The Use of a Logistic Map for Key Generation

by

Megumi Ando

S.B., Mathematics M.I.T., 2007
S.B., C.S. M.I.T., 2010

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Master of Engineering in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2010

Author .....
Department of Electrical Engineering and Computer Science
August 19, 2010

Certified by .....
Prof. Moe Z. Win
Associate Professor
Thesis Supervisor

Accepted by .....
Dr. Christopher J. Terman
Chairman, Department Committee on Graduate Theses

The Use of a Logistic Map for Key Generation

by

Megumi Ando

Submitted to the Department of Electrical Engineering and Computer Science
on September 1, 2010, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

A key generation scheme is proposed and its performance analyzed. The method, the logistic map scheme (LMS), is applicable for use on wireless networks because it does not require devices to engage in computationally intensive algorithms. In addition, the method is shown to achieve reliability from the perspective of the communication agents, as well as unpredictability and randomness from the perspective of an eavesdropper. Lastly, the performance of the LMS is compared against that of an existing technique. Results from a comparative analysis indicate that the proposed method generally yields a greater number of reliable, unpredictable, and random key bits than the existing technique under the same conditions.

Thesis Supervisor: Prof. Moe Z. Win
Title: Associate Professor

Acknowledgments

Foremost, I would like to acknowledge my research supervisor, Prof. Moe Win; I would not have been able to complete my masters research without his support and guidance. Prof. Win provided me with a solid foundation on communication theories. In addition, I have learned many necessary skills for becoming a future researcher, including how to formulate crisp mathematical definitions and how to write technical papers.

I would also like to thank my academic advisor, Prof. Albert Meyer, for his mentorship over the past five years. Under Prof. Meyer's tutelage, I have learned a great deal about mathematics and computer science as well as about life in general. I am particularly indebted to Prof. Meyer for offering me three separate TA-ships, which funded my masters research.

Special thanks are to Dr. Wesley (Wes) Gifford and Dr. Pedro Pinto: Wes for coaching me through the details of the system model, and Pedro for teaching me the various flavors of information-theoretic secrecy. Additionally, I would like to acknowledge the past and current members of the Wireless Communications Research Group for their helpful comments throughout my masters research; they are: Dr. Jowoon Chong, Ulric Ferner, Dr. Yohan Kim, Kentaro Kudo, William Wei-Liang Li, Dr. Santiago Mazuelas, Yuan Shen, Watcharapan (Ae) Suwansantisuk, and Dr. Henk Wymeersch.

I owe Dr. Jim Bales from the Edgerton Center very special thanks for the several conversations we had on chaos-based, physical-layer security systems. The idea for my research germinated over lively conversation in the Dome Cafe and two cups of coffee (cream, no sugar).

I would like to thank everyone at the MIT's Department of Computer Science and Electrical Engineering, especially Dr. Christopher Terman, Prof. Terry Orlando, and Anne Hunter, for their advice and for prodding me to complete my thesis in a timely fashion.

Lastly, I would like to acknowledge my family – my parents (Prof. Teiichi Ando and Sumiko Ando), my sister (Dr. Nozomi Ando), and my brother-in-law (Dr. Buz Barstow) – for their love and support. It is to them that I dedicate my thesis.

"Uh wugga wuh. Uh wugga wuh. Uh wugga wugga wugga. I wugga wuh uh wugga wuh Uh wugga wugga wugga." – Prof. Richard Feynman

Contents

List of Abbreviations

AWGN	$\triangleq$	additive white Gaussian noise
CDF	$\triangleq$	cumulative density function
LMS	$\triangleq$	logistic scheme
MPSS	$\triangleq$	modified per-sample scheme
NP	$\triangleq$	non-deterministic polynomial-time
P	$\triangleq$	(deterministic) polynomial-time
PDF	$\triangleq$	probability density function
PSS	$\triangleq$	per-sample scheme
UBW	$\triangleq$	ultra-wide bandwidth
UPSS	$\triangleq$	unmodified per-sample scheme

List of Notations

$\oplus$	$\triangleq$	signal convolution
$+$	$\triangleq$	signal addition
$\overrightarrow{\epsilon}$	$\triangleq$	allowable error vector
ϵ_1	$\triangleq$	allowable error in reliability
ϵ_2	$\triangleq$	allowable error in unpredictability
ϵ_3	$\triangleq$	allowable error in randomness
$\mathbb{E}\{X\}$	$\triangleq$	expected value of random variable, X
$f(x)$	$\triangleq$	$\frac{1}{\pi\sqrt{x(1-x)}}$
$h_{\mathrm{AB}}(t)$	$\triangleq$	channel impulse response from Alice to Bob
$h_{\mathrm{AE}}(t)$	$\triangleq$	channel impulse response from Alice to Eve
$h_{\mathrm{BA}}(t)$	$\triangleq$	channel impulse response from Bob to Alice
$h_{\mathrm{BE}}(t)$	$\triangleq$	channel impulse response from Bob to Eve
$g(x)$	$\triangleq$	$\frac{2}{\pi}\arcsin\left(x^{\frac{1}{2}}\right)$
$g^{-1}(x)$	$\triangleq$	$\sin\left(\frac{\pi x}{2}\right)^2$
$H(X)$	$\triangleq$	entropy of random variable, X
$I(X;Y)$	$\triangleq$	mutual information between random variables, X and Y
$\mathcal{K}$	$\triangleq$	keyspace
K_{A}	$\triangleq$	Alice's calculated key using the LMS, i.e., $q_\ell(\ell^N(X_{\mathrm{A}}))$
K_{B}	$\triangleq$	Bob's calculated key using the LMS, i.e., $q_\ell(\ell^N(X_{\mathrm{B}}))$
K_{E}	$\triangleq$	Eve's estimation of Alice's key, K_{A}, i.e., $q_\ell(\ell^N(X_{\mathrm{E}}))$
$K_{(s,\mathrm{A})}$	$\triangleq$	Alice's calculated key using the MPSS, i.e., $q_s(s^N(X_{\mathrm{A}}))$
$K_{(s,\mathrm{B})}$	$\triangleq$	Bob's calculated key using the MPSS, i.e., $q_s(s^N(X_{\mathrm{B}}))$
$K_{(s,\mathrm{E})}$	$\triangleq$	Eve's estimation of Alice's key, $K_{(s,\mathrm{A})}$, i.e., $q_s(s^N(X_{\mathrm{E}}))$
L	$\triangleq$	key length per sample

