difficult in general, analytical evaluation of the intended receiver $\Pr(\epsilon)$ is feasible in the limiting case $\overline{\gamma}_b \to \infty$ with finite $\overline{\gamma}_p$. Since $\lim_{\overline{\gamma}_b \to \infty} \gamma_O$ in (4.25a) is a chi-square-distributed random variable with $2KL$ degrees of freedom, the error

| $\overline{\gamma}_p$ (dB) | $K \cdot L = 4$ | $K \cdot L = 16$ | $K \cdot L = 64$ |
|---:|:---:|:---:|:---:|
| 0 | 1.1102e-02 | 1.4689e-06 | 2.6778e-021 |
| 10 | 9.6983e-06 | 1.5925e-18 | 8.2735e-069 |
| 20 | 1.3191e-09 | 5.9956e-34 | 1.8708e-130 |
| 30 | 1.3623e-13 | 6.8897e-50 | 3.3029e-194 |
| 40 | 1.3667e-17 | 6.9866e-66 | 3.4970e-258 |

Table 4.1: Analytically computed error floor (4.26) of the intended receiver with $K$-element receiver antenna array for spreading gain $L$ in fast flat fading.

floor associated with a given $\overline{\gamma}_p$ level can be readily obtained via a method similar to the one in App. C.3. Specifically, the $\Pr(\epsilon)$ of the intended receiver employing a $K$-element receiver antenna array for chaotic DS/SS with spreading gain $L$ asymptotically approaches, as $\overline{\gamma}_b$ increases,

$$\lim_{\overline{\gamma}_b \to \infty} \Pr(\epsilon) = \left[\frac{1}{2}\left(1 - \sqrt{\frac{\overline{\gamma}_p}{1+\overline{\gamma}_p}}\right)\right]^{KL} \sum_{k=0}^{KL-1} \binom{KL-1+k}{k} \left[\frac{1}{2}\left(1 + \sqrt{\frac{\overline{\gamma}_p}{1+\overline{\gamma}_p}}\right)\right]^{k} . \quad (4.26)$$

This error floor helps characterize the performance trends at high SNR, and is tabulated in Table 4.1. The table shows that the error floor is very low for a wide range of $K$ and $L$ values, and rapidly becomes insignificant with increasing spreading gains or numbers of antenna array elements.

Fig. 4.5 depicts the intended receiver $\Pr(\epsilon)$ trends vs. SNR for various channel estimate quality levels. As the figure suggests, the slope of the curves associated with finite $\overline{\gamma}_p$ does indeed taper off to an asymptotic plateau as $\overline{\gamma}_b$ increases, consistent with the preceding analysis that $\Pr(\epsilon)$ exhibits the error flooring effect. However, the adverse effects of noisy channel estimation on the $\Pr(\epsilon)$ does not become apparent for a very wide range of spreading gains and receiver antenna array sizes. This is a consequence of the steep reduction of the error floor as $\overline{\gamma}_p$, $L$, and $K$ increase, as

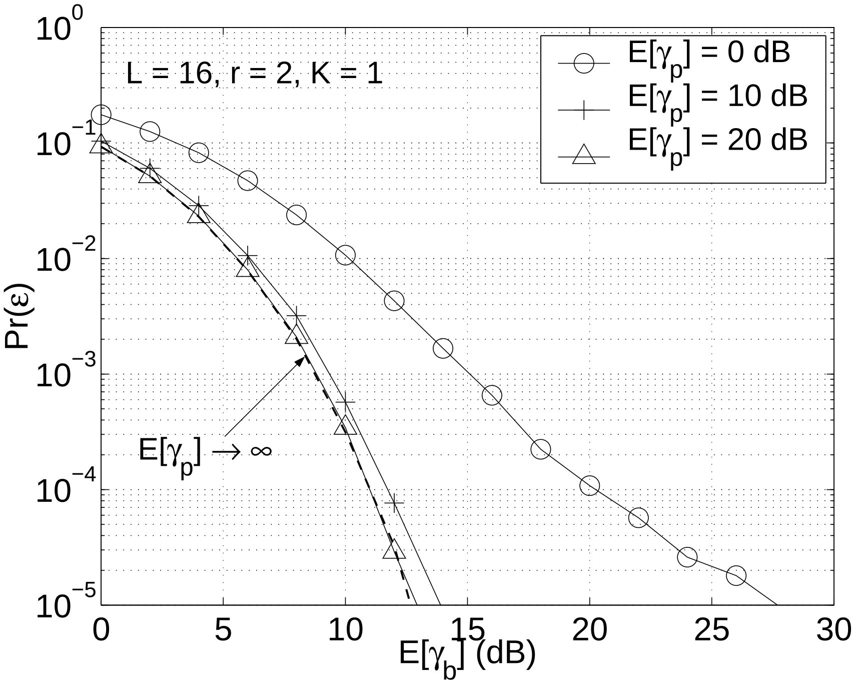


Figure 4.5: Simulated intended receiver $\Pr(\epsilon)$ (4.21) vs. $\overline{\gamma}_b$ for various level of pilot quality $\overline{\gamma}_p$. The dashed curve indicate the $\Pr(\epsilon)$ curve for perfect channel estimation, and the solid curves with markers indicate the $\Pr(\epsilon)$ curves for imperfect channel estimation.

shown in Table 4.1.

Figs. 4.6 and 4.7 illustrate the impact of diversity combining on the intended receiver performance in fast flat fading. For the case of perfect channel estimates at the receiver, the $\Pr(\epsilon)$ of the intended receiver exploiting the independence of $\alpha_k[n]$ with respect to $k$ and $n$ decays as $1/\overline{\gamma}_b^{KL}$ at high $\overline{\gamma}_b$. The figures also confirm our analysis that the performance improvement due to diversity combining reception largely mitigates the effects of imperfect channel estimation on the $\Pr(\epsilon)$ for a wide range of values of $\overline{\gamma}_p$, $L$, and $K$ that are of practical interest. The error floor, suggested for the very small spreading gain of 4 in Fig. 4.6, is consistent with the analytic prediction listed in Table 4.1.

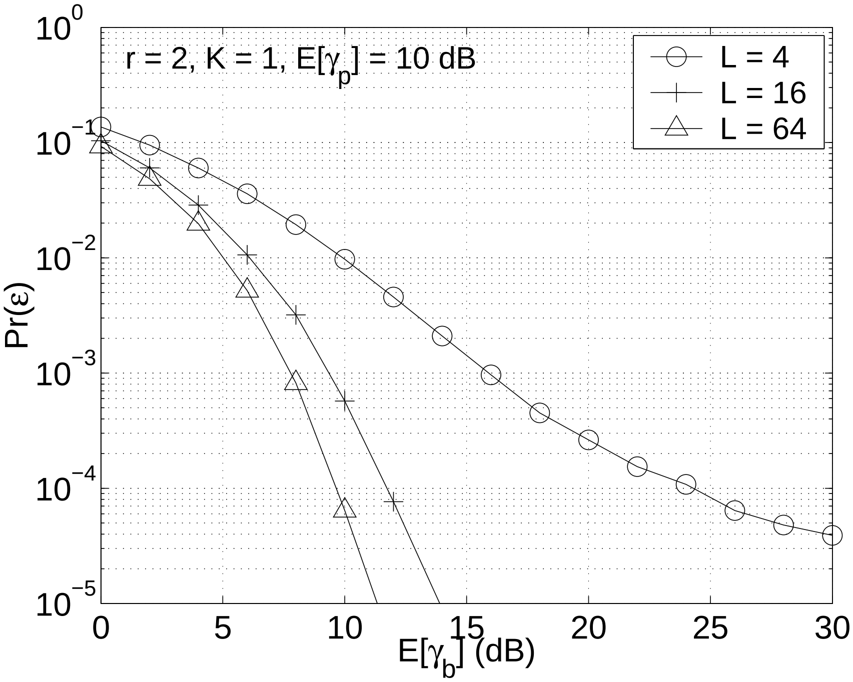


Figure 4.6: Simulated intended receiver $\Pr(\epsilon)$ vs. $\overline{\gamma}_b$ for various spreading gain $L$.

## 4.4 Unintended Receiver Performance

In this section we characterize the unintended receiver $\Pr(\epsilon)$ performance with a $K$-element receiver antenna array and channel estimates at the receiver for DS/SS communication with nested maps $F_{r,\ell}(\cdot)$ in Rayleigh fading. As in Section 3.2, we assume that the unintended receiver has complete knowledge of the modulation scheme including the chaotic map, but does not know the initial condition $c[0]$. In Section 4.4.1, we develop computationally viable metrics for evaluating the unintended receiver $\Pr(\epsilon)$ in slow flat fading, while in Section 4.4.2 we consider the fast flat fading case, using extension of the methods developed in Section 3.2.4. In Section 4.4.3, we derive the asymptotic decaying rate of the unintended receiver $\Pr(\epsilon)$ for the systems of interest over slow flat fading channels. We show that this decaying rate, coupled with its counterpart for AWGN channels in Section 3.2.3, can be used to help deduce

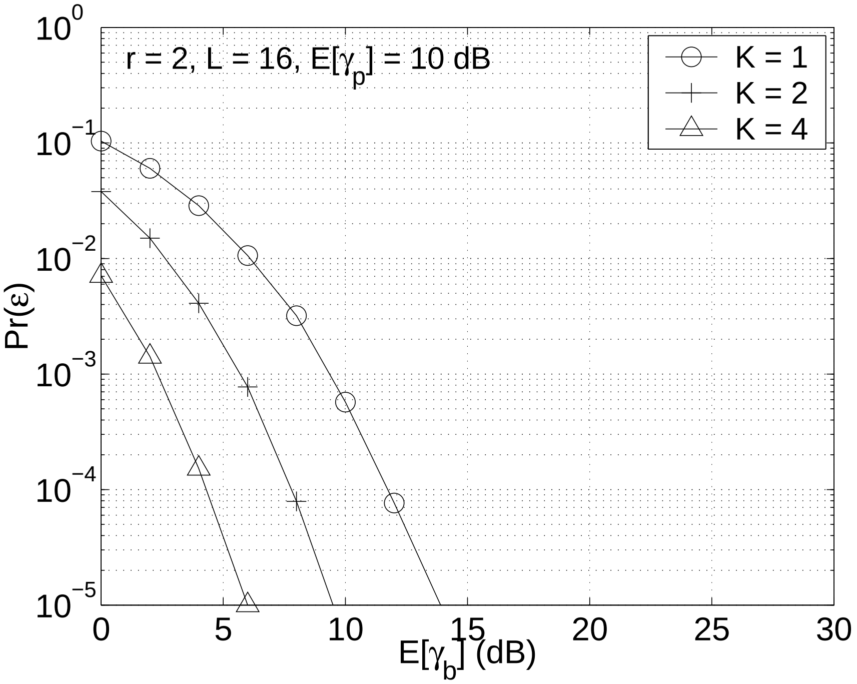


Figure 4.7: Simulated intended receiver $\Pr(\epsilon)$ vs. $\overline{\gamma}_b$ for various number of receiver antenna elements $K$.

the dependence of the unintended receiver performance on SNR.

### 4.4.1 Slow Flat Fading

In the following we develop computationally viable methods for evaluating the unintended receiver $\Pr(\epsilon)$ in slow flat Rayleigh fading for DS/SS signaling with the class of nested maps $F_{r,\ell}(\cdot)$ in Section 3.3. The methods herein can be readily extended to the class of odd $P \times Q$ partition maps and all the fading channel models captured by (4.1).

Using the results in App. C.4, the maximum-likelihood unintended detector, given the observation $\mathcal{Y}_{K,NL}$ in (4.6), corresponding to $\mathbf{b}$ in (3.11) and channel estimates

$$\hat{\mathbf{a}} \triangleq \begin{bmatrix} \hat{\alpha}_1 & \hat{\alpha}_2 & \cdots & \hat{\alpha}_K \end{bmatrix}^{\mathrm{T}} \tag{4.27}$$

derived from the pilot signal of quality $\overline{\gamma}_p$ in (4.4) at the receiver, is given by

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathcal{Y}) &= \arg\max_{\mathbf{b}} \int p_{\mathcal{Y}|\mathbf{b},c,\hat{\mathbf{a}}}(\mathcal{Y}|\mathbf{b},c,\hat{\mathbf{a}})\, p_{c[0]}(c)\, dc \\ &= \arg\max_{\mathbf{b}} \int \exp\left\{ -\frac{\mathrm{Re}\{\Psi(\mathcal{Y}|\mathbf{b},c,\hat{\mathbf{a}})\}}{N_o\left(\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\sum_{n=0}^{NL-1}\left(F^n(c)\right)^2+1\right)} \right\} p_{c[0]}(c)\, dc\,, \qquad (4.28)\end{aligned}$$

where the statistic $\Psi\left(\mathcal{Y}|\mathbf{b},c,\hat{\mathbf{a}}\right)$ for $c[0]=c$ is given by

$$\begin{aligned}\Psi(\mathcal{Y}|\mathbf{b},c,\hat{\mathbf{a}}) \triangleq \sum_{k=0}^{K} \Bigg\{ & \sum_{n=0}^{NL-1} |y_k[n]|^2 + \frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)} \Bigg( \sum_{n=0}^{NL-1} \sum_{l\neq n}^{NL-1} \left(F^l(c)\right)^2 |y_k[n]|^2 \\ & - 2 \sum_{n=0}^{NL-2} \sum_{l=n+1}^{NL-1} F^n(c) F^l(c)\, \mathrm{sgn}\left( b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] b\left[\left\lfloor \frac{l}{L} \right\rfloor\right] \right) y_k^*[n] y_k[l] \Bigg) \\ & - 2\,\hat{\alpha}_k^* \sqrt{\frac{3}{L}} \sum_{n=0}^{NL-1} F^n(c)\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] y_k[n] + |\hat{\alpha}_k|^2\, \frac{3\,\mathcal{E}_b}{L} \sum_{n=0}^{NL-1} \left(F^n(c)\right)^2 \Bigg\}\,. \qquad (4.29)\end{aligned}$$

For the special case of perfect channel estimation ($\overline{\gamma}_p \to \infty$), (4.28) reduces to

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathcal{Y}) &= \arg\max_{\mathbf{b}} \int \exp\Bigg\{ \frac{1}{N_o} \sum_{n=0}^{NL-1} \Bigg( 2\sqrt{\frac{3}{L}} F^n(c) b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] \mathrm{Re}\{y[n]\} \\ &\qquad - \mu \frac{3\,\mathcal{E}_b}{L} \left(F^n(c)\right)^2 \Bigg) \Bigg\}\, p_{c[0]}(c)\, dc\,, \qquad (4.30)\end{aligned}$$

where $y[n]$ is the signal at the output of MRC (4.10) and $\mu$ is as in (4.12). Thus the sequence of $y[n]$,

$$\mathbf{y} = \mathbf{y}^{NL} = \begin{bmatrix} y[0] & y[1] & \cdots & y[NL-1] \end{bmatrix}^{\mathrm{T}}, \qquad (4.31)$$

as a function of $\mathcal{Y}_{K,NL}$ is a sufficient statistic for $\mathbf{b}$ in the context of unintended detection given perfect channel estimates. As is the case for its counterpart in AWGN

(3.12) in Section 3.2.1, direct implementations of (4.28) and (4.30) are impractical except for very small values of $N$, $L$, and $r$, since each of the $2^{N-1}$ likelihoods requires computation of $r^{NL}$ integrals.

Computationally viable $\Pr(\epsilon)$ metrics for the class of nested map-based DS/SS can be readily constructed via extensions of the performance evaluation methods in Section 3.2.4. Specifically, with the assumption that the unintended receiver is provided with $b[0]$, $\{i[n];\ 1 \leq n \leq N-1,\ n \neq D\}$ where $b[n] = i[n]\,b[n-1]$, and knowledge of $c[0] \in \{c[m];\ m = 0, 1, \ldots, M_o - 1\}$ for some $M_o$ significantly larger than the observation interval $NL$, the ML detector of $i[D]$ in (3.19) extends to

$$\hat{i}_{\mathrm{LB}}(\mathcal{Y}) \;=\; \arg\max_{i\in\pm1} \sum_{m=0}^{M_o-1} \exp\left\{ -\frac{\mathrm{Re}\{\Psi\left(\mathcal{Y}|\mathbf{b}, c[m], \hat{\mathbf{a}}\right)\}}{N_o\left(\frac{3\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)} \sum_{n=0}^{NL-1} \left(F^n(c[m])\right)^2 + 1\right)} \right\} . \qquad (4.32)$$

In the case of perfect channel estimates, (4.32) specializes to

$$\begin{aligned} \hat{i}_{\mathrm{LB}}(\mathbf{y}) \;=\; \arg\max_{\mathbf{b}} \sum_{m=0}^{M_o-1} \exp\Bigg\{ \frac{1}{N_o} \sum_{n=0}^{NL-1} \Bigg( & 2\sqrt{\frac{3}{L}} F^n(c[m])\, b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] \mathrm{Re}\{y[n]\} \\ & - \mu \frac{3\,\mathcal{E}_b}{L} \left(F^n(c[m])\right)^2 \Bigg) \Bigg\} . \qquad (4.33) \end{aligned}$$

As in Section 3.2.4, exploiting the dominance of a small set of observations around the codeword boundaries on the $\Pr(\epsilon)$ due to the sensitive dependence of spreading sequences on initial conditions, computationally efficient approximations to the $\Pr(\epsilon)$ can be obtained by simulating (4.32) or (4.33) with $\mathcal{Y}$ replaced by a windowed observation vector

$$\mathcal{Y}_w \overset{\triangle}{=} \{y_k[n];\ k = 1, 2, \cdots, K \ \text{ and } \ n = DL-w, DL-w+1, \cdots, DL+w-1\} \ , \quad (4.34)$$

for $1 \leq w \leq (N-1)L$ and $1 \leq D \leq N-1$. Upper bounds on the unintended receiver $\Pr(\epsilon)$ can be similarly obtained by considering the optimum detector of $i[D]$ given the windowed observation $\mathcal{Y}_1$. This detector is also the optimum detector for the simpler binary-signaling-in-slow-fading problem, with sets of constellation points

$$\hat{\mathbf{c}}_{i,j} = \begin{bmatrix}\hat{c}_{i,j}[0] & \hat{c}_{i,j}[1]\end{bmatrix}^{\mathrm{T}} \triangleq \begin{bmatrix}\frac{2(j-1)-(P-1)}{P} & \frac{i(-1)^j(Q-2j+1)}{Q}\end{bmatrix}^{\mathrm{T}},\ i \in \pm 1,\ j = 1, 2, \ldots, P\ , \tag{4.35}$$

where $Q = 2^{\ell+1}$ and $P = rQ$ for nested maps. Via extensions of the method in App. C.2, this detector can be shown to be

$$\begin{aligned}\hat{i}_{\mathrm{UB}}(\mathcal{Y}_1) \ = \ \arg\min_i \min_j \ & \frac{1}{\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\left(\hat{c}^2_{i,j}[0]+\hat{c}^2_{i,j}[1]\right)+1} \operatorname{Re}\Bigg\{\sum_{k=1}^{K}\Big(|y_k[DL-1]|^2+|y_k[DL]|^2 \\ & + \frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\left|\hat{c}_{i,j}[1]y_k[DL-1]-\hat{c}_{i,j}[0]y_k[DL]\right|^2 \\ & - 2\,\hat{\alpha}^*_k\sqrt{\frac{3\,\mathcal{E}_b}{L}}\left(\hat{c}_{i,j}[0]y_k[DL-1]+\hat{c}_{i,j}[1]y_k[DL]\right) \\ & + |\hat{\alpha}_k|^2\,\frac{3\,\mathcal{E}_b}{L}\left(\hat{c}^2_{i,j}[0]+\hat{c}^2_{i,j}[1]\right)\Big)\Bigg\}\ . \end{aligned} \tag{4.36}$$

In the perfect channel estimates case, (4.36) simplifies to the following minimum distance detector:

$$\hat{i}_{\mathrm{UB}}(\mathbf{y}_1) = \arg\min_i \min_j \left\| \operatorname{Re}\left\{\mathbf{y}_1\right\} - \mu\sqrt{\frac{3\,\mathcal{E}_b}{L}}\hat{\mathbf{c}}_{i,j}\right\|^2\ , \tag{4.37}$$

where the vector of the MRC outputs

$$\mathbf{y}_w \triangleq \begin{bmatrix}y[DL-w] & y[DL-w+1] & \cdots & y[DL+w-1]\end{bmatrix}^{\mathrm{T}},\ 1 \leq w \leq (N-1)L \tag{4.38}$$

is a windowed version of (4.31).