$\ell(x) \triangleq 4x(1-x)$

$N \triangleq$ number of iterations

$n_{\mathrm{A}}(t) \triangleq$ Alice's observational noise

$n_{\mathrm{B}}(t) \triangleq$ Bob's observational noise

$n_{\mathrm{E}_1}(t) \triangleq$ Eve's observational noise during Alice's broadcast

$n_{\mathrm{E}_2}(t) \triangleq$ Eve's observational noise during Bob's broadcast

$\mathcal{N}(\mu, \sigma^2) \triangleq$ Gaussian distribution with mean, μ, and variance, σ^2

$\mathcal{N}_{[0,1]}(\mu, \sigma^2) \triangleq$ truncated Gaussian distribution with mean, μ, and variance, σ^2

$\mathbb{P}\{\mathcal{A}\} \triangleq$ probability of event $\mathcal{A}$

$p(t) \triangleq$ transmit signal

$$q(y, L) \triangleq \begin{cases} \left\lceil \frac{2^{L+1} \arcsin(\sqrt{y})}{\pi} \right\rceil, & y \in (0, 1] \\ 1, & y = 0 \end{cases}$$

$q_s(y, L) \triangleq \lceil 2^L y \rceil$

$r_{\mathrm{A}}(t) \triangleq$ Alice's receive waveform

$r_{\mathrm{B}}(t) \triangleq$ Bob's receive waveform

$r_{\mathrm{E}_1}(t) \triangleq$ Eve's receive waveform from Alice's broadcast

$r_{\mathrm{E}_2}(t) \triangleq$ Eve's receive waveform from Bob's broadcast

$\sigma_{\mathrm{B}} \triangleq$ standard deviation of noise in Bob's sample

$\sigma_{\mathrm{E}} \triangleq$ standard deviation of estimation error in Eve's sample

$$s(x) \triangleq \begin{cases} 2x, & 0 \leq x \leq 0.5 \\ 2x - 1, & 0.5 < x \leq 1 \end{cases}$$

$X \sim \triangleq$ distribution of random variable, X

$x_{\mathrm{A}} \triangleq$ Alice's sample value (real)

$x_{\mathrm{B}} \triangleq$ Bob's sample value (real)

$x_{\mathrm{E}} \triangleq$ Eve's sample value (real)

$\overrightarrow{x_{\mathrm{A}}} \triangleq$ vector of Alice's sample values (real)

$\overrightarrow{x_{\mathrm{B}}} \triangleq$ vector of Bob's sample values (real)

$\overrightarrow{x_{\mathrm{E}}} \triangleq$ vector of Eve's sample values (real)

$X_{\mathrm{A}} \triangleq$ Alice's sample modeled as a random variable

$X_{\mathrm{B}} \triangleq$ Bob's sample modeled as a random variable

$X_{\mathrm{E}} \triangleq$ Eve's sample modeled as a random variable

Chapter 1

Introduction

In this following chapter, we motivate the need for alternative methods for achieving covert communications. Secure wireless networks are essential for many military, commercial, and public service applications (e.g., air transportation systems, mobile wireless networks, and medical sensor networks). Current security systems (i.e., public-key schemes, such as RSA) rely on unproven computational complexity conjectures. Moreover, they are not appropriate for some applications. In particular, they are too computationally intensive to implement on ad-hoc networks.

1.1 Motivation

The security of known public-key systems relies on the intractability of computationally equivalent problems (e.g., the integer factorization problem and the quadratic residuosity problem). One concern is that it is currently unknown whether these computational problems belong to the class of NP-complete problems (i.e., generally considered intractable) or in P (i.e., generally considered tractable). Another concern is that the equivalence of the computational problems for public-key systems implies that if any of these is proven to be tractable, then all others are necessarily tractable as well. Finally, even if it is proven that these computational problems are NP-complete, the validity of computational security as a whole as well as the existence of pseudo-randomness depend on the unproven conjecture that the computational complexity classes, P and NP, are unequal. It is, therefore, prudent to find an alternative or complementary method whose security does not depend on the hardness of computational problems.

Moreover, even if the validity of computational methods can be assumed, the handshaking protocol in current public-key schemes are too computationally and energy intensive for use on ad-hoc networks in many military, commercial, and public-service applications. For example, tactical networks typically consist of sensor devices with low computational capabilities and battery life; meanwhile, these devices ideally engage in covert communications. As a second example, implantable medical sensors are not rechargeable and meant to last five to seven years without replacement [1–3]. Yet personal information from these devices should be kept private and encrypted.

1.2 Background

Researchers have approached the problem of securing networks from two basic vantage points: a computational complexity perspective, which relies on the intractability of computational problems [4, 5], and an information-theoretic perspective, which is a natural extension of Shannon's communication theories [6–10]. Historically, researchers in the field of cryptography have focused almost exclusively on computational approaches. However, in recent years more researchers are revisiting information-theoretic methods in part because they offer a higher level of security. Computational security relies on the eavesdropper's limitations as well as the intractability of computational problems. In contrast, information-theoretic security does not rely on either of the above assumptions. The above reasons motivate our interest in designing a communication system that is *operationally* informationally-secure.