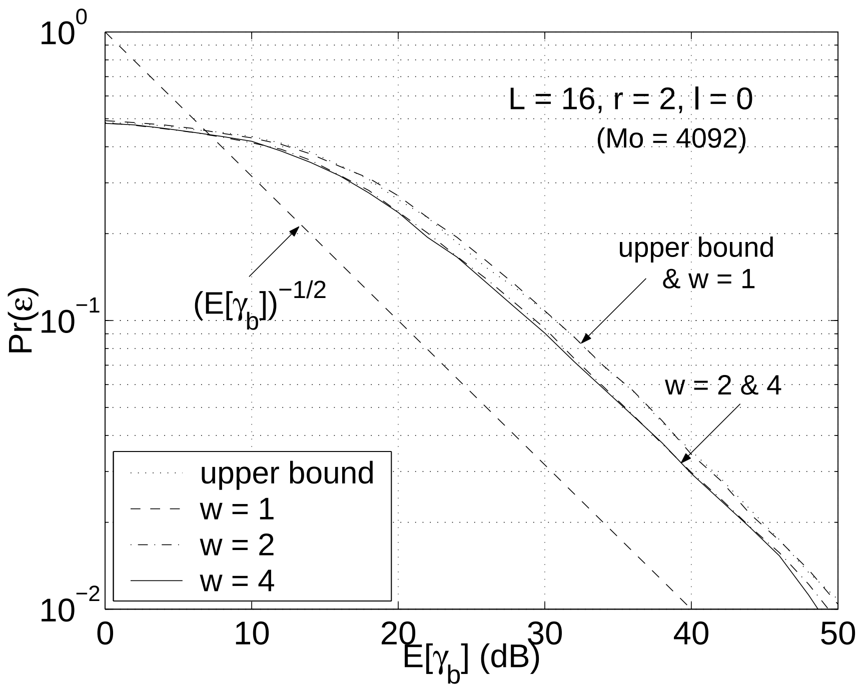


Figure 4.8: Simulated upper bound (4.37) and approximations to lower bound (4.33) on the unintended receiver $\Pr(\epsilon)$ for various values of $w$.

Fig. 4.8 shows the simulated upper bound (4.37) and approximations to the lower bound (4.33) on the $\Pr(\epsilon)$ of the unintended receiver for dyadic map-based DS/SS in slow flat fading as functions of $\overline{\gamma}_b$ for various values of the window size indicator $w$. The figure reveals that, for the dyadic map ($r = 2, \ell = 0$), the approximation with $w = 1$ nearly coincides with the upper bound and rapidly converges as $w$ increases, revealing that the approximations to (4.33) and the upper bound based on (4.37) predict the $\Pr(\epsilon)$ trends of unintended receivers with perfect channel estimates. The same trends are empirically observed with nested map DS/SS and imperfect channel estimates.

Fig. 4.9 depicts the unintended receiver $\Pr(\epsilon)$ performance in slow fading as a function of SNR for various levels of channel estimate quality $\overline{\gamma}_p$. The figure suggests that the unintended receiver $\Pr(\epsilon)$ in the case of perfect channel estimates at the

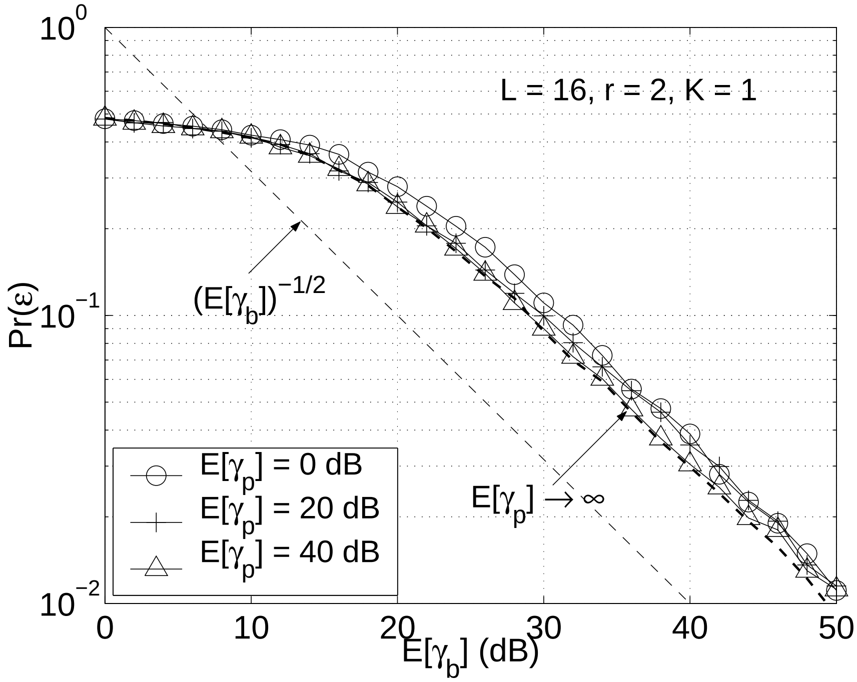


Figure 4.9: Simulated approximations to lower bounds (4.32) and (4.33) on the unintended receiver $\Pr(\epsilon)$ for various level of channel estimation quality $\overline{\gamma}_p$. The thicker dashed curve corresponds to the case of perfect channel estimation, and the solid curves with markers correspond to the case of imperfect channel estimation.

receiver, as its intended receiver counterpart in Section 4.3.1, can serve as a metric for determining the high SNR performance characteristics in the case of imperfect channel estimates. The figure shows that, as $\overline{\gamma}_b$ increases, the $\Pr(\epsilon)$ associated with finite $\overline{\gamma}_p$ exhibits the same decaying slope as the curve associated with perfect channel estimates, forming a parallel curve that is within a few dB of the latter. Thus the $\Pr(\epsilon)$ metrics in the perfect channel estimates case are suggestive of the performance characteristics when noisy channel estimates are available at the receiver. This is because the second term of $\Psi$ in (4.29) is independent of $\hat{\alpha}_k$ and eventually dominates the decision as $\overline{\gamma}_b$ increases, similar to the intended receiver case.

Figs. 4.8 and 4.9 also suggest that, at high $\overline{\gamma}_b$, the $\Pr(\epsilon)$ curves of unintended receivers with perfect channel estimates for nested map-based DS/SS systems decay at a constant rate. The figures reveal that this decaying rate is the same as its counterpart for AWGN channels, at $1/\sqrt{\overline{\gamma}_b}$ (the same as the slope of the dashed line). In general, this rate represents a lower bound on the $\Pr(\epsilon)$ curve decaying rate of the unintended receiver with channel estimates of arbitrary quality.

### 4.4.2 Fast Flat Fading

In this section we develop numerically efficient predictors of the unintended receiver $\Pr(\epsilon)$ in fast flat Rayleigh fading for the class of nested maps-based DS/SS. The developments herein follow closely those for slow flat fading in Section 4.4.1.

The maximum-likelihood unintended detector of $\mathbf{b}$, given the observation $\mathcal{Y}_{K,NL}$ in (4.6) and channel estimates

$$\hat{\mathcal{A}} \overset{\triangle}{=} \{\hat{\alpha}_k[n];\ k = 1, 2, \cdots, K \text{ and } n = 0, 1, \cdots, NL-1\}\ , \tag{4.39}$$

is, via the results in App. C.4, given by

$$\begin{aligned}
\hat{b}_{\mathrm{ML}}(\mathcal{Y}) &= \arg\max_{\mathbf{b}} \int p_{\mathcal{Y}|\mathbf{b},\mathbf{c}^{NL},\hat{\mathcal{A}}}(\mathcal{Y}|\mathbf{b}, \mathbf{c}^{NL}, \hat{\mathcal{A}}) p_{c[0]}(c)\, dc \\
&= \arg\max_{\mathbf{b}} \int \exp\Bigg\{-\frac{1}{N_o}\sum_{k=1}^{K}\sum_{n=0}^{NL-1}\Bigg(\frac{|y_k[n]|^2 - 2\sqrt{\frac{3}{L}}\,\mathrm{Re}\,\{\hat{\alpha}_k^*[n]y_k[n]\}F^n(c)b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]}{\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\,\left(F^n(c)\right)^2+1} \\
&\qquad + \frac{\frac{3\,\mathcal{E}_b}{L}\,|\hat{\alpha}_k[n]|^2\left(F^n(c)\right)^2}{\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\,\left(F^n(c)\right)^2+1}\Bigg)\Bigg\} p_{c[0]}(c)\, dc\,.
\end{aligned} \tag{4.40}$$

In the special case of perfect channel estimates, (4.40) reduces to

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathcal{Y}) \;&=\; \arg\max_{\mathbf{b}} \int \exp\left\{\frac{1}{N_o}\sum_{n=0}^{NL-1}\left(2\sqrt{\frac{3}{L}}F^n(c)b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\mathrm{Re}\{y[n]\}\right.\right.\\ &\qquad\left.\left. -\;\mu[n]\frac{3\,\mathcal{E}_b}{L}\left(F^n(c)\right)^2\right)\right\} p_{c[0]}(c)\,dc\,, \qquad (4.41)\end{aligned}$$

where $y[n]$ is the signal at the output of MRC in (4.22) and $\mu[n]$ is given by (4.24). Thus, as in Section 4.4.1, the sequence of $y[n]$ in the form of (4.31) is a sufficient statistic for $\mathbf{b}$ in the context of unintended detection given perfect channel estimates.

Computationally efficient $\Pr(\epsilon)$ metrics for the class of nested map-based DS/SS can be obtained via straightforward extensions of the corresponding metrics for slow fading case in Section 4.4.1. Assuming that the unintended receiver is given $b[0]$, $\{i[n];\, 1 \le n \le N-1,\, n\neq D\}$ where $b[n] = i[n]\,b[n-1]$, and the side information that $c[0] \in \{c[m];\, m = 0, 1, \ldots, M_o-1\}$ for sufficiently large $M_o$, the lower bound (4.32) extends to

$$\hat{i}_{\mathrm{LB}}(\mathcal{Y}) = \arg\max_{i\in\pm 1}\sum_{m=0}^{M_o-1}\exp\left\{-\frac{1}{N_o}\sum_{k=1}^{K}\sum_{n=0}^{NL-1}\frac{\left|y_k[n]-\sqrt{\frac{3}{L}}\hat{\alpha}_k[n]F^n(c[m])b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\right|^2}{\frac{3\,\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\;\left(F^n(c[m])\right)^2+1}\right\}\;,(4.42)$$

which, in the case of perfect channel estimates, reduces to

$$\begin{aligned}\hat{i}_{\mathrm{LB}}(\mathbf{y}) \;&=\; \arg\max_{\mathbf{b}}\sum_{m=0}^{M_o-1}\exp\left\{\frac{1}{N_o}\sum_{n=0}^{NL-1}\left(2\sqrt{\frac{3}{L}}F^n(c)b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\mathrm{Re}\{y[n]\}\right.\right.\\ &\qquad\left.\left. -\;\mu[n]\frac{3\,\mathcal{E}_b}{L}\left(F^n(c)\right)^2\right)\right\}\;. \qquad (4.43)\end{aligned}$$

As in Sections 3.2.4 and 4.4.1, computationally efficient approximations to $\Pr(\epsilon)$ can be obtained via (4.42) or (4.43) by employing a windowed observation $\mathcal{Y}_w$ from (4.34).

The upper bounds (4.36) and (4.37) extend to

$$\begin{aligned}\hat{i}_{\mathrm{UB}}(\mathcal{Y}_1) \;=\; \arg\min_i \min_j \sum_{k=1}^{K} \Bigg( & \frac{|y_k[DL-1]|^2}{\frac{3\,\overline{\gamma}_b}{L(\overline{\gamma}_p+1)}\hat{c}^2_{i,j}[0]+1} + \frac{|y_k[DL]|^2}{\frac{3\,\overline{\gamma}_b}{L(\overline{\gamma}_p+1)}\hat{c}^2_{i,j}[1]+1} \\ & - 2\sqrt{\frac{3}{L}}\Bigg(\frac{\hat{c}_{i,j}[0]\,\mathrm{Re}\,\{y_k[DL-1]\hat{\alpha}^*_k[DL-1]\}}{\frac{3\,\overline{\gamma}_b}{L(\overline{\gamma}_p+1)}\hat{c}^2_{i,j}[0]+1} \\ & + \frac{\hat{c}_{i,j}[1]\,\mathrm{Re}\,\{y_k[DL]\hat{\alpha}^*_k[DL]\}}{\frac{3\,\overline{\gamma}_b}{L(\overline{\gamma}_p+1)}\hat{c}^2_{i,j}[1]+1}\Bigg) \\ & + \frac{3\,\mathcal{E}_b}{L}\Bigg(\frac{|\hat{\alpha}_k[DL-1]|^2\,\hat{c}^2_{i,j}[0]}{\frac{3\,\overline{\gamma}_b}{L(\overline{\gamma}_p+1)}\hat{c}^2_{i,j}[0]+1} + \frac{|\hat{\alpha}_k[DL]|^2\,\hat{c}^2_{i,j}[1]}{\frac{3\,\overline{\gamma}_b}{L(\overline{\gamma}_p+1)}\hat{c}^2_{i,j}[1]+1}\Bigg)\Bigg) \quad (4.44)\end{aligned}$$

and

$$\begin{aligned}\hat{i}_{\mathrm{UB}}(\mathbf{y}_1) \;=\; \arg\min_i \min_j \Bigg( & \frac{3\,\mathcal{E}_b}{L}\left(\mu[DL-1]\hat{c}^2_{i,j}[0] + \mu[DL]\hat{c}^2_{i,j}[1]\right) \\ & -2\sqrt{\frac{3}{L}}\left(\hat{c}_{i,j}[0]y[DL-1] + \hat{c}_{i,j}[1]y[DL]\right)\Bigg)\,, \quad (4.45)\end{aligned}$$

respectively, where the windowed vector of MRC outputs $\mathbf{y}_w,\ 1 \le w \le (N-1)L$ is in the form of (4.38) with $y[n]$ in (4.22), and $\hat{c}_{i,j}[n],\ n = 0, 1$ from (4.35) form the set of constellation points for the binary-signaling-in-fast-fading problem.

Fig. 4.10 shows the unintended receiver $\Pr(\epsilon)$ curves vs. SNR for various levels of $\overline{\gamma}_p$. As the figure illustrates, the unintended receiver performance in fast flat fading suffers significantly from the presence of imperfect channel estimates at the receiver. In general, a 100-fold increase in the target level of $\overline{\gamma}_p$ is required to reduce ten-fold the associated error floor. This is in sharp contrast to the case of intended receiver, where a ten-fold increase in the target $\overline{\gamma}_p$ generally reduces the associated error floor by a factor of $10^{KL}$. This susceptibility of unintended receiver to the quality of noisy

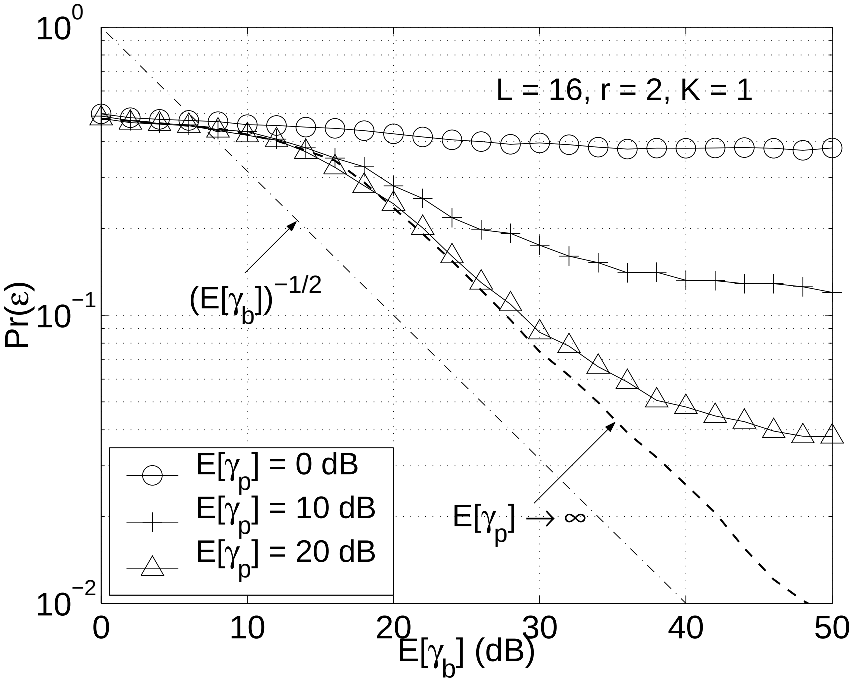


Figure 4.10: Simulated approximations to lower bounds (4.42) and (4.43) on the unintended receiver $\Pr(\epsilon)$ for various levels of channel estimation quality $\overline{\gamma}_p$. The dashed curve corresponds to the case of perfect channel estimation, and the solid curves with markers correspond to the case of imperfect channel estimation.

channel estimates at the receiver is a direct consequence of the $\Pr(\epsilon)$ decaying rates in the perfect channel estimates case; as Figs. 4.8, 4.9, and 4.10 show, the unintended receiver $\Pr(\epsilon)$ in fading asymptotically decays at the rate of $1/\sqrt{\overline{\gamma}_b}$, while the intended receiver $\Pr(\epsilon)$ in fast fading decays as $1/\overline{\gamma}_b^{KL}$. In the following section we verify that indeed the decaying rate is lower bounded by $1/\sqrt{\overline{\gamma}_b}$ for the class of nested maps.

### 4.4.3 Asymptotic Decaying Rate of $\Pr(\epsilon)$

In this section we modify the development in Section 3.2.3 and utilize the results developed in App. B.2 to prove that the unintended receiver $\Pr(\epsilon)$ for $r$-adic map based DS/SS in slow flat Rayleigh fading channels, with a $K$-element receiver antenna diversity and perfect channel estimates, is lower bounded by a function that decays as

$1/\sqrt{\overline{\gamma}_b}$ at high $\overline{\gamma}_b$.[1] Since for any nested map there exists a corresponding initializing $r$-adic map with lower unintended receiver $\Pr(\epsilon)$, the $1/\sqrt{\overline{\gamma}_b}$ bound also holds for all nested maps generated via the algorithms developed in Section 3.3, initialized with an $r$-adic map. In addition, this rate bounds the unintended receiver $\Pr(\epsilon)$ over Rayleigh fading channels, irrespective of the time selectivity of the channel, since $1/\sqrt{\overline{\gamma}_b}$ bounds the asymptotic $\Pr(\epsilon)$ slope of both the slow (time-nonselective) fading and AWGN channels.

We develop a lower bound on the $\Pr(\epsilon)$ of detecting an arbitrary, but fixed, differentially encoded symbol given observation of $y[n]$ in (4.10). In particular, we assume that an IID sequence $i[n] = \pm 1$ is differentially encoded into the sequence $b[n] = i[n]\, b[n-1]$ used in (4.1), and focus on detection of $i[D]$, for some $1 \leq D \leq N-1$, based on the sufficient statistic $\mathbf{y}$ in (4.31).

To obtain a lower bound on the $\Pr(\epsilon)$, we consider a detector that is provided with the remaining information symbols $\{i[n];\, 1 \leq n \leq N-1,\, i \neq D\}$ as well as some additional side information that depends on whether or not $c[0]$ belongs in the set $I_o \overset{\triangle}{=} \bigcup_{c \in \mathcal{C}^{(D)}} I(c)$, where $I(c) \overset{\triangle}{=} (c, c{+}\Delta)$, $\Delta \overset{\triangle}{=} 2\, r^{-(NL-1)}$, and $\mathcal{C}^{(D)}$ is the preimage of $\{0\}$ under $F^{DL-1}$. Specifically, when $c[0] \notin I_o$, $i[D]$ is declared to the receiver; when $c[0] \in I_o$, the receiver is only told that $c[0]$ is from the set $\{\pm \underline{c}[0] + \delta\}$, where $\underline{c}[0]$ denotes the unique $c \in \mathcal{C}^{(D)}$ for which $c[0] \in (c, c+\Delta)$, and $\delta \overset{\triangle}{=} \delta(c[0]) = c[0] - \underline{c}[0]$. As App. B.2 shows, the optimal receiver with this side information and knowledge of channel gains

$$\mathbf{a} \overset{\triangle}{=} \begin{bmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_K \end{bmatrix}^{\mathrm{T}}$$

is inferior to the optimal detector in the context of binary signaling with codewords

[1] As a direct consequence, the rate of $1/\sqrt{\overline{\gamma}_b}$ lower bounds the asymptotic $\Pr(\epsilon)$ decaying rate of the unintended receiver with imperfect channel estimation.

$\mathbf{x}_{i[D]}$ and $\mathbf{x}_{-i[D]}$, where $\mathbf{x}_{i[D]}$ is the transmitted vector, defined as in (3.15) with $x[n] = \frac{A}{\sqrt{L}}\mu c[n]\, b[\lfloor n/L \rfloor]$ and $\mu$ as in (4.12) with $\hat{\alpha}_k = \alpha_k$, and where $\mathbf{x}_{-i[D]}$ is the vector closest in Euclidean distance to $\mathbf{x}_{i[D]}$ among those associated with the antipodal hypothesis, and corresponds to using $c[n]$ generated from $c[0] = -\underline{c}[0] + \delta$. Thus,

$$\Pr(\epsilon | c = \underline{c}[0] + \delta, \mathbf{a}) \geq \mathcal{Q}\left(\sqrt{\tilde{\gamma}(\delta, \mathbf{a})}\right) \tag{4.46}$$

where

$$\tilde{\gamma}(\delta, \mathbf{a}) = \frac{\left\|\mathbf{x}_1 - \mathbf{x}_{-1}\right\|^2}{2N_o} = \delta^2 \frac{6\,\mu\,\mathcal{E}_b(r^{2DL} - 1)}{(r^2 - 1)\,N_o} = C\,\overline{\gamma}_b \delta^2\,, \tag{4.47}$$

with $C = \frac{6\,\mu\,(r^{2DL}-1)}{r^2-1}$. Conditioned on $\mu$ and $c[0] \in I(\underline{c}[0])$, $\delta$ is uniformly distributed in $(0, \Delta)$ and, hence, the PDF of $\tilde{\gamma}$ in (4.47) is

$$p_{\tilde{\gamma}}(\gamma) = \frac{1}{\Delta}\sqrt{\frac{\pi}{\gamma\, C\, \overline{\gamma}_b}}\,\mathcal{Q}\left(\sqrt{\frac{2\gamma}{\Delta^2 C \overline{\gamma}_b}}\right)\,.$$

We next pick an arbitrary but fixed $\gamma_o$ (independent of $\overline{\gamma}_b$). Using (4.46), we have

$$\begin{aligned}
\Pr(\epsilon) &\geq \Pr\left(c[0] \in I_o\right) \int_0^\infty \mathcal{Q}\left(\sqrt{\gamma}\right)\, p_{\tilde{\gamma}}\left(\gamma\right) d\gamma \\
&\geq r^{(D-N)L} \mathcal{Q}\left(\sqrt{\gamma_o}\right) \int_0^{\gamma_o} p_{\tilde{\gamma}}\left(\gamma\right) d\gamma \\
&= r^{(D-N)L} \mathcal{Q}\left(\sqrt{\gamma_o}\right) \left\{ 2\sqrt{\frac{\pi\gamma_o}{\Delta^2 C \overline{\gamma}_b}}\,\mathcal{Q}\left(\sqrt{\frac{2\,\gamma_o}{\Delta^2 C \overline{\gamma}_b}}\right) \right. \\
&\qquad\qquad \left. +1 - \exp\left\{-\frac{\gamma_o}{\Delta^2 \overline{\gamma}_b C}\right\}\right\}\,. 
\end{aligned} \tag{4.48}$$

As $\overline{\gamma}_b$ increases, (4.48) converges to the following desired bound:

$$\Pr(\epsilon) \geq \mathcal{Q}\left(\sqrt{\gamma_o}\right)\, \frac{1}{\sqrt{\overline{\gamma}_b}} \frac{r^{NL-1}}{2} \sqrt{\frac{\pi\gamma_o(r^2 - 1)}{6\,\mu\,(r^{2DL} - 1)}}\,. \tag{4.49}$$

## 4.5 Implications of Fading on Privacy

In this section we show that the communication privacy provided by the class of chaotic DS/SS systems based on a nested map, first demonstrated for the case of AWGN channels in Chapter 3, is not compromised by the presence of channel gain in fading channels. In particular, for the systems of interest, and provided perfect channel estimates are available, unintended receivers cannot achieve full diversity benefits, in contrast to intended receivers. As shown in the Sections 4.3 and 4.4, the presence of noisy channel estimates does not help unintended receivers, since its impact on privacy is insignificant in slow fading and largely mitigated for a wide range of system parameters in fast fading. In particular, in fast flat fading, the error floor on the $\Pr(\epsilon)$ of unintended receiver with noisy channel estimates is consistently and substantially higher than the associated error floor on the $\Pr(\epsilon)$ of intended receiver. We first focus on the case of perfect channel estimation to illustrate some of the important privacy characteristics in fading. We then demonstrate that the presence of imperfect channel estimates at the receiver does not degrade the available privacy benefits.

For the nested maps, the time- and frequency-selectivity of channel and the available degree of diversity do not affect the asymptotic decaying rate of the unintended receiver $\Pr(\epsilon)$, *i.e.*, irrespective of the type of fading, unintended receivers cannot achieve full diversity. Specifically, the $\Pr(\epsilon)$ decaying rate of the unintended receiver with an arbitrary number of independently faded observations in a general time- and frequency-selective channel is $1/\sqrt{\overline{\gamma}_b}$. This is because, regardless of the available degrees of diversity, the decaying rate is upper and lower bounded by $1/\sqrt{\overline{\gamma}_b}$, *i.e.*, by the $\Pr(\epsilon)$ decaying rates over the worst case channel of slow flat fading and the best case channel of AWGN. This is illustrated via simulations for the dyadic map-based

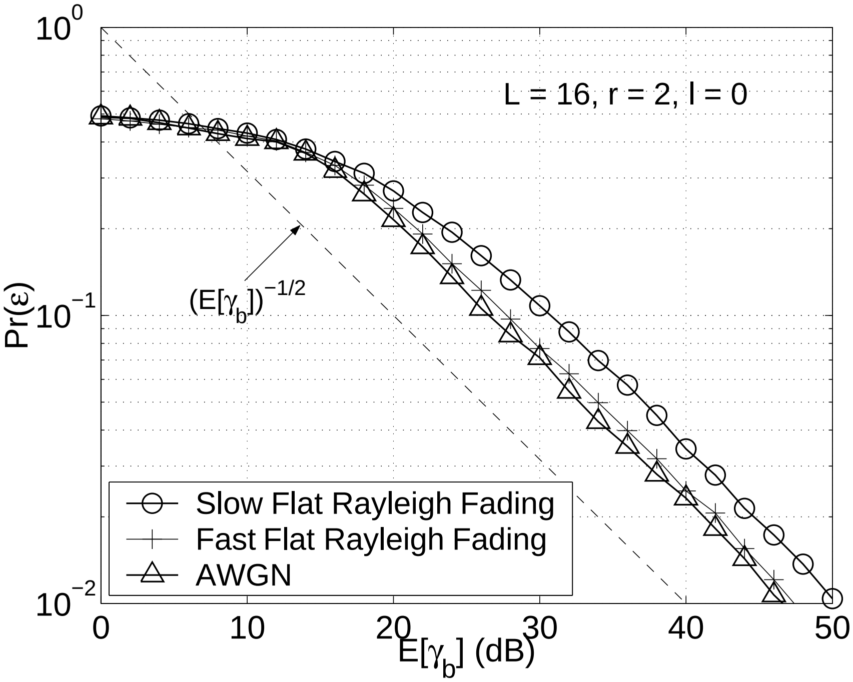


Figure 4.11: Approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ in Rayleigh fading and AWGN.

DS/SS in Fig. 4.11. This lack of dependence of the decaying rate on the degrees of diversity in the channel is due to chaotic spreading. Indeed, from the perspective of unintended users, chaotic spreading can be viewed as an additional fading process with uniform PDF, dominating the channel fading process and, hence, the decaying rate.

Little benefit in the unintended receiver $\Pr(\epsilon)$ can be attained with temporal or spectral diversity, since not only the associated decaying rate of the $\Pr(\epsilon)$ does not change but also the highest achievable SNR gain via these diversity techniques given a target $\Pr(\epsilon)$ is minuscule. This is again illustrated in Fig. 4.11, where the gap between the $\Pr(\epsilon)$ in slow flat fading and the $\Pr(\epsilon)$ in AWGN is less than 4 dB. As a result, in the presence of $K$ degrees of spectral or temporal diversity, the unintended receiver $\Pr(\epsilon)$ gap in $\overline{\gamma}_b$ between $K = 1$ and $K = \infty$ is at most 4 dB. Such a small

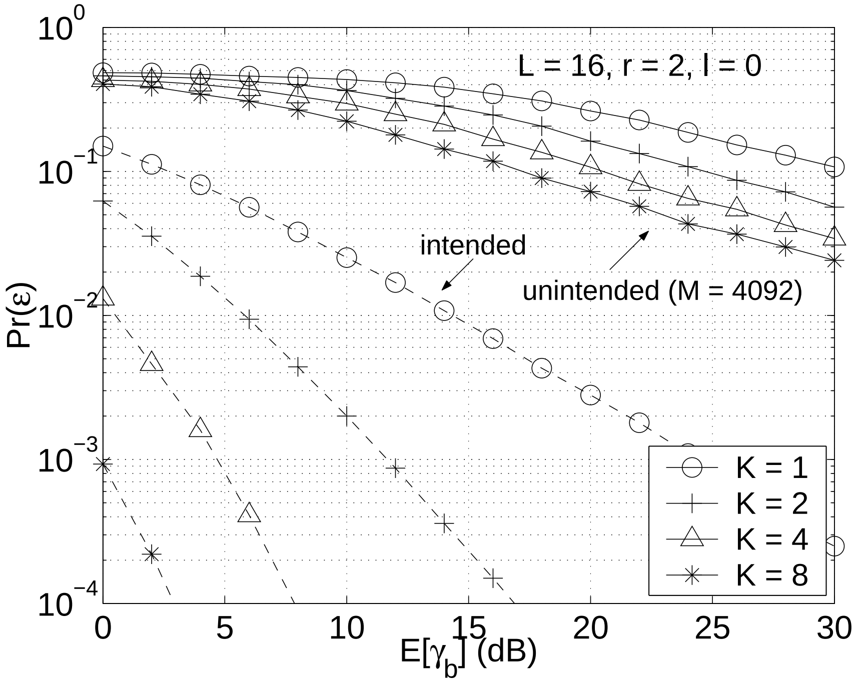


Figure 4.12: Intended receiver $\Pr(\epsilon)$ (dashed) and approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ (solid) for $K$ degrees of spatial diversity in slow flat Rayleigh fading.

gap, empirically verified for the class of nested maps, is due to the dominant effect of the induced fading process $c[n]$ on the $\Pr(\epsilon)$.

Spatial diversity via $K$-element receiver antenna arrays, yielding $K$-fold average output SNR gains, also bestows only marginal benefits on the associated unintended receiver $\Pr(\epsilon)$. In fact, as Figs. 4.12 and 4.13 demonstrate, the $\Pr(\epsilon)$ performance improvements due to increasing the number of antenna elements are far more substantial for intended users. This is a direct consequence of the difference between the asymptotic decaying rates of the intended and unintended receiver $\Pr(\epsilon)$. Even for scenarios where the unintended receiver can exploit a larger number of antennas, the additional number of antennas required for the unintended receiver to outperform intended receivers at a target $\Pr(\epsilon)$ is impractical. For instance, in slow flat fading, $K \approx 256$ antennas are needed by the unintended user to outperform a single-antenna

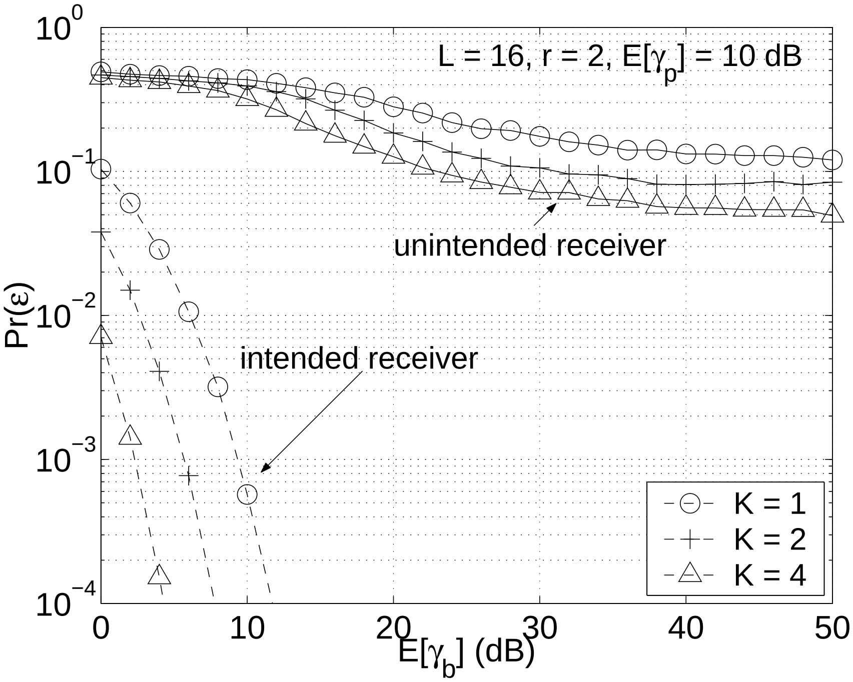


Figure 4.13: Intended receiver $\Pr(\epsilon)$ (dashed) and approximate lower bounds on the unintended receiver $\Pr(\epsilon)$ (solid) for $K$ degrees of spatial diversity and imperfect channel estimation in fast flat Rayleigh fading.

intended receiver at a target $\Pr(\epsilon)$ of 0.1 for a dyadic map DS/SS with $L = 16$. Furthermore, the number of antennas $K$ grow exponentially fast with lower target $\Pr(\epsilon)$ or higher $r$, $\ell$, and $L$.