Ultra-wide bandwidth (UWB) channels offer an alternative approach to generating keys in wireless networks. The idea is to design a computationally lightweight private-key system by utilizing the intrinsic properties of wireless communication channels: namely, the reciprocity of a channel response and the uncertainty of channel responses over a static environment found in the channel responses. The first property facilitates efficient key agreement, while the second property provides unpredictability. Since physical-layer systems can bypass a resource intensive handshaking protocol, it also meets the efficiency criteria of wireless networks.

UWB signals are an ideal candidate for this kind of key-generating systems, because they allow for fine time delay resolution, thus facilitating the precise estimation of the of

multipath delays [11–23]. Compared with narrow band signals, UWB signals can convey more information about the environment, and so the communication agents are able to agree on a longer shared key. The idea for using UWB signals for key generation was proposed by [24]; three schemes, the per-sample, block-coded, and trellis-coded schemes, have been designed for physical-layer systems based on the theory of forward error correction. These schemes all work in the same basic way, as described below.

In the first round of communication, Alice and Bob (i.e., the communicating agents) send each other the same transmit signal, and each agent samples and decorrelates his or her respective receive waveforms. Two samples (or blocks of samples) are defined to be equivalent if they are the same up to some observational noise. Thus, the space of samples / blocks of samples can be partitioned into cosets, where each coset consists only of equivalent samples / blocks of samples. It is assumed that such a coset assignment is available to all agents operating in the network. In the second round of communication, Bob publicly reveals the cosets corresponding to his samples; and Alice is able to infer Bob's complete sequence of samples since Alice and Bob's receive waveforms are identical up to observational noise by the reciprocity of their shared channel.

The reliability (i.e., the probability of key agreement) for the per-sample scheme, the block-code, and the trellis-code schemes were tested via Monte Carlo simulations [24]. The 802.15.3a UWB channel model proposed in [25] was utilized; and a raised cosine pulse with 4 GHz bandwidth and 7 GHz center frequency was used as the transmit signal. Of the three methods, the per-sample scheme yielded the smallest error probability for a theoretical shared bit per sample according to the published results. *In this thesis, an alternative key generation scheme is proposed, and its performance is compared against that of a modification to the best performing scheme, the per-sample scheme.*

1.3 Road Map of Thesis

The remaining chapters are organized as follows. In ch. 2, we formally define our problem statement and justify our mathematical models for the communication channels as well as the agents' observables. In chs. 3 and 4, we present our key generation scheme as well as the performance analysis of the scheme. In ch. 5, we present a modification to an existing scheme, the per-sample scheme, proposed in [24] and, likewise, present its performance

analysis. Finally, in chs. 6 and 7, we present the results from our analyses and deliver our conclusion and recommendations for future work.

Chapter 2

System Model

In order to explain design choices, it is necessary to first lay down the system model. In this chapter, the system model for the proposed scheme is described; while the proposed key generation scheme is detailed in ch. 3.

We begin the discussion with the problem statement: Alice and Bob are two agents in a UWB wireless network who wish to send each other messages, such that the contents of their messages remain a secret to all other observers within range. Eve is a passive eavesdropper whose intent is to discover the contents of Alice and Bob's covert communications. The objective is enabling such secure communications. Specifically, the problem is in designing a scheme, which allows Alice and Bob to agree on a random key, such that Eve cannot determine the key. This key will then be used in a private-key cryptosystem to allow for proper encryption and decryption of messages.

2.1 Reciprocity

It will be assumed that the given environment exhibits the following two properties: reciprocity as well as uncertainty of the communication channels. These properties are described below.

A given communication channel exhibits *reciprocity* if the channel response in one direction is identical to the channel response in the opposite direction up to some observational noise. In the proposed scheme, the channel between Alice and Bob is assumed to be reciprocal. That is, the channel response, h_{AB}, from Alice to Bob is assumed to be the same as the channel response, h_{BA}, from Bob to Alice up to some observational noise.

A channel response is *uncertain* if any eavesdropper located some distance away from the receive antenna cannot determine the channel response. We assume that Alice and Bob are operating in a UWB channel environment; and, furthermore, the eavesdropper cannot precisely model the environment. Thus, in addition to reciprocity, uncertainty of the channels over a fixed, time-invariant environment is assumed.

Given the above assumptions, the general strategy for the key agreement scheme is as follows: In the handshaking phase, Alice broadcasts a signal, $p(t)$. The signal Bob receives can be modeled as $r_{\mathrm{B}}(t) = p(t) \otimes h_{\mathrm{AB}}(t) + n_{\mathrm{B}}(t)$, where h_{AB} denotes Alice and Bob's shared channel, $n_{\mathrm{B}}(t)$ denotes Bob's observational noise, $\otimes$ denotes signal convolution, and $+$ denotes signal addition. Then Bob broadcasts the same transmit signal, $p(t)$; while Alice receives $r_{\mathrm{A}}(t) = p(t) \otimes h_{\mathrm{AB}}(t) + n_{\mathrm{A}}(t)$, where $n_{\mathrm{A}}(t)$ denotes Alice's observational noise.[1] The signal received by Eve due to Alice and Bob's separate transmissions during the handshaking phase can be modeled as $r_{\mathrm{E}_1}(t) = p(t) \otimes h_{\mathrm{AE}}(t) + n_{\mathrm{E}_1}(t)$ and $r_{\mathrm{E}_2}(t) = p(t) \otimes h_{\mathrm{BE}}(t) + n_{\mathrm{E}_2}(t)$, respectively, where $h_{\mathrm{AE}}(t)$ denotes Alice and Eve's shared channel, h_{BE} denotes Bob and Eve's shared channel, and $n_{\mathrm{E}_1}(t)$ and $n_{\mathrm{E}_2}(t)$ denote Eve's observational noises. A schematic of the handshaking phase is given in fig. 2-1.