Imperfect channel estimation does not compromise the communication privacy provided by chaotic DS/SS, as Fig. 4.13 reveals. The figure shows that the error floor effect on the unintended receiver $\Pr(\epsilon)$ is much more pronounced than the effect on the intended receiver $\Pr(\epsilon)$. Indeed, for a given $\overline{\gamma}_p$ and $L$, increasing $K$ by $K_o$ reduces the error floor of unintended receiver $\Pr(\epsilon)$ by $\sqrt{K_o}$ in general, while for intended receiver it reduces the error floor by $\overline{\gamma}_p^{K_o}$. This is again due to the difference in asymptotic decaying rates between the intended and unintended receivers.

# Chapter 5

# Analysis and Design of Pseudochaotic DS/CDMA Systems: Multiuser Case

In this chapter, we investigate the potential of a class of pseudochaotic DS/CDMA systems for providing private and reliable multiuser communications. In a wide array of communication scenarios where multiple transmitters share a common channel, there is a dual requirement on the modulation process for discouraging unintended reception as well as achieving desired intended reception performance in the presence of signals from other transmitters. CDMA extensions of the class of pseudochaotic DS/SS systems studied in the previous chapters, whereby the spreading sequence for each user is generated via the same chaotic map but initialized with distinct initial condition, have the potential of satisfying these requirements. As we have shown in Chapters 3 and 4, the class of nested map-based DS/SS systems can furnish attractive privacy benefits to intended receivers in a broad range of channel types. In addition, chaotic sequences produced with the same map but distinct initial conditions, in general, have wideband spectra and cross-spectra. Furthermore, chaotic sequences can be designed to exhibit desired spectral properties [29].

To demonstrate the privacy potential of chaotic DS/CDMA systems, we focus on synchronous multiuser transmission of DS/CDMA signals based on nested maps in Section 3.3 over AWGN channels. This scenario is captured by the system model in Section 2.1. The intended and unintended users' received signal is of the form

$$y[n] = \frac{A}{\sqrt{L}} \sum_{m=1}^{M} c_m[n] b_m \left[ \left\lfloor \frac{n}{L} \right\rfloor \right] + w[n] \,, \tag{5.1}$$

where $M$ is the number of active transmitters and $c_m[n]$ is generated by iterating the initial condition $c_m[0]$ through a nested map. We assume that the same nested map is used for all transmitters but the initial conditions used to generate the individual sequences are distinct, *i.e.*, $c_i[0] \neq c_j[0]\,,\ i \neq j$. We also assume that only the intended receivers for $m$-th sequence are provided with the key $c_m[0]$. Hence, a legitimate user within the network knows the initial conditions of only the transmissions intended for the user. This constraint is a necessity in many applications, where, for instance, a subscriber to a particular channel may opt to listen to unsubscribed channels, or a network node may be compromised by a hostile entity with the intention to eavesdrop on other transactions in the network. In this context, we develop and evaluate the optimal intended and unintended multiuser receivers. While our scope of synchronous transmission is somewhat narrow, this special case is suggestive of some of the privacy characteristics these chaotic DS/CDMA systems provide in general asynchronous multiuser transmission scenarios. In addition, our findings for AWGN case can serve as a basis for designing chaotic DS/CDMA with attractive privacy benefits in fading channels, as we have shown in Chapter 4.

Correlation and power spectral properties of spreading sequences are important in CDMA systems, where the level of multiuser interference (MUI) have a direct impact on system capacity. Low auto- and cross-correlation of spreading sequences and, hence, flat and wideband spectra and cross-spectra are desirable characteristics in DS/CDMA since such sequences reduce the MUI and lessens the probability of signal interception by unintended receivers. In this chapter we study the correlation and spectral properties of sequences from the nested maps as well as their digital implementations, to ascertain the suitability of these sequences as multiuser CDMA spreading codes.

In Section 5.1 we examine the correlation and power spectra of the pseudochaotic sequences from the nested maps developed in Section 2.3 and the underlying true chaotic trajectories the digital sequences are based on. In Section 5.2 we develop a general multiuser detector structure and associated $\Pr(\epsilon)$ metric that capture the intended and unintended receiver with knowledge on the initial conditions of various combinations of transmitters in the multiuser network. Finally, in Section 5.3 we explore the privacy characteristics of chaotic DS/CDMA system with an example case of two-user synchronous system in AWGN.

## 5.1 Correlation and Spectral Characteristics

In this section we study second-order correlation statistics and power spectra of the chaotic sequences from nested maps and the digitized pseudochaotic implementation of these sequences. We focus on the autocorrelation, since this suffices in deducing MUI characteristics in the context of synchronous transmission with each user's spreading sequence obtained from different shifts of a single sequence.

The statistics of the pseudochaotic sequences implemented through the methods in Section 2.3 with sufficiently large bit precision depth can, for all practical purposes, accurately approximate those of the underlying chaotic sequences. Specifically, for the class of nested map-based sequences, the autocorrelation

$$R_c[k] = E\left[c[n]c[n+k]\right] \tag{5.2}$$

of the pseudochaotic sequences generated as in Section 2.3 with sufficiently large bit precision depth closely approximates that of the underlying true chaotic sequences. The autocorrelation of chaotic sequences from nested maps can be determined in closed form via the methods in [19]. In turn, for the pseudochaotic sequences with very large periods, the estimate of the autocorrelation in the form

$$\hat{R}_c[k] = \frac{1}{L_o} \sum_{n=0}^{L_o-1} c[n]c[n+k]\ ,\ k < L_o\,, \tag{5.3}$$

where the observation length $L_o$ is less than or equal to the sequence period, can serve as an accurate substitute for (5.2) ($\hat{R}_c[k] = R_c[k]$ if $L_o$ is the sequence period). Fig. 5.1 shows, for some nested maps $F_{r,\ell}$, the closed form solution of (5.2) for true chaotic sequences and empirically obtained (5.3) of their numerical realizations. As the figure suggests, the autocorrelation of the numerically generated pseudochaotic sequences indeed accurately approximates the underlying nested map-based chaotic trajectories. This is because, for the maps of interest in this dissertation, the *shadowing* property holds, *i.e.*, although a numerical trajectory diverges from the true trajectory with the same initial condition, there exists a true trajectory with a slightly different initial condition that stays near (shadows) the numerical trajectory [2,30]. Thus, within the period, the maximal-length pseudochaotic sequences based on the nested maps form a subset of the set of true trajectories and exhibit the same statistical characteristics.

Fig. 5.2 shows the analytically obtained autocorrelations of sequences from the nested maps along with the autocorrelation of the sequences from the tent map in

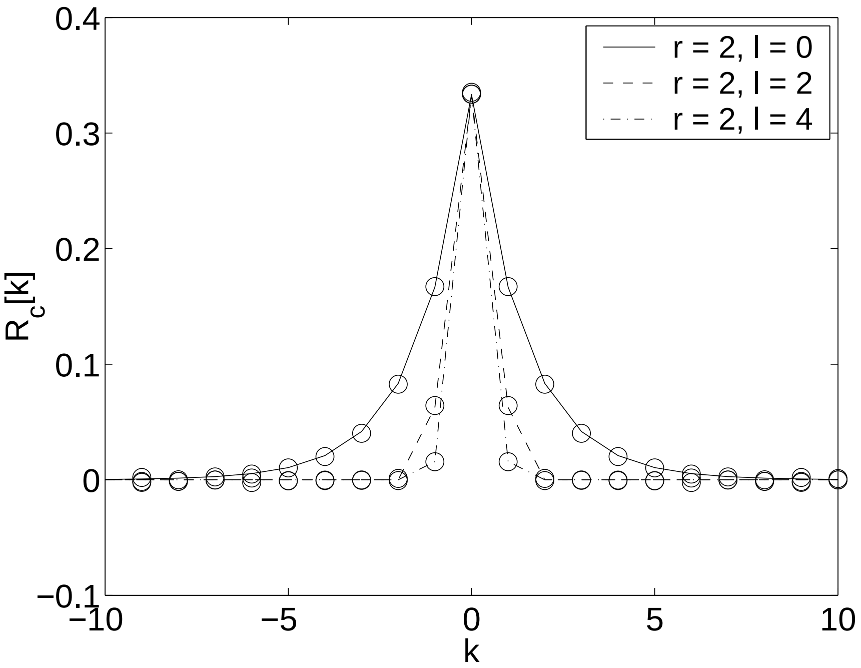


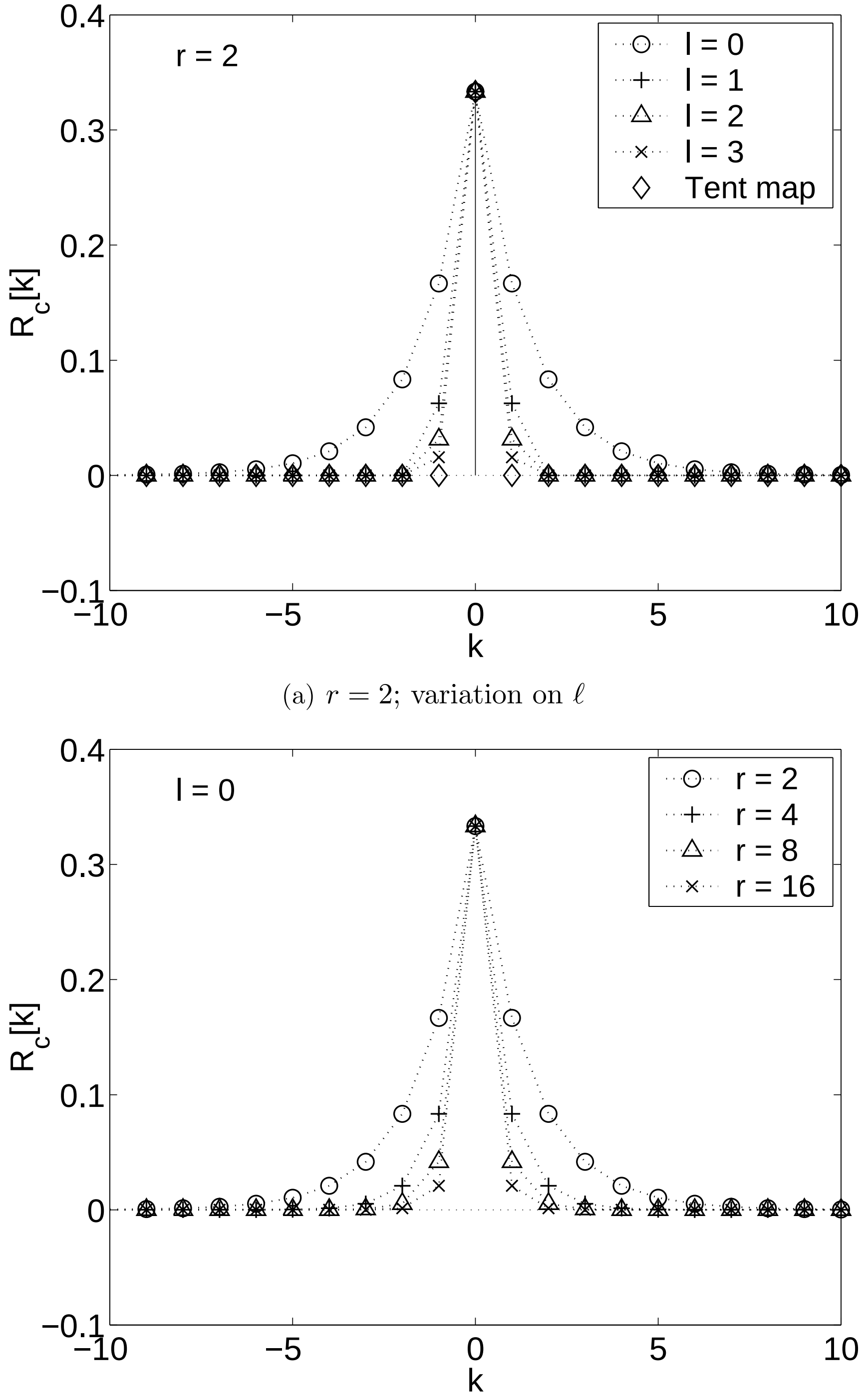
Figure 5.1: Comparison of analytically computed autocorrelation of sequences from nested maps and empirical autocorrelation estimates of their pseudochaotic implementation. The lines represent analytically obtained autocorrelations of true chaotic trajectories, and the circles represent empirical estimates of numerical trajectories. Empirical estimates are obtained via (5.3) with $L_o = 100000$ on 48-bit precision realization.

(2.14), represented by the diamonds in Fig. 5.2(a). The figure illustrates that, as $r$ or $\ell$ increases, the autocorrelation $R_{c,\{r,\ell\}}[k]$ of the sequences from the nested maps $F_{r,\ell}$ converges to that of the Tent map, $R_{c,\mathrm{T}}[k] = \frac{1}{3}\,\delta[k]$, in the mean square sense, *i.e.*,

$$\lim_{\ell\to\infty}\left\|R_{c,\{r,\ell\}}[k] - \frac{1}{3}\,\delta[k]\right\| = 0 \quad \text{and} \quad \lim_{r\to\infty}\left\|R_{c,\{r,\ell\}}[k] - \frac{1}{3}\,\delta[k]\right\| = 0\,, \tag{5.4}$$

where $\|\cdot\|$ denotes $\mathcal{L}_2$-norm and

$$\delta[k] = \begin{cases} 1, & k = 0 \\ 0, & |k| \geq 1 \end{cases}$$



(a) $r = 2$; variation on $\ell$

(b) $\ell = 0$; variation on $r$

Figure 5.2: Analytically computed autocorrelation of the sequences from nested maps and the tent map.

is the unit impulse. Since such convergence to an impulsive autocorrelation implies reduction of MUI in synchronous channels, (5.4) suggests that increasing $r$ or $\ell$ has a two-fold effect: first, it reduces MUI and, hence, improves the intended receiver performance in multiuser settings. Second, it degrades the unintended receiver performance, as we have shown in the previous chapters. Such enhancement of $R_c[k]$ is due to the reduction in the expected duration of a trajectory following a linear segment of the map that comes from increasing $r$ or $\ell$. We note that the sequences from any even-symmetric $P$-partition maps, including the tent map, possess flat spectra and, hence, $R_c[k] = \frac{1}{3}\,\delta[k]$. Since a white spreading sequence, with flat spectra, does not induce MUI in synchronous channels, synchronous DS/CDMA systems based on even-symmetric $P$-partition maps, unlike their nested map counterparts, do not suffer from MUI and, hence, result in the optimal intended receiver performance. However, as shown in Section 3.2.2, they are unattractive candidates for providing privacy in multiuser networks, since the associated unintended receiver $\Pr(\epsilon)$ is far inferior to that associated with odd symmetric maps, as discussed in Section 3.2.2. In general, employing the odd-symmetric nested maps of Section 3.3 instead of even-symmetric $P$-partition maps in synchronous multiuser networks leads to a moderate increase in the intended receiver $\Pr(\epsilon)$ while providing substantial gains in privacy. Furthermore, increasing the nested map parameters $r$ or $\ell$ results in smaller degradation of the intended receiver $\Pr(\epsilon)$ and larger gains in privacy, as higher $r$ and $\ell$ reduce the MUI while increasing the unintended receiver $\Pr(\epsilon)$.

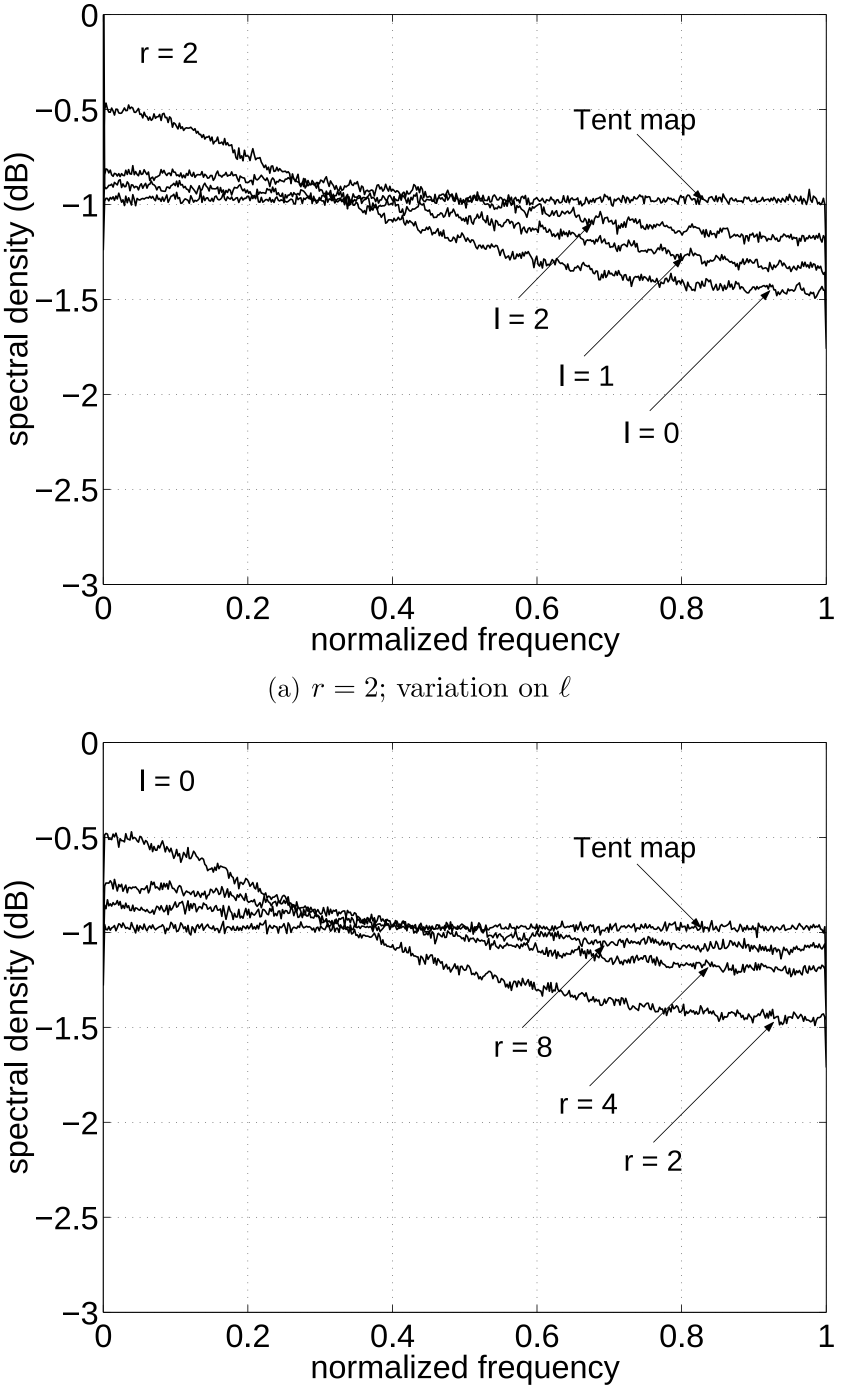
The power spectral densities of sequences generated by the nested maps of Section 3.3, while not flat, have significant components over the entire spectrum and converge in the mean square sense to a flat spectrum as $r$ or $\ell$ increases. This is consistent with our preceding observation that the autocorrelation of these nested map-based sequences approaches $\frac{1}{3}\,\delta[k]$. This is illustrated in Fig. 5.3, which shows the empirical power spectra for the nested maps and the tent map, obtained via periodogram averaging on sample pseudochaotic sequence realizations. Although sequences from the even-symmetric $P$-partition maps possess flat spectra that are best suited for achieving the highest DS/CDMA system capacity and provide the optimum low probability-of-intercept (LPI) capability in the context of synchronous systems, the nested map-based sequences have broadband spectra that rapidly converge to a flat spectrum as $r$ or $\ell$ increases.