By the reciprocity assumption, $r_{\mathrm{A}}(t)$ and $r_{\mathrm{B}}(t)$ are identical up to some observational noise; and, by the uncertainty assumption, Eve is unable to determine an accurate enough approximation of either $r_{\mathrm{A}}(t)$ or $r_{\mathrm{B}}(t)$. The reciprocity assumption, therefore, explains how two agents at opposite ends of a channel may be able to communicate encrypted messages to each other; while, the uncertainty assumption explains how a third, unauthorized agent may be unable to decrypt these communications.

2.2 Channel and Sample Models

Because observational noise is composed mainly of thermal noise, it is usually modeled as white noise with constant spectral density. Such a channel model is a widely accepted standard and is referred to by the communications community as *additive white Gaussian noise (AWGN)*. In keeping with the AWGN model, all observational noises are modeled as white noise in the context of this thesis.

[1] It is assumed that the handshaking phase occurs within a coherence time of Alice and Bob's shared channel (i.e., an interval of time in which the main channel is time-invariant); and, therefore, the objective is to produce some shared key bits in every coherence time during which Alice and Bob wish to communicate securely.

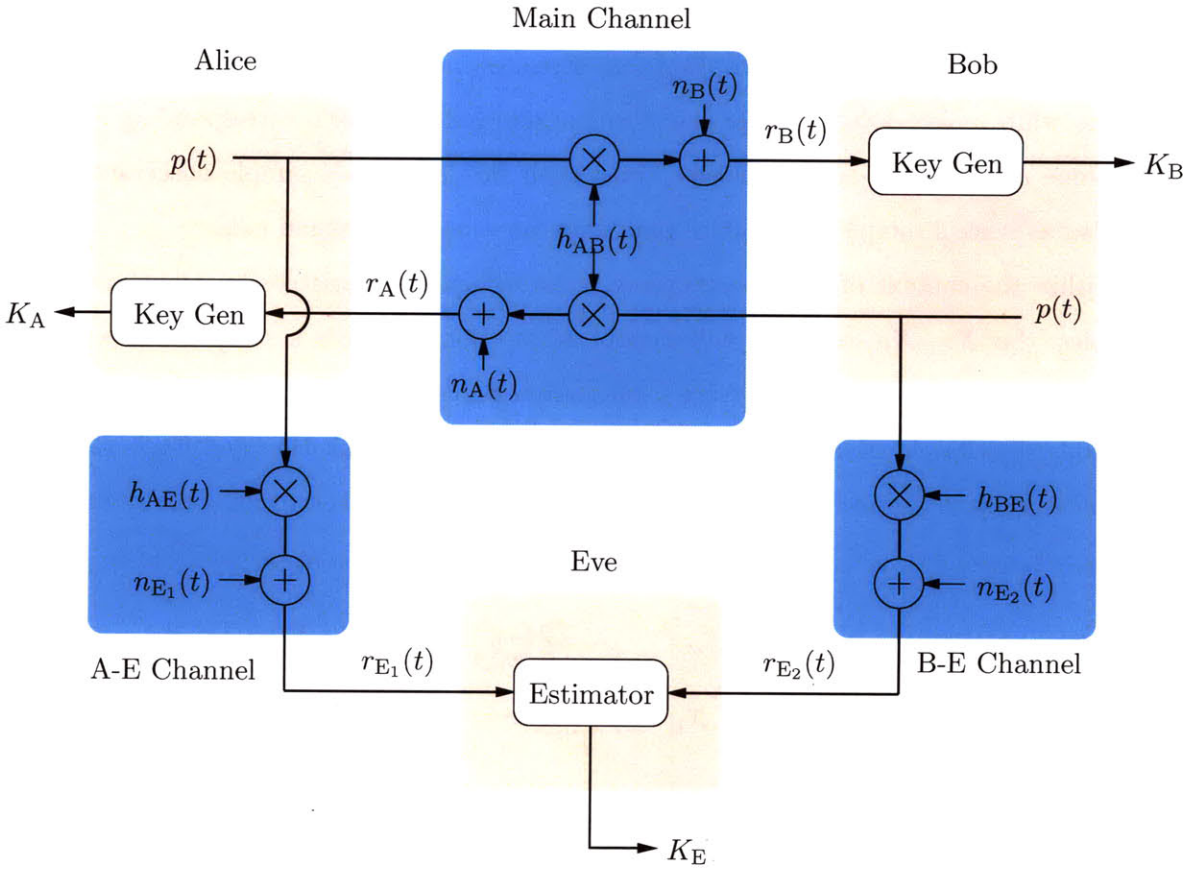


Figure 2-1: A schematic drawing of the handshaking phase for the logistic map scheme.

In the key-generating phase of the proposed scheme, Alice and Bob sample their respective receive waveforms, and then decorrelate and normalize their respective samples. Let $\overrightarrow{x_A} = [x_{(A,1)}, x_{(A,2)}, \ldots, x_{(A,n)}]$ and $\overrightarrow{x_B} = [x_{(B,1)}, x_{(B,2)}, \ldots, x_{(B,n)}]$ denote decorrelated and normalized samples from Alice and Bob's received waveforms, respectively; and let $\overrightarrow{x_E} = [x_{(E,1)}, x_{(E,2)}, \ldots, x_{(E,n)}]$ denote Eve's best estimation of Alice's samples.