## 5.2 ML Reception of Chaotic DS/CDMA Signals

In the following we develop metrics for evaluating the $\Pr(\epsilon)$ performance of intended and unintended receivers for nested map-based synchronous DS/CDMA communication over AWGN channels. In particular, in the context of $M$ active transmitters employing the same map but distinct initial conditions, we construct a general ML multiuser detector structure that captures various intended and unintended receiver settings. Consistent with the single user setting, we assume that the unintended receiver knows the modulation scheme including the chaotic map but does not know the initial condition of the targeted transmitter.

The ML multiuser detector with the knowledge of the number of active transmitters in the network and the distribution (or candidate sets) of their initial conditions, reflecting available side information on them, is a generalization of the conventional multiuser detector for synchronous channels in [1, 31, 32]. We assume that sequences of bits $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_M$ are transmitted, where

$$\mathbf{b}_m \triangleq \begin{bmatrix} b_m[0] & b_m[1] & \cdots & b_m[N-1] \end{bmatrix}^{\mathrm{T}}, \tag{5.5}$$



(a) $r = 2$; variation on $\ell$

(b) $\ell = 0$; variation on $r$

Figure 5.3: Empirical power spectra of sequences from the nested maps and the tent map. The spectra are obtained by applying periodogram averaging with a window length of 1024 to a numerical trajectory of length 1024000.

and $\mathbf{y}$ in the form of (3.10) with $y[n]$ as in (5.1) is observed. Then the maximum likelihood detector of the bit sequence of the $i$-th transmitter is given by

$$\begin{aligned}
\hat{\mathbf{b}}_{i,\mathrm{ML}}(\mathbf{y}) &= \arg\max_{\mathbf{b}_i} \int\!\!\int \cdots \int \sum_{\underline{\mathbf{b}} \in \mathcal{B}(\mathbf{b}_i)} p_{\mathbf{y}|\underline{\mathbf{b}},\mathcal{C}}(\mathbf{y}|\underline{\mathbf{b}},\mathcal{C}) p_{c_1[0]}(c_1) p_{c_2[0]|c_1[0]}(c_2|c_1) \\
&\qquad \cdots p_{c_M[0]|c_{M-1}[0],\ldots,c_1[0]}(c_M|c_{M-1},\ldots,c_1)\, dc_1 dc_2 \cdots dc_M \\
&= \arg\max_{\mathbf{b}_i} \int\!\!\int \cdots \int \sum_{\underline{\mathbf{b}} \in \mathcal{B}(\mathbf{b}_i)} \exp\left\{ -\frac{1}{N_o} \sum_{n=0}^{NL-1} \left( y[n] - \sqrt{\frac{3}{L}} \sum_{m=1}^{M} F^n(c_m) b_m \left[ \left\lfloor \frac{n}{L} \right\rfloor \right] \right)^2 \right\} \\
&\qquad \cdot p_{c_1[0]}(c_1) p_{c_2[0]|c_1[0]}(c_2|c_1) \\
&\qquad \cdots p_{c_M[0]|c_{M-1}[0],\ldots,c_1[0]}(c_M|c_{M-1},\ldots,c_1)\, dc_1 dc_2 \cdots dc_M, \qquad (5.6)
\end{aligned}$$

where

$$\underline{\mathbf{b}} \triangleq \begin{bmatrix} \mathbf{b}_1^{\mathrm{T}} & \mathbf{b}_2^{\mathrm{T}} & \cdots & \mathbf{b}_M^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}},$$

$$\mathcal{B}(\mathbf{b}_i) \triangleq \left\{ \underline{\mathbf{b}} = \begin{bmatrix} \theta_1^{\mathrm{T}} & \theta_2^{\mathrm{T}} & \cdots & \theta_M^{\mathrm{T}} \end{bmatrix}^{\mathrm{T}} ;\ \theta_i = \mathbf{b}_i \right\},$$

and

$$\mathcal{C} \triangleq \{ c_m[0];\ m = 1, 2, \ldots, M \} .$$

The sum over $\underline{\mathbf{b}} \in \mathcal{B}(\mathbf{b}_i)$ in (5.6) represents the expectation of the likelihood function taken over the $2^{N(M-1)}$ possible combinations of $\underline{\mathbf{b}}$ given $\mathbf{b}_i$.

For proper choice of $p_{c_j[0]}(c_j)$, $1 \le j \le M$, the detector (5.6) captures various intended and unintended receiver scenarios. In particular, the intended receiver that knows the initial conditions of all the active transmitters is captured by setting

$$p_{c_j[0]}(c) = \delta(c - c_j[0])\ , \forall j\,,$$

where $\delta(c)$ is the Dirac delta function. The intended receiver for the $i$-th transmitter sequence only is captured with $p_{c_i[0]}(c) = \delta(c - c_i[0])$ and $p_{c_j[0]}(c_j) = 1/2$, $j \neq i$. Various unintended receivers that may arise can also be captured with (5.6) by suitably setting $p_{c_j[0]}(c)$ for all $j$. For instance, the collusion scenarios, where multiple receivers in a network share their knowledge of initial conditions to better demodulate an unintended transmission with unknown initial condition, are supported by setting $p_{c_j[0]}(c) = \delta(c - c_j[0])$ if the initial condition for $j$-th transmitter is known and $p_{c_j[0]}(c_j) = 1/2$ if it is unknown. Furthermore, (5.6) can be readily extended to accommodate multiple targeted transmitters.

The $\Pr(\epsilon)$ performance trends of (5.6) can be characterized with numerically computable generalizations of the bounds developed in Section 3.2.4. In particular, assuming that the initial condition of the $m$-th transmitter is from the set $\{c_m[h_m]; h_m = 0, 1, \ldots, H_m - 1\}$, the ML detector of $\mathbf{b}_i$, given the side information $c_m[0] \in \{c_m[h_m]; h_m = 0, 1, \ldots, H_m - 1\}$, is an extension of the lower bound (3.19) given by

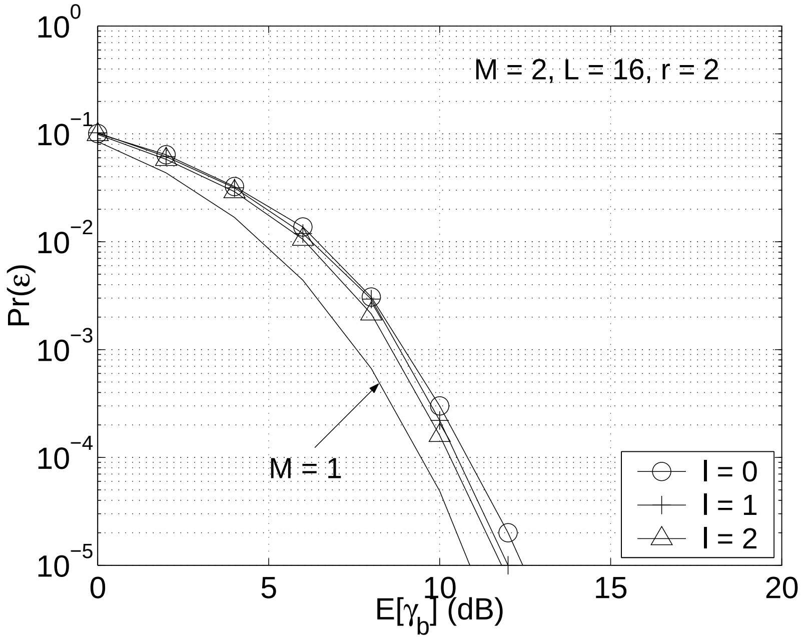
$$\hat{\mathbf{b}}_{i,\mathrm{LB}}(\mathbf{y}) = \arg\max_{\mathbf{b}_i} \sum_{h_1=0}^{H_1-1} \cdots \sum_{h_M=0}^{H_M-1} \sum_{\underline{\mathbf{b}} \in \mathcal{B}(\mathbf{b}_i)} \exp\left\{ -\frac{1}{N_o} \sum_{n=0}^{NL-1} \left( y[n] - \sqrt{\frac{3}{L}} \sum_{m=1}^{M} F^n(c_m[h_m]) b_m\left[\left\lfloor \frac{n}{L} \right\rfloor\right] \right)^2 \right\}, \quad (5.7)$$

where $H_j = 1$ if $c_j[0]$ is known to the receiver. Our analysis in the previous chapters suggests that this metric, with sufficiently large $H_m$ for $m \neq j$ where $c_j[0]$ is known, can provide accurate approximations to the intended and unintended receiver $\Pr(\epsilon)$ and its trends.

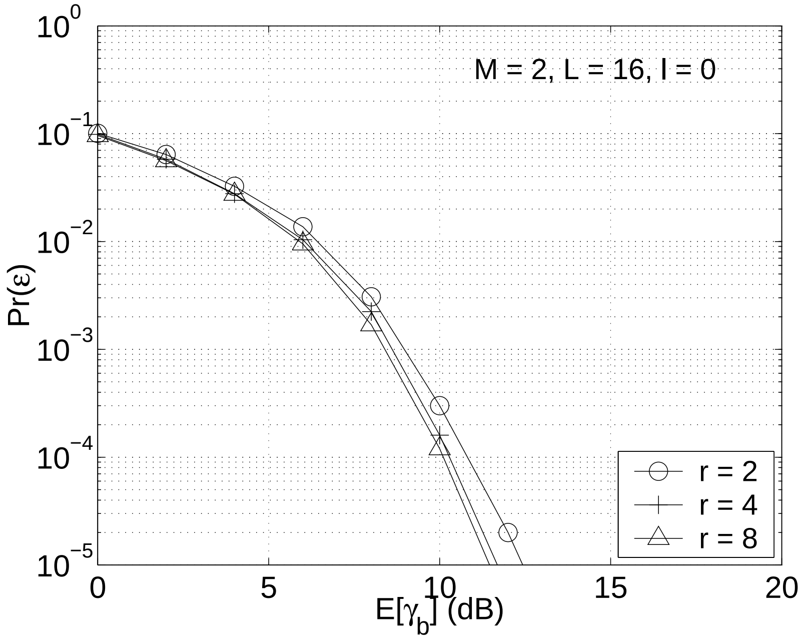
## 5.3 Privacy Characteristics of Multiuser Systems

In the following we consider a couple of simple representative examples that can serve as brief illustrations of the privacy characteristics of DS/CDMA systems based on the nested maps and, in particular, their trends with respect to the nested map parameters. First, we consider a two-transmitter system, where the signal from the 1st transmitter is for demodulation by both the intended and unintended receivers. We assume that the intended receiver knows $c_1[0]$ but does not know $c_2[0]$, while the unintended receiver is a legitimate receiver for the 2nd transmitter and, hence, knows $c_2[0]$ but not $c_1[0]$. We remark that the performance of this unintended receiver within the network furnishes a lower bound on that of the unintended receiver without the knowledge of initial conditions of any of the transmitters in the targeted network. Next, we consider a characterization of privacy in general $M \geq 2$ systems by developing suboptimal intended receivers in the $M$-user system of interest and comparing them with the optimal unintended receiver in single-user system. We show that, while conservative, such characterization can still illustrate the privacy potential of the pseudochaotic DS/CDMA for multiuser communications.

Fig. 5.4 depicts the intended receiver $\Pr(\epsilon)$ as a function of SNR for various nested maps in the two-transmitter system. As the figure suggests, the $\Pr(\epsilon)$ in a two-transmitter network is worse than the $\Pr(\epsilon)$ in a single-user system. This is consistent with the preceding analysis in Section 5.1 that the sequences from nested maps do not have flat spectra and, hence, result in a non-zero level of MUI. The figure, however, also reveals that, for $M = 2$, increasing the nested map parameters $r$ or $\ell$ improves the intended receiver performance. This again is as expected from our findings in Section 5.1 that increasing $r$ or $\ell$ of the nested maps improves the autocorrelation and, hence, reduces the MUI of the sequences. Such enhancement of



(a) $r = 2$; variation on $\ell$



(b) $\ell = 0$; variation on $r$

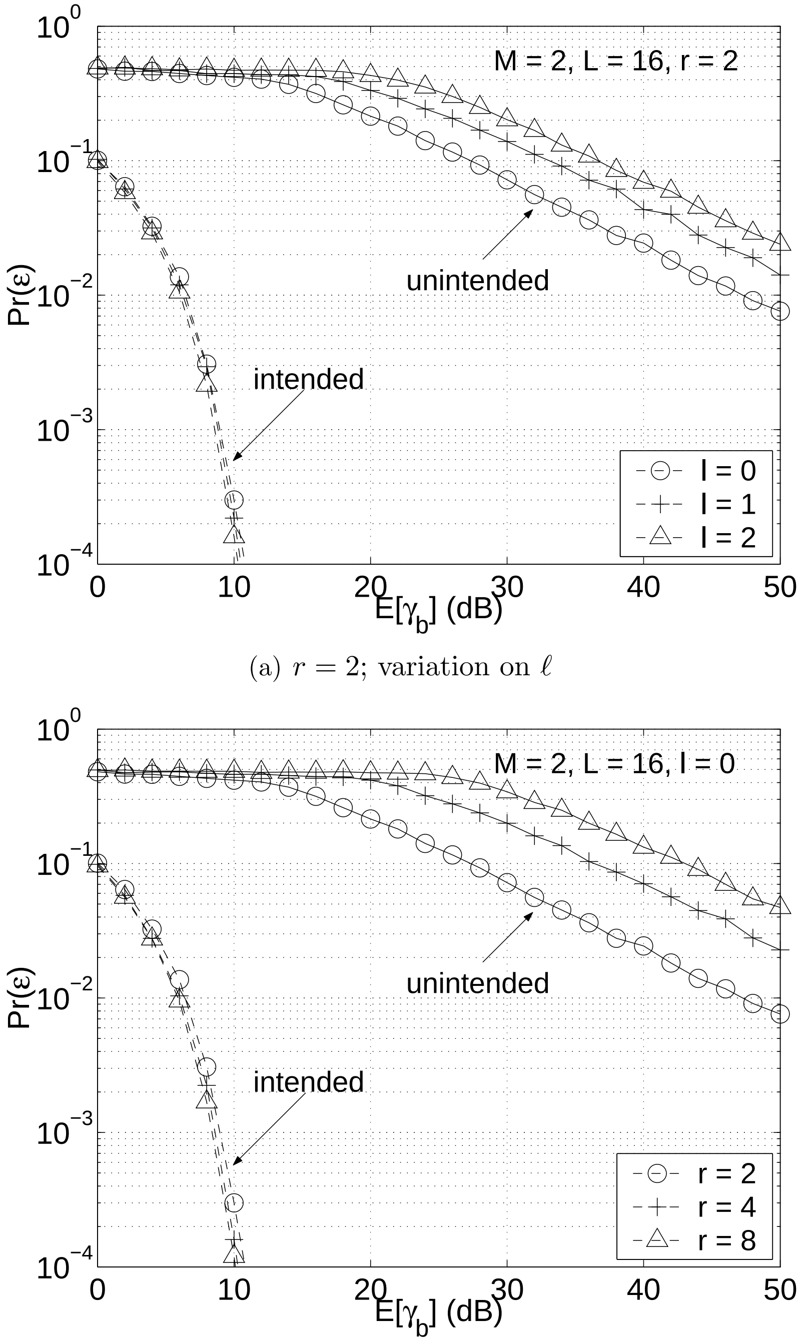
Figure 5.4: Simulated lower bound on the $\Pr(\epsilon)$ of the intended receiver for the 1st transmitter via (5.7) vs. SNR for various nested maps in a two-transmitter system ($H_2 = 2028$). Solid curves with markers correspond to $M = 2$, and solid curve without markers corresponds to analytically computed $\Pr(\epsilon)$ for single-user case ($M = 1$).

intended receiver $\Pr(\epsilon)$ is in contrast to the single-user case in Chapter 3, where the intended receiver $\Pr(\epsilon)$ is independent of $\ell$ and degrades with increasing $r$, although this degradation is largely mitigated with higher spreading gain. Since this $\Pr(\epsilon)$ degradation with higher $r$ is due to a reduction in minimum power of the spreading codeword as discussed in Sections 2.2.2 and 3.1, the $\Pr(\epsilon)$ trends with respect to the parameter $r$ in $M = 2$ system suggest that the MUI dominates over the minimum sequence power characteristics in determining the $\Pr(\epsilon)$ performance in multiuser systems.

Fig. 5.5 provides a comparison of the intended and unintended receiver $\Pr(\epsilon)$ performance as a function of SNR for several nested maps in the $M = 2$ system. The figure illustrates that the addition of another transmitter does not fundamentally alter the privacy characteristics of the single-user system explored in Chapter 3. Specifically, the decaying rate of the optimal unintended receiver $\Pr(\epsilon)$ for the $M = 2$ system is lower bounded by that of the single-user system and, hence, by $1/\sqrt{\text{SNR}}$. The intended receiver $\Pr(\epsilon)$, in contrast, decays at an exponential rate as a function of $\overline{\gamma}_b$. Moreover, for fixed $M$, the unintended receiver performance monotonically degrades as the nested recursion parameters $r$ and $\ell$ increase, while the intended receiver performance improves as observed above.