Let the triple, $[x_A, x_B, x_E]$, denote an arbitrarily chosen $x_{(A,i)}$ and corresponding samples, $x_{(B,i)}$ and $x_{(E,i)}$. The analysis presented in this thesis will be conducted on this triple; that is, the reliability of the proposed scheme as well as the unpredictability and randomness of the shared key will be studied on a per sample basis. We choose to work with a per sample analysis due to its better readability. Moreover, because the samples are assumed to be decorrelated, results from the per sample analysis are easily extended to include cases where $\overrightarrow{x_A}$, $\overrightarrow{x_B}$, and $\overrightarrow{x_E}$ are of length greater than one. (A discussion on how to extend the results from ch. 4 is given in sec. 6.1.)

Because the waveforms received by Alice and Bob are identical up to some white noise,

Bob's sample is modeled as Alice's corresponding sample plus some zero-mean, Gaussian noise. Under the reasonable assumption that Eve's estimation of Alice's receive waveform is some white noise, Eve's sample can also be modeled as Alice's corresponding sample plus some zero-mean, Gaussian noise. Thus, both Bob and Eve's sample observables are modeled as Alice's sample observables plus some zero-mean, Gaussian noise.

Within the context of this thesis, we will use upper case variables to denote random variables. So X_{A}, X_{B}, and X_{E} will denote Alice, Bob, and Eve's samples modeled as random variables, respectively. Alice's random variable sample, X_{A}, is assumed to be uniformly distributed over the interval, $[0, 1]$; and, given $X_{\mathrm{A}} = \xi$, Bob and Eve's random variable samples, X_{B} and X_{E}, are normally distributed with ξ as their mean. So, conditioned on $X_{\mathrm{A}} = \xi$,

$$X_{\mathrm{B}} = \mathcal{N}_{[0,1]}\left(\xi, \sigma_{\mathrm{B}}^2\right)$$
$$X_{\mathrm{E}} = \mathcal{N}_{[0,1]}\left(\xi, \sigma_{\mathrm{E}}^2\right)$$

where $\mathcal{N}_{[0,1]}(\mu, \sigma^2)$ denotes the normalized Gaussian distribution with mean, μ, and standard deviation, σ, truncated at 0 and 1.[2]

[2]Note that, while it is standard practice to model noise as a Gaussian distribution (partially for tractability), the methods presented here will work for any analytic function used to model the noise distribution.

Chapter 3

Logistic Map Scheme

The logistic map scheme is a key generation scheme whose unpredictability is guaranteed by properties of a logistic map.[1] The main contributions of the research described in this thesis are the design and performance analysis of the logistic map scheme and, to a lesser degree, a modification to an existing scheme (the per-sample scheme proposed in [24]) and its performance analysis.

In this chapter, we present the logistic map scheme. A detailed analysis of its reliability, unpredictability, and randomness are presented in the next chapter.

3.1 Scheme

The logistic map scheme (LMS) is described in two parts: the handshaking phase and the key-generating phase.

1. *In the handshaking phase:* Alice and Bob send each other the same transmit signal. A schematic of the handshaking phase is given in fig. 2-1.

   (a) Alice broadcasts a signal, $p(t)$. The signal Bob receives can be modeled as $r_{\mathrm{B}}(t) = p(t) \otimes h_{\mathrm{AB}}(t) + n_{\mathrm{B}}(t)$.

   (b) Then Bob broadcasts the same transmit signal, $p(t)$; while Alice receives $r_{\mathrm{A}}(t) = p(t) \otimes h_{\mathrm{AB}}(t) + n_{\mathrm{A}}(t)$.

[1] A *logistic map* is the result of several iterations of a quadratic transformation of the form

$$cx(1-x)$$

where c is some constant. The logistic map for when $c = 4$ is a well-known chaotic iterator [26].

2. *In the key-generating phase:* Alice and Bob each extract a key from his or her respective receive waveform. Each agent first generates decorrelated, normalized samples from his or her respective receive waveform and then computes a key from the amplitudes of these samples.[2] A flowchart of the key-generating phase is given in fig. 3.1.

   (a) For each normalized sample, x, the agent first computes $y = \ell^N(x)$, where $\ell : [0,1] \to [0,1]$ is a well-known chaotic iterator [26] defined as:

   $$\ell(x) = 4x(1-x)$$

   $\ell^N(x)$ denotes the N-times composition function of $\ell(x)$, and an appropriate N is determined by the statistics of Alice and Bob's observational noise as well as Eve's estimation error.[3]

   (b) For each transformed sample, y, the agent then computes $q : [0,1] \times \mathbb{N} \to \{1, 2, \ldots, 2^L\}$ defined as:

   $$q(y, L) = \begin{cases} \left\lceil \frac{2^{L+1} \arcsin(\sqrt{y})}{\pi} \right\rceil, & y \in (0,1] \\ 1, & y = 0 \end{cases}$$

   where L denotes the number of binary key bits per sample. Note that the outputs of $q(\cdot,\cdot)$ are discrete. The quantized values for a sequence of y's are then concatenated sequentially to produce the final key.

It will be assumed that all agents operating in the network, including Eve, know the N- and L-values for the samples.

[2]The preprocessing techniques depend highly on the bandwidth of the channel, and a full discussion on the design and implementation of these techniques is outside the scope of this thesis. As an example, UWB channel impulse responses can be modeled as multipath components whose delays and amplitudes are Poisson and Rayleigh distributed, respectively. In such instances, the time delays of the multipath components can be located by applying a linear predictive coder to determine the samples with highest signal to noise ratio. Standard signal processing techniques then can be applied to reduce the time dependencies of the amplitudes at these time delays.

[3]In order to be stored and computed digitally, x is pre-quantized in a practical system. However, so long as x is represented with on average $(L + 2^N)$-bits of precision, the analysis made in ch. 4 remains valid since the Lyapunov exponent (i.e., the growth rate of infinitesimally small differences in initial conditions) for $\ell(x)$ is 2.