The privacy provided via the multiuser DS/CDMA systems based on nested maps can be efficiently, albeit conservatively, characterized by the $\Pr(\epsilon)$ of unintended receiver in the single-user system and the suboptimal intended receivers in the multiuser system of interest. In particular, the $\Pr(\epsilon)$ of the conventional single-user detector for the $i$-th transmitter, given by

$$\hat{b}(\mathbf{y}, c_i[0]) = \operatorname{sgn}\left(\sum_{n=0}^{L-1} F^n\left(c_i[0]\right) y[n]\right), \tag{5.8}$$



(a) $r = 2$; variation on $\ell$

(b) $\ell = 0$; variation on $r$

Figure 5.5: Simulated lower bounds on the $\Pr(\epsilon)$ of the intended and unintended receiver for 1st transmitter via (5.7) vs. SNR for various nested maps in a two-transmitter system. Dashed curves correspond to the intended receiver ($H_2 = 2028$) and solid curves correspond to the unintended receiver ($H_1 = 2028$).

where $y[n]$ is as in (5.1), can furnish a loose upper bound on the $\Pr(\epsilon)$ of the optimal intended receiver that is captured by the ML multiuser detector in (5.6). In addition, the unintended receiver performance in the single-user system, explored in Section 3.2, lower bounds its counterpart in multiuser systems. The privacy characterized with these bounds is pessimistic; the $\Pr(\epsilon)$ of (5.8) is substantially inferior to that of the optimal intended receiver, since this single-user detector in effect treats the MUI as additive Gaussian noise and its performance is interference limited. Moreover, the unintended receiver performance in the single-user system lower bounds the unintended receiver $\Pr(\epsilon)$ in the collusion scenarios where all receivers except the intended one in a network share their initial conditions to better demodulate a particular transmission. Thus such single-user system performance does not reflect not only the presence of MUI but also the possible (and likely) lack of knowledge of multiple initial conditions. Nevertheless, for systems with moderate-to-high spreading gain that is significantly higher than the number of users, this pessimistic setting can still illustrate the strength of privacy provided with the pseudochaotic DS/CDMA systems for a wide range of system parameters.

Fig. 5.6 shows the $\Pr(\epsilon)$ performance of the conventional single-user intended receiver in a four-transmitter network and that of the unintended receiver in the single-user system in Section 3.2 for the nested map $F_{16,4}$ and the spreading gain $L = 64$. This figure illustrates a conservative estimate of the privacy achievable in any $M = 4$ scenarios, given $r, \ell$, and $L$. In particular, the $\Pr(\epsilon)$ of unintended receiver in the single-user setting lower bounds that of the colluding unintended receivers that do not know the initial condition of the intended transmitter but do know those of the remaining three transmitters. As is apparent from the figure, the class of DS/CDMA systems based on nested maps can provide private and reliable multiuser

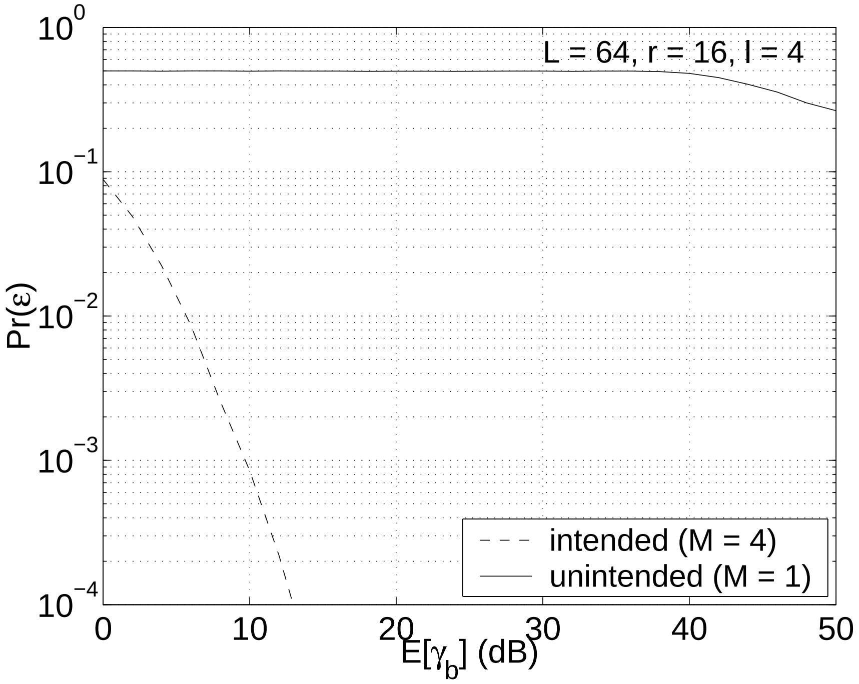


Figure 5.6: Simulated $\Pr(\epsilon)$ of single-user intended receiver (5.8) in $M = 4$ system (dashed curve) and simulated unintended receiver $\Pr(\epsilon)$ in $M = 1$ system via (3.19) (solid curve), for the nested map $F_{16,4}$ and $L = 64$.

communication that is not compromised by the presence of interference from other transmitters as well as potential collusion among multiple unintended receivers within the network.

# Chapter 6

# Contributions and Future Directions

This final chapter summarizes the contributions of this dissertation and highlights some of the areas that merit further research.

## 6.1 Contributions

In this dissertation we have focused on design and analysis of a class of pseudochaotic DS/CDMA systems for providing a desired level of privacy benefits to authorized users. In the context of linear modulation with spreading sequences arising from a class of one-dimensional piecewise-linear chaotic maps, we have explored the bit error probability performance advantages that these modulation techniques can provide to intended receivers that know the initial condition over unintended receivers that do not know the initial condition of targeted transmitter. Specifically, we have developed systematic design methods for generating pseudochaotic spreading sequences with successively worse unintended receiver performance. These sequences yield intended user performance similar to that of conventional DS/CDMA systems, in addition to quantifiable unintended user performance that is provably and substantially worse than the intended ones.

We have found that the class referred to as piecewise-linear $P \times Q$ partition maps contains rich subclass of maps that are amenable to efficient evaluation of the associated receiver performance. These maps exhibit a wide range of performance behaviors, which can be customized with variation of map parameters. We have introduced useful representations for these maps and described the associated sequence power characteristics. This characterization allowed the construction of computationally efficient evaluation metrics of the bit error probability performance.

As a main contribution of this dissertation, we have identified key relationships between features of $P \times Q$ partition maps and the intended and unintended receiver performance, and exploited such relationships to construct recursive algorithms for constructing nested sequences of maps that improve the privacy benefits at each step of the recursion, without affecting the intended receiver performance. The motivation behind these algorithms came from our revelation that the map symmetry and the partitioning of decision regions for signal detection are of prime importance in providing attractive privacy. First, we have found that maps with the same sensitivity to initial conditions and the same intended receiver performance can provide remarkably different privacy trends. In particular, DS/CDMA systems based on odd symmetric maps provide superior privacy over those with even or asymmetric maps, as in the former systems information bits are effectively distinguishable only at codeword boundaries. Among the subclass of fully-stretching $P \times Q$ partition maps with the same level of sensitivity to initial conditions, the $r$-adic maps are optimal since this class of odd maps has the finest partitioning of decision regions at codeword boundaries. These findings led to the nesting algorithms for producing spreading sequences that can meet a required level of intended receiver performance while satisfying a constraint on the unintended receiver performance.

As the next key contribution, we have developed efficient metrics for quantifying the unintended receiver performance in the context of the nested maps from the above recursive algorithms, and found that the class of DS/CDMA systems employing these maps can provide substantial privacy benefits while proving resilient against channel effects and multiuser interference. To obtain such performance metrics, we have derived and utilized the asymptotic decaying rate of the unintended receiver error probability as well as the dependence of $\Pr(\epsilon)$ on the nesting algorithm step and the spreading gain. In the process, we have shown that the unintended receiver $\Pr(\epsilon)$ follows a decaying rate of $1/\sqrt{\mathrm{SNR}}$ that is independent of the type of channel as well as the type and degree of diversity available. Because of this remarkable characteristic, the unintended receiver performance in time-varying channels is crippled in the presence of channel estimation errors, while the associated degradation of intended receiver $\Pr(\epsilon)$ is minimal for system parameters of practical interest. Moreover, as we have illustrated, multiuser interference does not compromise the privacy trends of nested map-based synchronous DS/CDMA, since the spreading sequences possess attractive correlation and broadband spectra that improve with the nested recursion step.

Finally, we have developed optimal digital implementation methods for generating pseudochaotic spreading sequences based on finite precision digital implementations. These methods produce maximal-length sequences, the set of which, for channels of practical interest and sufficient precision depth, closely approximates that of chaotic trajectories from nested maps and preserves the important properties of the underlying trajectories for attaining private and reliable communications.

## 6.2 Future Directions

There are a number of interesting and fruitful directions for further research that arise as extensions of this dissertation. In the following we summarize a representative collection of the important directions for future work, including some of the issues that have been identified in the earlier chapters.

While our investigation of the pseudochaotic DS/CDMA systems over synchronous channels illustrates many of the key privacy characteristics in multiuser networks, important extensions can be pursued in an effort towards efficient evaluation of a wide range of multiuser communication scenarios. For instance, our analysis can be extended to the case of asynchronous channels that arise in many applications. Such extensions entail examining the partial correlation properties of pseudochaotic sequences considered. Moreover, more accurate and efficient lower and upper bounds on the optimal and suboptimal detector performance can be developed to facilitate performance characterization in scenarios with a large number of transmitters. In particular, the $\Pr(\epsilon)$ characteristics of suboptimal detectors with attractive performance-complexity trade-offs, in conjunction to the maximum-likelihood multiuser detectors developed in this dissertation, may provide efficient characterization of privacy trends. In addition, these suboptimal detectors can be the most attractive practical option for both intended and unintended receivers, because the prohibitive computational complexity of optimal detectors severely limit their usefulness in networks with even moderate number of users.

Another interesting future direction lies in filtering of spreading sequences for different trade-off characteristics between modulator complexity and privacy benefits from those associated with spreading sequences considered in this work. Suitable quantization of the pseudochaotic sequences based on nested maps, for instance, can yield modulation outputs with good peak-to-average power ratio and less stringent requirements on amplifier linearity, at the cost in privacy.

A natural, if daunting, extension of our work is to increase the degrees of freedom in choosing what constitutes the side information (the key) for intended receivers and in selecting the chaotic dynamics for spreading sequence generation. A parameterized description of the chaotic map, for example, can be part of the side information along with the initial condition, for DS/CDMA systems that can employ a range of chaotic maps. Increasing the degree of uncertainty for unintended receivers comes at the price of smaller number of bits (precision depth) for describing the initial condition or larger key size and, hence, reduced bandwidth efficiency. Also, there may be an additional hardware cost that arises from enabling changes of the chaotic map. Such extensions create several interesting trade-offs among allocation of the amount of side information between the initial condition and the choice of map, the associated privacy, and the bandwidth efficiency. Another possible extension is to optimize the privacy benefits over a richer class of chaotic maps, including multidimensional dynamics. The challenge in these extensions is to ensure that such class provides a framework wherein systematic selections of pseudochaotic sequences with broadband spectra and cross-spectra can be made for attractive implementation and privacy benefits that can be efficiently quantified.

The offshoot from this work that can be perhaps the most consequential in a broad range of disciplines in science and engineering is the generalization of the optimal digital implementation methods developed herein to broader families of pseudochaotic sequences. Methods for generating pseudochaotic sequences that preserve important properties of the underlying trajectories from a chaotic map of interest can be useful in many applications exploiting chaotic trajectories as well as in numerical study of chaotic dynamics. Examples of such applications range from sigma-delta modulator designs for analog-to-digital conversion [33] and error correcting coding [34] to random number generation [15, 35] and weather forecasting [36].

# Appendix A

## A.1 Definitions for Chaotic Map Characteristics

In this appendix we present the definitions of important properties that the chaotic maps of interest and the associated sequences have, *i.e.*, exactness, ergodicity, and Markovity, in the context of this dissertation. Specifically, all $P$-partition maps are Markov, exact, and (hence) ergodic maps, and all nested maps in Section 3.3 are Markov and can be made to be exact and ergodic:

**Definition 2.** *[19, 20] A piecewise linear map $F(\cdot)$ is Markov, if $F(\cdot)$ maps the set of partition points $\mathbf{P} = \{a_0, a_1, \ldots, a_P\}$ into $\mathbf{P}$. If $F(\cdot)$ is discontinuous at $a_i \in I$, both $F(a_i^-)$ and $F(a_i^+)$ need be in $\mathbf{P}$, where $F(a_i^-)$ and $F(a_i^+)$ are the right and left limits of $F$ at $a_i$, respectively.*

**Definition 3.** *[20] Let $l(J)$ denote the length of an interval $J$ on the set of real values $\mathbf{R}$. A map $F : I \to I$ is called exact if for any interval $J \subset I$ with $l(J) > 0$,*

$$\lim_{n\to\infty} l\left(F^n(J)\right) = l(I), \tag{A.1}$$

*where $F^n(\cdot)$ denotes the $n$-fold composition of $F(\cdot)$.*

**Definition 4.** *[20] A nonsingular map $F : I \to I$ is called ergodic if every set $J \in I$,* *for which* $F^{-1}(J) = J$, *is such that either* $l(J) = 0$ *or* $l(I \cap J^c) = 0$.

# Appendix B

## B.1 Approximate Maximum Likelihood Sequence Estimation for Nested Maps

In this appendix we present extensions of ML estimation algorithms in [24] for the class of nested maps in Sec. 3.3 that includes the class of $P$-partition maps. These extensions are exploited in the construction of the GLRT detector presented in Sec. 3.2.

We denote by $\hat{c}_{\mathrm{ML}}[n|k, \mathbf{b}_o]$ the ML estimate of $c[n]$ given $y[m]$ for $m \leq k$, and assuming

$$\mathbf{b} = \mathbf{b}_o \overset{\triangle}{=} \begin{bmatrix} b_o[0] & b_o[1] & \cdots & b_o[N-1] \end{bmatrix}^{\mathrm{T}}$$

is transmitted. The filtered ML estimates $\hat{c}_{\mathrm{ML}}[n|n, \mathbf{b}_o]$, for $n = 0, 1, \ldots, NL-1$, can be readily obtained via a straightforward extension of the algorithm in [24], by exploiting the identity

$$\left| a - F_s^{-1}(b) \right| = \left| F_s(a) - b \right| / \beta \,,$$

where $\beta = |P/Q|$, and which holds for any $a, b \in I$ and any admissible $s$ in a nested map $F(\cdot)$. Given $\tilde{y}[n] = y[n]/A$, the recursion for the intermediate sequence of estimates $\hat{c}[n|n, \mathbf{b}_o]$ is given by

$$\hat{c}[n|n, \mathbf{b}_o] = \frac{(\beta^2 - 1)\,\beta^{2n}\tilde{y}[n]b_o\left[\lfloor n/L \rfloor\right] + (\beta^{2n} - 1)\,\hat{c}[n|n-1, \mathbf{b}_o]}{\beta^{2(n+1)} - 1}\,, \tag{B.1}$$

where

$$\hat{c}[n|n-1, \mathbf{b}_o] = F\left(\hat{c}[n-1|n-1, \mathbf{b}_o]\right)\,,$$

and where the recursion is initialized via $\hat{c}[0|0, \mathbf{b}_o] = \tilde{y}[0]b_o[0]$. The ML estimate is then obtained by amplitude-limiting this intermediate estimate according to

$$\hat{c}_{\mathrm{ML}}[n|n, \mathbf{b}_o] = \mathcal{I}\left(\hat{c}[n|n, \mathbf{b}_o]\right)$$

where

$$\mathcal{I}(x) = \begin{cases} x, & |x| \le 1 \\ \mathrm{sgn}(x), & |x| \ge 1 \end{cases}\,,$$

and where $\mathrm{sgn}(x)$ in (4.8) denotes the sign of $x$. The smoothed ML estimates $\hat{c}_{\mathrm{ML}}[n|NL{-}1, \mathbf{b}_o]$, in contrast, cannot be readily obtained for nested maps, because the ML estimate of an itinerary point $\hat{s}[n|N]$, in general, cannot be expressed in terms of $\hat{c}_{\mathrm{ML}}[n|n, \mathbf{b}_o]$. However, computationally efficient algorithmic extensions yielding smoothed estimates can be used to approximate the performance characteristics of the smoothed ML estimates. Specifically, we consider the estimates formed via

$$\hat{c}\,[n|NL-1, \mathbf{b}_o] = F^{-1}_{\tilde{s}[n]}\left(\hat{c}\,[n+1|NL-1, \mathbf{b}_o]\right)\,, \tag{B.2}$$

initialized with $\hat{c}[NL-1|NL-1, \mathbf{b}_o] = \hat{c}_{\mathrm{ML}}[NL-1|NL-1, \mathbf{b}_o]$, where

$$\tilde{s}[n] = \underset{s[n]\in\mathcal{S}_n}{\arg\min}\left\{\tilde{y}[n]\,b_o\left[\left\lfloor\frac{n}{L}\right\rfloor\right] - F^{-1}_{s[n]}\left(\hat{c}\,[n+1|NL-1, \mathbf{b}_o]\right)\right\}^2\,, \tag{B.3}$$

and where $\mathcal{S}_n$ denotes the set of admissible $s[n]$ for the given map. As illustrated in Sec. 3.2, (B.3) results in estimates $\hat{c}\,[n|NL-1, \mathbf{b}_o]$, which, when used in the context of the GLRT-type detector (3.14), yield $\Pr(\epsilon)$ performance close to that predicted by the lower bound provided by the detector defined in (3.13).

## B.2 A Detection Scenario for Lower Bounding the Unintended Receiver $\Pr(\epsilon)$

In this appendix we develop a communication scenario, the optimal receiver $\Pr(\epsilon)$ for which can be used to lower bound the $\Pr(\epsilon)$ of unintended receiver for DS/SS based on $r$-adic maps. This scenario is exploited in deriving the asymptotic decaying rate of the unintended receiver $\Pr(\epsilon)$ in Section 3.2.3 and Section 4.4.3.

We consider the unintended detection of a differentially encoded symbol based on observation

$$\begin{aligned} y[n] &= x[n] + w[n] \\ &= \frac{A}{\sqrt{L}}\,\alpha F^n(c)\; b\Big[\Big\lfloor \frac{n}{L} \Big\rfloor\Big] + w[n]\,, \end{aligned} \tag{B.4}$$

a single-user model simplified from (2.3) for general slow fading channels. As in Section 3.2.3 and Section 4.4.3, we assume that an IID sequence $i[n] = \pm 1$ is differentially encoded into the sequence $b[n] = i[n]\,b[n-1]$, and focus on the detection of $i[D]$, $1 \leq D \leq N-1$, given the observation $\mathbf{y}$ in the form of (3.10) with $y[n]$ in (B.4).

We first consider a detector that is provided with the remaining $N-2$ information symbols

$$\tilde{\mathbf{i}} \stackrel{\triangle}{=} \Big[ i[1] \quad \cdots \quad i[D-1] \quad i[D+1] \quad \cdots \quad i[N-1] \Big]^T \,, \tag{B.5}$$

as well as some additional side information that depends on whether or not $c[0]$ belongs in the set

$$I_o \stackrel{\triangle}{=} \bigcup_{c \in \mathcal{C}^{(D)}} I(c)\,,$$

where $I(c) \stackrel{\triangle}{=} (c, c+\Delta)$, $\Delta \stackrel{\triangle}{=} 2\,P^{-(NL-1)}$, and $\mathcal{C}^{(D)}$ is the preimage of $\{0\}$ under $F^{DL-1}$, *i.e.*,

$$\mathcal{C}^{(D)} \stackrel{\triangle}{=} F^{-(DL-1)}(0) = \Big\{ c \in I; \quad F^{DL-1}(c) = 0 \Big\} \ . \tag{B.6}$$

Specifically, if $c[0] \notin I_o$, the receiver is provided with the value of $i[D]$. If $c[0] \in I_o$, the receiver is only told that the initial condition is from the set $\{\pm \underline{c}[0] + \delta\}$, where $\underline{c}[0]$ denotes the unique $c \in \mathcal{C}^{(D)}$ for which $c[0] \in I(c)$, and $\delta \stackrel{\triangle}{=} \delta(c[0]) = c[0] - \underline{c}[0]$. Note, that since $F$ is odd, $\underline{c}[0] \in \mathcal{C}^{(D)}$, implies that $-\underline{c}[0] \in \mathcal{C}^{(D)}$. Also,[1] since $|\mathcal{C}^{(D)}| = P^{DL-1}$, $\Pr(c[0] \in I_o) = P^{(D-N)L}$.

The availability of (B.5) limits the possible $\mathbf{b}$ candidates under hypothesis $i[D] = \imath$ at the receiver to $\tilde{\mathcal{S}}_{\imath}^{(D)} = \{\bar{\mathbf{b}}_{\imath},\, -\bar{\mathbf{b}}_{\imath}\}$, where

$$\bar{\mathbf{b}}_{\imath} \stackrel{\triangle}{=} \Big[ \bar{b}[0] \quad \bar{b}[1] \quad \cdots \quad \bar{b}[D] \quad \imath\,\bar{b}[D+1] \quad \cdots \quad \imath\,\bar{b}[N-1] \Big]^{\mathrm{T}} \,,$$

and where the $n$th entry of $\bar{\mathbf{b}}_{\imath}$ denotes the $n$th differentially encoded symbol, in the case that $i[D] = \imath$, $\tilde{\mathbf{i}}$ is as in (B.5), and given $\bar{b}[0] = \sqrt{\mathcal{E}_b}$. Hence, when $c[0] \in I_o$, the

[1] The set $I_o$ could be made larger, *e.g.*, by also including all sets of the form $(c - \Delta, c)$ with $c \in \mathcal{C}^{(D)}$. Although this would yield a somewhat tighter lower bound, its rate of decay cannot be made lower than $1/\sqrt{\overline{\gamma}_b}$.

optimal detector is given by $\hat{\imath}_1[D] = \arg\max_{\imath \in \pm 1} \Pr\left(\mathbf{x} \in \mathcal{X}_{\imath}^{(D)} | \mathbf{y}\right)$, where the signal set under hypothesis $i[D] = \imath$ is given by

$$\mathcal{X}_{\imath}^{(D)} = \left\{ \mathbf{x}(c, \mathbf{b}); \quad c \in \{\pm \underline{c}[0] + \delta\}, \mathbf{b} = \tilde{\mathcal{S}}_{\imath}^{(D)} \right\} \ . \tag{B.7}$$

Letting $\epsilon_1$ denote the error event of this receiver we have

$$\Pr(\epsilon) \ \geq \ \Pr(c[0] \in I_o) \ \Pr(\epsilon_1 | c[0] \in I_o) \ . \tag{B.8}$$

We next lower bound $\Pr(\epsilon_1 | c[0] \in I_o)$. First, when $c[0] \in I_o$ and $\mathbf{b} = \bar{\mathbf{b}}_1$ the signal term is given by

$$x[n; c[0], \bar{\mathbf{b}}_1] = \underline{x}[n] + r[n] \tag{B.9a}$$

for all $0 \leq n \leq NL - 1$, where

$$\underline{x}[n] = \lim_{u \to 0^+} x[n; \underline{c}[0] + u, \bar{\mathbf{b}}_1] \,, \tag{B.9b}$$

$$r[n] = \frac{A}{\sqrt{L}} \alpha s[n] \, \bar{b}\left[ \left\lfloor \frac{n}{L} \right\rfloor \right] \ P^n \delta \,, \tag{B.9c}$$

and where $s[n]$ is defined via the recursion

$$s[n] = s[n-1] \ \mathrm{sgn}\left(\underline{c}[n]\right)$$

with $\underline{c}[n] \overset{\triangle}{=} \lim_{u \to 0^+} F^n(\underline{c}[0] + u)$, and initialized with $s[0] = 1$. Consequently, $x[n; c[0], \bar{\mathbf{b}}_1]$ varies *linearly* with $c[0]$ (or, rather $\delta = c[0] - \underline{c}[0]$). The significance of (B.9) is that, as the reader can readily verify, the sets $\mathcal{X}_{\imath}^{(D)}$ from (B.7) can be expressed in the following convenient form:

$$\mathcal{X}_{\imath}^{(D)} = \left\{ \mathbf{x}; \quad \mathbf{x} = \ell \begin{bmatrix} \mathbf{p} + m\,\imath\,\mathbf{r} \\ m\,\mathbf{u} \end{bmatrix}, \quad \ell,\, m \in \{-1,\, 1\} \right\} \tag{B.10}$$

where $\mathbf{p} = \begin{bmatrix} \underline{x}[0] & \underline{x}[1] & \underline{x}[2] & \cdots & \underline{x}[DL-1] \end{bmatrix}^T$, $\mathbf{r} = \begin{bmatrix} r[0] & r[1] & \cdots & r[DL-1] \end{bmatrix}^T$, and

$$\mathbf{u} = \begin{bmatrix} x[DL; c[0], \bar{\mathbf{b}}_1] & x[DL+1; c[0], \bar{\mathbf{b}}_1] & \cdots & x[NL-1; c[0], \bar{\mathbf{b}}_1] \end{bmatrix}^T ,$$

and where $\underline{x}[n]$, $x[n; c[0], \bar{\mathbf{b}}_1]$, and $r[n]$ are given by (B.9). Finally, given a fixed $c[0] \in I_o$, $\Pr(\epsilon_1 | c[0])$ is lower bounded by the probability of error of a detector that must decide between $\tilde{\mathbf{x}} = \mathbf{x}_1$ and $\tilde{\mathbf{x}} = \mathbf{x}_{-1}$, based on $\tilde{\mathbf{y}} = \tilde{\mathbf{x}} + \mathbf{w}$, where $\mathbf{x}_\imath = [\mathbf{p}^T + \imath\mathbf{r}^T \;\; \mathbf{u}^T]^T$, and $\mathbf{w}$ is defined as $\mathbf{y}$ in (3.10) with $y[n]$ replaced by $w[n]$. Indeed, $\mathbf{x}$ from (B.10) can be viewed as the output of a channel with input $\tilde{\mathbf{x}}$: given $\tilde{\mathbf{x}} = [\mathbf{p}^T + \imath\mathbf{r}^T \;\; \mathbf{u}^T]^T$, the channel outputs $\mathbf{x} = \ell[\mathbf{p}^T + \imath m\mathbf{r}^T \;\; m\mathbf{u}^T]^T$, where $m, \ell = \pm 1$ are random variables with equally likely values and statistically independent of one another and $\tilde{\mathbf{x}}$. Hence, due to the data processing inequality [37], the optimal receiver based on (B.10) cannot outperform the one that detects $\tilde{\mathbf{x}}$ based on $\tilde{\mathbf{y}}$, *i.e.*,

$$\Pr(\epsilon_1 | c = \underline{c}[0] + \delta, \alpha) \geq \mathcal{Q}\left(\sqrt{\tilde{\gamma}(\delta, \alpha)}\right) \tag{B.11}$$

where

$$\tilde{\gamma}(\delta, \alpha) = \frac{\|\mathbf{x}_1 - \mathbf{x}_{-1}\|^2}{2N_o} = \frac{2\,\|\mathbf{r}\|^2}{N_o} = \delta^2 \frac{6\,\alpha^2 \mathcal{E}_b (P^{2DL} - 1)}{L(P^2 - 1)\,N_o} = C\overline{\gamma}_b \alpha^2 \delta^2 ,$$

with $C = \frac{6(P^{2DL}-1)}{L(P^2-1)}$. The above results can be readily modified for AWGN channels in Chapter 3 and slow flat fading channels in Chapter 4 by setting $\alpha = 1$ and $\alpha = \mu$ in (4.12), respectively.

# Appendix C

## C.1 Probability Density Function of Observables in Slow Flat Fading

In this appendix we characterize the joint conditional PDF of observables in slow flat fading that is useful in constructing $\Pr(\epsilon)$ performance metrics for intended and unintended receivers in Chapter 4 via the developments in App. C.2.

Given

$$\hat{\mathbf{a}} \stackrel{\triangle}{=} \begin{bmatrix} \hat{\alpha}_1 & \hat{\alpha}_2 & \cdots & \hat{\alpha}_K \end{bmatrix}^{\mathrm{T}}$$

and

$$\mathbf{y}_k \;=\; \mathbf{y}_k^L \;\stackrel{\triangle}{=}\; \begin{bmatrix} y_k[0] & y_k[1] & \cdots & y_k[L-1] \end{bmatrix}^{\mathrm{T}} \tag{C.1}$$

with $y_k[n]$ as in (4.5), the joint PDF of

$$\mathcal{Y} \;\stackrel{\triangle}{=}\; \{y_k[n];\; k = 1, 2, \cdots, K \text{ and } n = 0, 1, \cdots, NL-1\}$$

conditioned on $\mathbf{b}$ in (3.11), $\mathbf{c}^{NL}$, and $\hat{\mathbf{a}}$ is given by

$$p_{\mathcal{Y}|\mathbf{b},\mathbf{c}^L,\hat{\mathbf{a}}}(\mathcal{Y}|\mathbf{b},\mathbf{c}^L,\hat{\mathbf{a}}) = \frac{1}{(2\pi)^{\frac{NLK}{2}} \left|\frac{N_o}{2}\Xi\right|^{\frac{K}{2}}} \exp\left\{-\frac{1}{N_o}\sum_{k=1}^{K}(\mathbf{y}_k-\mathbf{m}_k)^H \Xi^{-1}(\mathbf{y}_k-\mathbf{m}_k)\right\},$$

where $\mathbf{x}^H$ denotes the conjugate transpose of $\mathbf{x}$,

$$\begin{aligned}
\mathbf{m}_k &= \mathbf{m}_k^{NL} \overset{\triangle}{=} E\left[\mathbf{y}_k | b, \mathbf{c}^{NL}, \hat{\alpha}_k\right] \\
&= \left[\hat{\alpha}_k \tfrac{A}{\sqrt{L}} c[0]b[0] \quad \hat{\alpha}_k \tfrac{A}{\sqrt{L}} c[1] b\left[\left\lfloor \tfrac{1}{L} \right\rfloor\right] \quad \cdots \quad \hat{\alpha}_k \tfrac{A}{\sqrt{L}} c[NL-1] b[N-1]\right]^{\mathrm{T}}, \qquad \text{(C.2)}
\end{aligned}$$

and the scaled covariance matrix $\Xi \overset{\triangle}{=} \frac{1}{N_o} E\left[(\mathbf{y}_k - \mathbf{m}_k)(\mathbf{y}_k - \mathbf{m}_k)^H\right]$ is a symmetric matrix with its element at $i$-th row, $j$-th column given by

$$\Xi_{i,j} = \begin{cases} \frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} c^2[i] + 1 & i = j \\ \frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} c[i]c[j] \operatorname{sgn}\left(b\left[\left\lfloor \frac{i}{L} \right\rfloor\right] b\left[\left\lfloor \frac{j}{L} \right\rfloor\right]\right) & i \neq j \end{cases} \qquad \text{(C.3)}$$

for $1 \leq i \leq NL$, $1 \leq j \leq NL$. The inverse of $\Xi$ can be readily shown to be a symmetric matrix, whose element at $i$-th row, $j$-th column is given by

$$\Xi_{i,j}^{-1} = \begin{cases} \frac{1}{|\Xi|} \left( \frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} \sum_{n \neq i} c^2[n] + 1 \right) & i = j \\ \frac{1}{|\Xi|} \cdot \frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} c[i]c[j] \operatorname{sgn}\left(b\left[\left\lfloor \frac{i}{L} \right\rfloor\right] b\left[\left\lfloor \frac{j}{L} \right\rfloor\right]\right) & i \neq j \end{cases} \qquad \text{(C.4)}$$

for $1 \leq i \leq NL$, $1 \leq j \leq NL$, where the determinant of $\Xi$ is

$$|\Xi| = \frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} \sum_{n=0}^{NL-1} c^2[n] + 1 \,. \qquad \text{(C.5)}$$

Using (C.2) and (C.4), we have

$$\begin{aligned}
\mathbf{y}_k^H \Xi^{-1} \mathbf{y}_k = \frac{1}{|\Xi|} \Bigg\{ & \sum_{n=0}^{NL-1} |y_k[n]|^2 + \frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} \left( \sum_{n=0}^{NL-1} \left( \sum_{l=0}^{NL-1} c^2[l] - c^2[n] \right) |y_k[n]|^2 \right. \\
& \left. - 2 \sum_{n=0}^{NL-2} \sum_{l=n+1}^{NL-1} c[n]c[l] \operatorname{sgn}\left( b\left[\left\lfloor \frac{n}{L} \right\rfloor\right] b\left[\left\lfloor \frac{l}{L} \right\rfloor\right] \right) y_k^*[n] y_k[l] \right) \Bigg\} \,, \qquad \text{(C.6)}
\end{aligned}$$

$$\mathbf{m}_k^H \Xi^{-1} \mathbf{y}_k \;=\; \hat{\alpha}_k^* \frac{A}{\sqrt{L}\,|\Xi|} \sum_{n=0}^{NL-1} c[n] b \left[ \left\lfloor \frac{n}{L} \right\rfloor \right] y_k[n] \;, \tag{C.7}$$

and

$$\mathbf{m}_k^H \Xi^{-1} \mathbf{m}_k \;=\; |\hat{\alpha}_k|^2 \frac{A^2 \mathcal{E}_b}{L\,|\Xi|} \sum_{n=0}^{NL-1} c^2[n] \;. \tag{C.8}$$

The above equations (C.6), (C.7), and (C.8) are utilized in deriving the intended and unintended receiver structures in the following App. C.2 and the $\Pr(\epsilon)$ performance metrics in Section 4.3.1 and Section 4.4.1.

## C.2 Maximum Likelihood Reception in Slow Flat Fading

In this appendix we exploit the findings in App. C.1 to develop the optimum intended and unintended receiver in slow flat Rayleigh fading with the knowledge of channel estimates $\hat{\alpha}_k$.

The maximum likelihood intended receiver of the transmitted bit sequence $\mathbf{b}$ based on observations $\mathcal{Y}^{K,NL}$ in (4.6), $c[0]$, and $\hat{\mathbf{a}}$ in (4.27) is

$$\begin{aligned} \hat{\mathbf{b}}_{\mathrm{ML}}(\mathcal{Y}, c[0]) \;&=\; \arg\max_{\mathbf{b}} \; p_{\mathcal{Y}|\mathbf{b},\mathbf{c}^{NL},\hat{\mathbf{a}}}(\mathcal{Y}|\mathbf{b},\mathbf{c}^{NL},\hat{\mathbf{a}}) \\ &=\; \arg\min_{\mathbf{b}} \; \mathrm{Re}\left\{ \sum_{k=1}^{K} \left( \mathbf{y}_k^H \Xi^{-1} \mathbf{y}_k - 2\, \mathbf{m}_k^H \Xi^{-1} \mathbf{y}_k + \mathbf{m}_k^H \Xi^{-1} \mathbf{m}_k \right) \right\} \;, \end{aligned} \tag{C.9a}$$

where $\mathbf{y}_k = \mathbf{y}_k^{NL}$ in (C.1) is the observed sequence at the $k$-th receiver antenna element, $\mathbf{m}_k$ is as in (C.2), and $\Xi^{-1}$ defined in (C.4) is the inverse of $\Xi$, the covariance matrix of $\mathbf{y}_k$ scaled by $1/N_o$. Using (C.6), (C.7), and (C.8) in App. C.1, (C.9a) can be expressed as

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathcal{Y}, c[0]) = \arg\max_{\mathbf{b}} \Bigg\{ & \frac{A^2\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)} \\ & \cdot \sum_{n=0}^{NL-2}\sum_{l=n+1}^{NL-1} F^n(c)F^l(c)\,\mathrm{sgn}\left(b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]b\left[\left\lfloor\frac{l}{L}\right\rfloor\right]\right)\sum_{k=1}^{K}\mathrm{Re}\{y_k^*[n]y_k[l]\} \\ & + \frac{A}{\sqrt{L}}\sum_{n=0}^{NL-1} F^n(c)b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\sum_{k=1}^{K}\mathrm{Re}\left\{\hat{\alpha}_k^* y_k[n]\right\}\Bigg\}\ . \end{aligned} \tag{C.9b}$$

The maximum likelihood unintended receiver of the transmitted bit sequence $\mathbf{b}$ based on observation $\mathcal{Y}^{K,NL}$ with the knowledge of the channel estimates $\hat{\mathbf{a}}$ but without the knowledge of the initial condition $c[0]$ is given by

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathbf{y}) &= \arg\max_{\mathbf{b}} \int p_{\mathcal{Y}|\mathbf{b},c,\hat{\mathbf{a}}}(\mathcal{Y}|\mathbf{b},c,\hat{\mathbf{a}})p_{c[0]}(c)\,dc \\ &= \arg\max_{\mathbf{b}} \int \exp\Bigg\{-\frac{1}{N_o}\,\mathrm{Re}\Bigg\{\sum_{k=1}^{K}\big(\mathbf{y}_k^H\Xi^{-1}\mathbf{y}_k - 2\,\mathbf{m}_k^H\Xi^{-1}\mathbf{y}_k \\ &\qquad\qquad + \mathbf{m}_k^H\Xi^{-1}\mathbf{m}_k\big)\Bigg\}\Bigg\}\, p_{c[0]}(c)\,dc\ . \end{aligned} \tag{C.10a}$$

Taking the same step as in the above intended receiver case, using (C.6), (C.7), and

(C.8), (C.10a) can be expressed as

$$\begin{aligned}\hat{\mathbf{b}}_{\mathrm{ML}}(\mathbf{y}) = \arg\max_{\mathbf{b}} \int \exp\Bigg\{ -\frac{1}{N_o|\Xi|}\, \mathrm{Re}\Bigg\{ \sum_{k=0}^{K} \Bigg\{ \sum_{n=0}^{NL-1} |y_k[n]|^2 \\ + \frac{A^2\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)} \Bigg( \sum_{n=0}^{NL-1} |y_k[n]|^2 \Bigg( \sum_{l=0}^{NL-1} \left(F^l(c)\right)^2 - \left(F^n(c)\right)^2 \Bigg) \\ - 2 \sum_{n=0}^{NL-2} \sum_{l=n+1}^{NL-1} F^n(c) F^l(c)\, \mathrm{sgn}\Big( b\Big[\Big\lfloor \frac{n}{L} \Big\rfloor\Big]\, b\Big[\Big\lfloor \frac{l}{L} \Big\rfloor\Big] \Big) y_k^*[n] y_k[l] \Bigg) \\ - 2\, \hat{\alpha}_k^* \frac{A}{\sqrt{L}} \sum_{n=0}^{NL-1} F^n(c) b\Big[\Big\lfloor \frac{n}{L} \Big\rfloor\Big] y_k[n] \\ + \; |\hat{\alpha}_k|^2 \frac{A^2\mathcal{E}_b}{L} \sum_{n=0}^{NL-1} \left(F^n(c)\right)^2 \Bigg\}\Bigg\}\Bigg\}\, p_{c[0]}(c)\, dc \;,\end{aligned} \tag{C.10b}$$

where $|\Xi|$ in (C.5) is the determinant of $\Xi$.