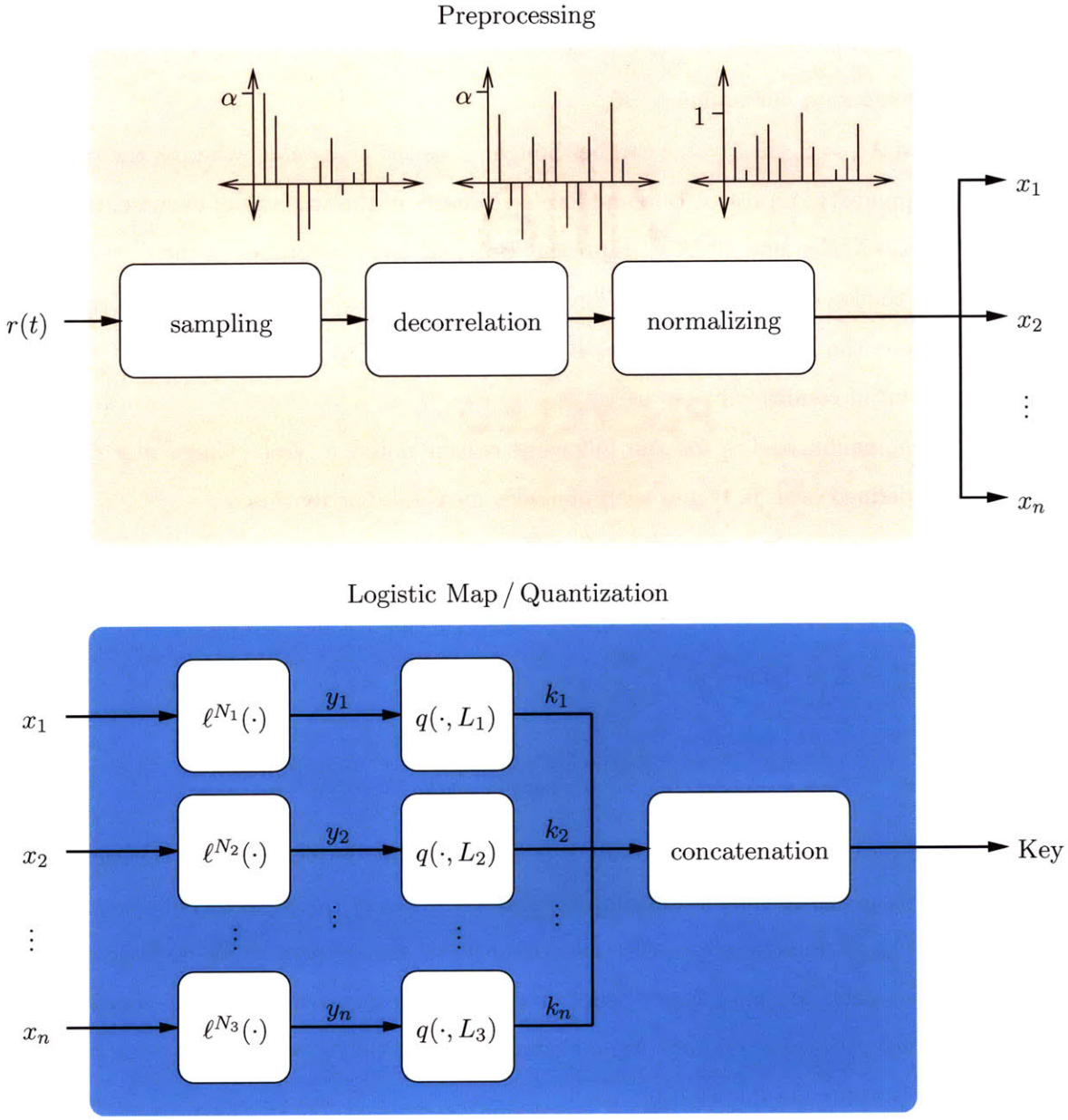


Figure 3-1: A flowchart of the key-generating phase for the logistic map scheme.

3.2 Rationale

In this section, we provide some insight into why the LMS may be a scheme that provides unpredictability and randomness. Let Alice's calculated key segment be $K_{\mathrm{A}} = q(\ell^N(X_{\mathrm{A}}), L)$; and let Bob's key be $K_{\mathrm{B}} = q(\ell^N(X_{\mathrm{B}}), L)$. Conditioned on $K_{\mathrm{A}} = K_{\mathrm{B}} = K$, the shared key segment, K, is *unpredictable* if Eve's observables, $Z = q(\ell^N(X_{\mathrm{E}}), L)$, do not contain any statistical information pertaining to K.

For a fixed $X_{\mathrm{A}} = \xi$, the ξ-value can be thought of as the *true value*, whereas the random variables, X_{B} and X_{E}, represent Bob and Eve's estimates of the true value; likewise, the random variables, $\ell^N(X_{\mathrm{B}})$ and $\ell^N(X_{\mathrm{E}})$, represent Bob and Eve's estimates of the $\ell^N(\xi)$-value. In step (a) of the key-generating phase, any statistical information that Eve might otherwise have had about the final sample value, $\ell^N(\xi)$, is destroyed by sufficiently amplifying the noise in the initial conditions.

This phenomenon occurs for the following reason noted in [26]: Given any random variable, X, defined over $[0, 1]$ and with non-zero measure distribution, d,

$$\lim_{N \to \infty} \ell^N(x) \sim f(x)$$

where $f : [0, 1] \to \mathbb{R}$ is defined as

$$f(x) = \frac{1}{\pi\sqrt{x(1-x)}}$$

For example, by utilizing parameters for the sample model derived from a realistic UWB channel environment, it can be determined that Eve's *belief* (i.e., the distribution of her estimate, $\ell^N(X_{\mathrm{E}})$) converges to a distribution close to $f(\cdot)$ after a small number of iterations (see sec. 6.1). Because Eve's belief eventually transforms to the same distribution irrespective of K, it cannot contain any information about the agreed key segment, K; and, therefore, K is unpredictable as desired.