## C.3 Intended Receiver $\Pr(\epsilon|\mathbf{c}^L)$ in Slow Flat Rayleigh Fading

In the following we focus on the case of perfect channel estimation and derive the intended receiver $\Pr(\epsilon)$ conditioned on $\mathbf{c}^L$ that is useful in obtaining the $\Pr(\epsilon)$ performance metrics in Section 4.3.1.

We first show that the output bit SNR $\gamma_O\left(\mu, \mathbf{c}^L\right)$ in (4.11) associated with a specific $\mathbf{c}^L$ is a chi-square-distributed random variable with $2K$ degrees of freedom. Since $\mathrm{Re}\{\alpha_k\}$ and $\mathrm{Im}\{\alpha_k\}$ are both IID, zero-mean, real-valued Gaussian random variables with variance $1/2$, $\mu = \sum_{k=1}^{K} |\alpha_k|^2$ follows chi-square distribution with $2K$ degrees of freedom;

$$p_\mu(\mu) = \frac{1}{(K-1)!}\, \mu^{K-1} \exp\{-\mu\} \;,$$

and, hence, the PDF of $\gamma_O$ conditioned on $\mathbf{c}^L$ is given by

$$p_{\gamma_{O|\mathbf{c}^L}}(\gamma) = \frac{1}{(K-1)!\left(\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)\right)^K}\,\gamma^{K-1}\exp\left\{-\frac{\gamma}{\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)}\right\}\,, \tag{C.11}$$

where

$$\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right) \overset{\triangle}{=} E\left[\gamma_b|\mathbf{c}^L\right] = A^2\,\overline{\gamma}_b\,\mathcal{E}\left(\mathbf{c}^L\right)\,. \tag{C.12}$$

The bit error probability conditioned on $\mathbf{c}^L$ can be obtained via methods in [38], using the following alternative definition of $\mathcal{Q}(\nu)$ in (3.5):

$$\mathcal{Q}(\nu) = \int_0^{\pi/2}\exp\left\{-\frac{\nu}{\sin^2\theta}\right\}\,d\theta\,. \tag{C.13}$$

Exploiting (C.13), we have

$$\begin{aligned}
\Pr(\epsilon|\mathbf{c}^L) &= \int_0^{\infty}\mathcal{Q}\left(\sqrt{\gamma}\right)p_{\gamma_{O|\mathbf{c}^L}}(\gamma)\,d\gamma \\
&= \frac{1}{\pi}\int_0^{\pi/2}\int_0^{\infty}\exp\left\{-\frac{\gamma}{\sin^2\theta}\right\}p_{\gamma_{O|\mathbf{c}^L}}(\gamma)\,d\gamma d\theta \qquad \text{(C.14a)}\\
&= \frac{1}{\pi}\int_0^{\pi/2}\left(1-\frac{\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)}{\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)+\sin^2\theta}\right)^K d\theta \qquad \text{(C.14b)}
\end{aligned}$$

where (C.14a) is due to (C.13) and the fact that the integrand is Lebesgue integrable, and (C.14b) is obtained by noting that the inner integral in (C.14a) is the Laplace transform of $p_{\gamma_{O|\mathbf{c}^L}}(\gamma)$. Expanding and integrating (C.14b) gives the desired expression

$$\begin{aligned}
\Pr(\epsilon|\mathbf{c}^L) &= \left[\frac{1}{2}\left(1-\sqrt{\frac{\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)}{1+\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)}}\right)\right]^K \\
&\quad\cdot\sum_{k=0}^{K-1}\binom{K-1+k}{k}\left[\frac{1}{2}\left(1+\sqrt{\frac{\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)}{1+\overline{\gamma}_{b|\mathbf{c}^L}\left(\mathbf{c}^L\right)}}\right)\right]^k \qquad \text{(C.14c)}
\end{aligned}$$

that is utilized in obtaining (4.14), (4.16), (4.17), (4.18), and (4.20).

## C.4 Maximum Likelihood Reception in Fast Flat Fading

In this appendix we develop the optimum intended and unintended receiver in slow flat Rayleigh fading with the knowledge of channel estimates $\hat{\alpha}_k$.

We first characterize the joint conditional PDF of observables in fast flat fading. Given

$$\hat{\mathcal{A}} \overset{\triangle}{=} \{\hat{\alpha}_k[n];\ k = 1, 2, \cdots, K \text{ and } n = 0, 1, \cdots, NL - 1\}$$

and $\mathcal{Y}^{K,NL}$ in (4.6), the joint PDF of $\mathcal{Y}$ conditioned on $\mathbf{b}$ in (3.11), $\mathbf{c}^{NL}$, and $\hat{\mathcal{A}}$ is given by

$$p_{\mathcal{Y}|\mathbf{b},\mathbf{c}^{NL},\hat{\mathcal{A}}}(\mathcal{Y}|\mathbf{b}, \mathbf{c}^{NL}, \hat{\mathcal{A}}) = \frac{1}{(2\pi)^{\frac{NLK}{2}} \left|\frac{N_o}{2}\Xi\right|^{\frac{K}{2}}} \exp\left\{-\sum_{k=1}^{K}\sum_{n=0}^{NL-1} \frac{\left|y_k[n] - \frac{A}{\sqrt{L}}\hat{\alpha}_k[n]c[n]b\left[\left\lfloor\frac{n}{L}\right\rfloor\right]\right|^2}{N_o\left(\frac{A^2\overline{\gamma}_b}{L\left(\overline{\gamma}_p+1\right)}\, c^2[n] + 1\right)}\right\},$$

where the scaled covariance matrix $\Xi$ is, in contrast to its counterpart (C.3) in slow fading, a diagonal matrix.

The maximum likelihood intended and unintended receivers are readily derived from the conditional PDF of $\mathcal{Y}$ above. First, the ML detector of the transmitted bit

$b[0]$ given $\mathcal{Y}$, $c[0]$, and $\hat{\mathcal{A}}$ is

$$\begin{aligned}
\hat{b}_{\mathrm{ML}}(\mathcal{Y}, c[0]) &= \arg\max_{b} p_{\mathcal{Y}|b,\mathbf{c}^L,\hat{\mathcal{A}}}(\mathcal{Y}|b, \mathbf{c}^L, \hat{\mathcal{A}}) \\
&= \arg\min_{b} \sum_{k=1}^{K} \sum_{n=0}^{L-1} \frac{|y_k[n]|^2 - 2\frac{A}{\sqrt{L}} \operatorname{Re}\{\hat{\alpha}_k^*[n] y_k[n]\} c[n] b + \frac{A^2 \mathcal{E}_b}{L} |\hat{\alpha}_k[n]|^2 c^2[n]}{\frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} c^2[n] + 1} \\
&= \arg\max_{b} \sum_{n=0}^{L-1} \frac{c[n] \sum_{k=1}^{K} \operatorname{Re}\left\{\hat{\alpha}_k^*[n] y[n]\right\}}{\frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} c^2[n] + 1} b \\
&= \operatorname{sgn}\left( \sum_{n=0}^{L-1} \frac{c[n] \operatorname{Re}\left\{y[n]\right\}}{\frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} c^2[n] + 1} \right), \qquad \text{(C.15)}
\end{aligned}$$

where

$$y[n] = \sum_{k=1}^{K} \hat{\alpha}_k^*[n] \, y_k[n]$$

is the output of the MRC. Next, the ML detector of the transmitted bit sequence $\mathbf{b}$ based on observation $\mathcal{Y}$ with the knowledge of the channel estimates $\hat{\mathcal{A}}$ but without the knowledge of the initial condition $c[0]$ is given by

$$\begin{aligned}
\hat{b}_{\mathrm{ML}}(\mathcal{Y}) &= \arg\max_{\mathbf{b}} \int p_{\mathcal{Y}|\mathbf{b},\mathbf{c}^{NL},\hat{\mathcal{A}}}(\mathcal{Y}|\mathbf{b}, \mathbf{c}^{NL}, \hat{\mathcal{A}}) p_{c[0]}(c) \, dc \\
&= \arg\max_{\mathbf{b}} \int \exp\Biggl\{ -\frac{1}{N_o} \sum_{k=1}^{K} \sum_{n=0}^{NL-1} \Biggl( \frac{|y_k[n]|^2 - 2\frac{A}{\sqrt{L}} \operatorname{Re}\left\{\hat{\alpha}_k^*[n] y_k[n]\right\} F^n(c) b\left[\left\lfloor \frac{n}{L} \right\rfloor\right]}{\frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} \left(F^n(c)\right)^2 + 1} \\
&\qquad + \frac{\frac{A^2 \mathcal{E}_b}{L} |\hat{\alpha}_k[n]|^2 \left(F^n(c)\right)^2}{\frac{A^2 \overline{\gamma}_b}{L\left(\overline{\gamma}_p + 1\right)} \left(F^n(c)\right)^2 + 1} \Biggr) \Biggr\} p_{c[0]}(c) \, dc \,. \qquad \text{(C.16)}
\end{aligned}$$

# Bibliography

[1] J. G. Proakis, *Digital Communications*, 4th ed. New York, NY: McGraw Hill, 2001.

[2] E. Ott, *Chaos in Dynamical Systems*, 2nd ed. Cambridge, UK: Cambridge University Press, 2002.

[3] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, “Synchronization of Lorenz-based chaotic circuits with applications to communications,” *IEEE Trans. Circuits Syst. II*, vol. 40, no. 10, pp. 626–633, Oct. 1993.

[4] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, Feb. 1990.

[5] ——, “Driving systems with chaotic signals,” *Phys. Rev. A*, vol. 44, no. 4, pp. 2374–2383, Aug. 1991.

[6] G. Heidari-Bateni and C. D. McGillem, “A chaotic direct-sequence spread-spectrum communication system,” *IEEE Trans. Commun.*, vol. 42, no. 2/3/4, pp. 1524–1527, Feb./Mar./Apr. 1994.

[7] T. Yang and L. O. Chua, “Chaotic digital code-division multiple access (CDMA) communication systems,” *Intl. J. of Bifurcation and Chaos*, vol. 7, no. 12, pp. 2789–2805, Dec. 1997.

[8] C.-C. Chen, K. Yao, K. Umeno, and E. Biglieri, “Design of spread-spectrum sequences using chaotic dynamical systems and ergodic theory,” *IEEE Trans. Circuits Syst. I*, vol. 48, no. 9, pp. 1110–1114, Sept. 2001.

[9] G. Mazzini, G. Setti, and R. Rovatti, “Chaotic complex spreading sequences for asynchronous DS-CDMA – Part I: System modeling and results,” *IEEE Trans. Circuits Syst. I*, vol. 44, no. 10, pp. 937–947, Oct. 1997.

[10] R. Rovatti, G. Setti, and G. Mazzini, “Chaotic complex spreading sequences for asynchronous CDMA – Part II: Some theoretical performance bounds,” *IEEE Trans. Circuits Syst. I*, vol. 45, no. 4, pp. 496–506, Apr. 1998.

[11] R. Rovatti, G. Mazzini, and G. Setti, "Interference bounds for DS-CDMA systems based on chaotic piecewise-affine Markov maps," *IEEE Trans. Circuits Syst. I*, vol. 47, no. 6, pp. 885–896, June 2000.

[12] G. Setti, G. Mazzini, R. Rovatti, and S. Callegari, "Statistical modeling of discrete-time chaotic processes – basic finite-dimensional tools and applications," *Proc. IEEE*, vol. 90, no. 5, pp. 662–690, May 2002.

[13] D. León, S. Balkir, M. Hoffman, and L. C. Pérez, "Fully programmable, scalable chaos-based PN sequence generation," *Electronics Letters*, vol. 36, no. 16, pp. 1371–1372, Aug. 2000.

[14] T. L. Carroll, "Spread-spectrum sequences from unstable periodic orbits," *IEEE Trans. Circuits Syst. I*, vol. 47, no. 4, pp. 443–447, Apr. 2000.

[15] T. Kohda, "Information sources using chaotic dynamics," *Proc. IEEE*, vol. 90, no. 5, pp. 641–661, May 2002.

[16] I. Hen and N. Merhav, "On the threshold effect in the estimation of chaotic sequences," in *The 22nd Convention of Electrical and Electronics Engineers in Israel*, Dec. 2002, pp. 29–31.

[17] M. J. Mihaljević and J. D. Golić, "A comparison of cryptanalytic principles based on iterative error-correction," in *Advances in Cryptology – EUROCRYPT '91*, vol. 547. Berlin, Germany: Springer-Verlag, 1991, pp. 527–531.

[18] ——, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence," in *Advances in Cryptology – EUROCRYPT '92*, vol. 658. Berlin, Germany: Springer-Verlag, 1993, pp. 124–137.

[19] S. H. Isabelle and G. W. Wornell, "Statistical analysis and spectrum estimation techniques for one-dimensional chaotic signals," *IEEE Trans. Signal Processing*, vol. 45, no. 6, pp. 1495–1506, June 1997.

[20] A. Lasota and M. C. Mackey, *Chaos, Fractals, and Noise*, 2nd ed. New York, NY: Springer-Verlag, 1994.

[21] C. Grebogi, E. Ott, and J. A. Yorke, "Roundoff-induced periodicty and the correlation dimension of chaotic attractors," *Phys. Rev. A*, vol. 38, no. 7, pp. 3688–3692, Oct. 1988.

[22] S. B. Wicker, *Error Control Systems for Digital Communication and Storage.* Upper Saddle River, NJ: Prentice Hall, 1995.

[23] H. L. Royden, *Real Analysis*, 3rd ed. Englewood Cliffs, NJ: Prentice Hall, 1988.

[24] H. C. Papadopoulos and G. W. Wornell, "Maximum-likelihood estimation of a class of chaotic signals," *IEEE Trans. Inform. Theory*, vol. 41, no. 1, pp. 312–317, Jan. 1995.

[25] H. V. Poor and G. W. Wornell, Eds., *Wireless Communications: Signal Processing Perspectives.* Upper Saddle River, NJ: Prentice Hall, 1998.

[26] W. C. Jakes, Ed., *Microwave Mobile Communications.* Piscataway, NJ: IEEE Press, 1994.

[27] W. Feller, *An Introduction to Probability Theory and Its Applications*, 3rd ed. New York, NY: John Wiley & Sons, 1968, vol. 1.

[28] S. L. Zabell, "Alan Turing and the central limit theorem," *Amer. Math. Monthly*, vol. 102, no. 6, pp. 483–494, Jun./Jul. 1995.

[29] A. Abel and W. Schwarz, "Chaos communications – principles, schemes, and system analysis," *Proc. IEEE*, vol. 90, no. 5, pp. 691–710, May 2002.

[30] S. M. Hammel, J. A. Yorke, and C. Grebogi, "Do numerical orbits of chaotic dynamical processes represent true orbits?" *Journal of Complexity*, vol. 3, pp. 137–145, 1987.

[31] S. Verdú, "Minimum probability of error for asynchronous gaussian multiple-access channels," *IEEE Trans. Inform. Theory*, vol. 32, no. 1, pp. 85–96, Jan. 1986.

[32] ——, *Multiuser Detection.* Cambridge, UK: Cambridge University Press, 1998.

[33] L. Risbo, "On the design of tone-free sigma-delta modulators," *IEEE Trans. Circuits Syst. II*, vol. 42, no. 1, pp. 52–55, Jan. 1995.

[34] B. Chen and G. W. Wornell, "Analog error-correcting codes based on chaotic dynamical systems," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 881–890, July 1998.

[35] D. Knuth, *The Art of Computer Programming 2, Seminumerical Algorithms*, 2nd ed. Reading, MA: Addison-Wesley, 1981.

[36] A. A. Tsonis, "Choas and unpredictibility of weather," *Weather*, vol. 44, no. 6, pp. 258–263, June 1989.

[37] T. C. Cover and J. Thomas, *Elements of Information Theory.* New York, NY: John Wiley & Sons, 1991.

[38] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Performance Analysis.* New York, NY: John Wiley & Sons, 2000.