Conditioned on $K_{\mathrm{A}} = K_{\mathrm{B}} = K$, the shared key segment, K, is *uniformly random* if the probability that $K = k$ is the same for any $k \in \mathcal{K}$, where $\mathcal{K}$ denotes the keyspace. In step (b) of the key-generating phase, uniformity in K occurs because a sample from a random variable, $X \sim f(x)$, quantizes to an arbitrarily chosen bin with uniform probability, and because the distribution of K is sufficiently close to $f(x)$.

Chapter 4

Performance Analysis

In this chapter, we define performance metrics, which we then use to formally analyze our proposed scheme. Interpretations and further analysis of the equations derived in this chapter are given in sec. 6.1.

4.1 Performance Metrics

We begin the discussion with the definitions for the performance metrics:

Definition 4.1.1 *The* reliability *of the key agreement scheme is defined as*

$$\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}}\}$$

where $\mathbb{P}\{\mathcal{A}\}$ *denotes the probability of event,* $\mathcal{A}$*; and* K_{A} *and* K_{B} *are Alice and Bob's keys, respectively. Thus,* unreliability *is defined as* $1 - \mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}}\}$.

Definition 4.1.2 *When* $K_{\mathrm{A}} = K_{\mathrm{B}} = K$*, the* predictability *of the shared key is defined as*

$$\frac{I(K;Z)}{\log(|\mathcal{K}|)}$$

where I *denotes mutual information; and* K *is the shared key,* Z *is Eve's observables,*[1] *and* $\mathcal{K}$ *is the keyspace. Thus,* unpredictability *is defined as* $1 - \frac{I(K;Z)}{\log(|\mathcal{K}|)}$.

[1] In other words, Z is what is observed by Eve during the handshaking phase of the key agreement protocol.

Definition 4.1.3 *When $K_A = K_B = K$, the* randomness *of the shared key is defined as*

$$\frac{H(K)}{\log(|\mathcal{K}|)}$$

where H denotes entropy. Thus, unrandomness *is defined as* $1 - \frac{H(K)}{\log(|\mathcal{K}|)}$.

The metrics given in defs. 4.1.1, 4.1.2, and 4.1.3, measure the reliability, unpredictability, and randomness of a key-generating system for the following reasons. High reliability is equivalent to high probability of key agreement. High unpredictability is equivalent to low mutual information. High randomness is equivalent to high entropy.[2]

We claim (and prove later in sec. 6.1) that our key generation scheme provides security in the sense that non-zero, secret key lengths are achievable for some positive key length L and for some reasonably small, allowable errors in reliability, unpredictability, and randomness.

4.2 Reliability

To determine the probability of key agreement (as well as the mutual information between the shared key and Eve's observables, and the entropy of the shared key), we need a way of tracking the underlying distribution of $\ell^N(X_B)$ given $X_A = \xi$, where N is an arbitrary number of iterations of the chaotic map. Since $\ell : [0,1] \to [0,1]$ defined as

$$\ell(x) = 4x(1-x)$$

is monotonic over each of the disjoint intervals $\left[0, \frac{1}{2}\right]$ and $\left(\frac{1}{2}, 1\right]$, the usual rule for monotonic transformations on cumulative density functions (CDFs) can be applied in a piece-wise fashion. Thus, the formula for the CDF at the N^{th} iteration is as follows: Let X be a

[2]We chose to work with these definitions, because they relate to the standard definition of secret key rate, $\mathcal{R}(X;Y||Z)$, given in [7, 24]. By considering the scheme's handshaking phase to occur within a coherence time, the problem statement broadens to include time-variant systems. Thus generalized, the definition can be extended to include maximum achievable secret key rates with allowable errors. For infinitesimally small errors, the extended definition matches that of the achievable secret key rate.

random variable defined over $[0,1]$. The CDF of $\ell^N(X)$ at x is

$$F_{\ell^N(X)}(x) = \sum_{i=1}^{2^{N-1}} \left[F_X\left(g^{-1}\left(\frac{i-1}{2^{N-1}} + \frac{g(x)}{2^N}\right)\right) - F_X\left(g^{-1}\left(\frac{i-1}{2^{N-1}}\right)\right) \right.$$
$$\left. + F_X\left(g^{-1}\left(\frac{i}{2^{N-1}} + \frac{g(x)}{2^N}\right)\right) - F_X\left(g^{-1}\left(\frac{i}{2^{N-1}}\right)\right)\right], \qquad 0 \le x \le 1$$

where $F_X(\cdot)$ is the CDF of the original random variable, X; $g(x) = \frac{2}{\pi}\arcsin\left(x^{\frac{1}{2}}\right)$; and $g^{-1}(x) = \sin\left(\frac{\pi x}{2}\right)^2$. (A detailed derivation of the transformation is given in appendix A.)

The probability of key agreement is the probability that $\ell^N(X_\mathrm{A})$ and $\ell^N(X_\mathrm{B})$ quantize to the same bin. It is the probability that $q\left(\ell^N(X_\mathrm{A}), L\right) = q\left(\ell^N(X_\mathrm{B}), L\right)$, where L denotes the per sample key length. For any $k \in \mathcal{K}$, the probability that $K_\mathrm{B} = k$ is given by

$$\begin{aligned}
\mathbb{P}\{K_\mathrm{B} = k\} &\overset{(a)}{=} \mathbb{E}_{X_\mathrm{A}}\{\mathbb{P}\{K_\mathrm{B} = k | X_\mathrm{A}\}\} \\
&\overset{(b)}{=} \int_0^1 \mathbb{P}\{K_\mathrm{B} = k | X_\mathrm{A} = \xi\}\, f_{X_\mathrm{A}}(\xi) d\xi \\
&\overset{(c)}{=} \int_0^1 \mathbb{P}\{K_\mathrm{B} = k | X_\mathrm{A} = \xi\}\, d\xi
\end{aligned} \tag{4.1}$$

Here, (a) follows from the law of total probability; (b) follows from the definition of expectation of a continuous random variable; and (c) follows from the uniformity of the random variable, X_A.

Conditioned on X_A, the probability that $\ell^N(x_\mathrm{B})$ falls into the k^{th} quantization bin can be found by subtracting the CDF of $\ell^N(X_\mathrm{B})$ at the lower endpoint of the k^{th} bin from the CDF of $\ell^N(X_\mathrm{B})$ at the upper endpoint of the k^{th} bin. Thus,

$$\mathbb{P}\{K_\mathrm{B} = k | X_\mathrm{A}\} = F_{\ell^N(X_\mathrm{B})}\left(g^{-1}\left(\frac{k-1}{2^L}\right)\middle| X_\mathrm{A}\right) - F_{\ell^N(X_\mathrm{B})}\left(g^{-1}\left(\frac{k}{2^L}\right)\middle| X_\mathrm{A}\right) \tag{4.2}$$

Now fix $X_\mathrm{A} = \xi$, and let k be the quantization of $\ell^N(\xi)$. Then, the probability that $\ell^N(X_\mathrm{B})$ falls in the same quantization bin as $\ell^N(X_\mathrm{A})$ precisely matches the expression above; and so the probability of key agreement is given by

$$\begin{aligned}
\mathbb{P}\{K_\mathrm{A} = K_\mathrm{B}\} = \int_0^1 \left[F_{\ell^N(X_\mathrm{B})}\left(g^{-1}\left(\frac{q(\ell^N(\xi), L) - 1}{2^L}\right)\middle| X_\mathrm{A} = \xi\right) - \right. \\
\left. F_{\ell^N(X_\mathrm{B})}\left(g^{-1}\left(\frac{q(\ell^N(\xi), L)}{2^L}\right)\middle| X_\mathrm{A} = \xi\right)\right] d\xi
\end{aligned} \tag{4.3}$$

Fig. 4-1 is drawn from the analytical formula given in (4.3) and plots the *un*reliability for $L = 2$. Note that as N increases, the reliability decreases and settles to $\frac{1}{2^L}$; this is expected since the chaotic iterator has amplified small deviations in initial conditions (the noise in Bob's received transmission) with each iteration. (Plots of the numerical results from this chapter are presented at the end of appendix A along with the corresponding plots of the competing scheme that is introduced in ch. 5.)

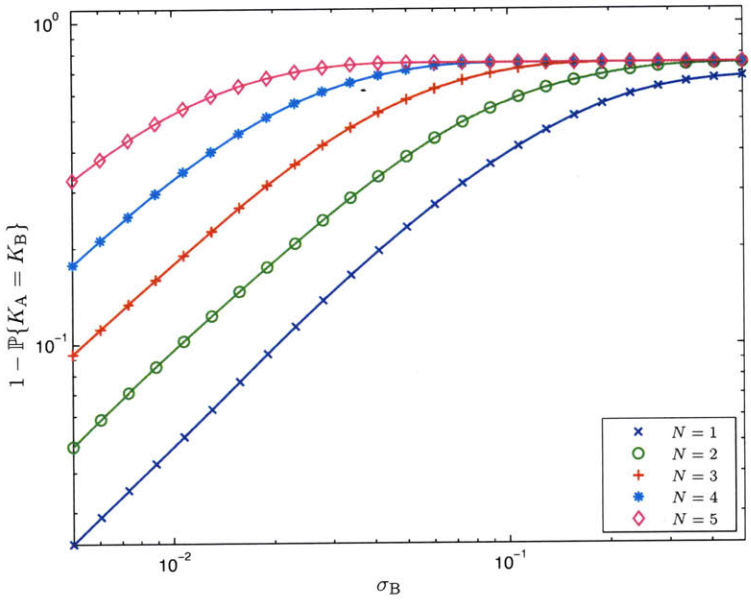


Figure 4-1: *Un*reliability plotted against σ_B for $L = 2$ and various N.

4.3 Unpredictability

By definition, unpredictability, $\frac{I(K;K_E|K_A=K_B)}{\log(|\mathcal{K}|)}$, is given by:

$$\frac{I(K;K_E|K_A = K_B)}{\log(|\mathcal{K}|)} = \frac{1}{\log(|\mathcal{K}|)} \cdot \sum_{k\in\mathcal{K}} \sum_{k_E\in\mathcal{K}} p(k,k_E) \log\left(\frac{p(k,k_E)}{p_1(k_E)p_2(k)}\right) \tag{4.4}$$

where $p(k,k_E) = \mathbb{P}\{K = k \text{ and } K_E = k_E|K_A = K_B\}$, $p_1(k_E) = \mathbb{P}\{K_E = k_E|K_A = K_B\}$, and $p_2(k) = \mathbb{P}\{K = k|K_A = K_B\}$.

To derive the mutual information, $I(K, K_E|K_A = K_B)$, we first determine the joint and marginal probabilities associated with the shared key, K, and Eve's estimate, K_E. That is, we derive formulas for: (1) the probability that $K_E = k_E$ conditioned on $K_A = K_B$, (2) the

probability that $K = k$ conditioned on $K_A = K_B$, and (3) the joint probability that $K = k$, and $K_E = k_E$ conditioned on $K_A = K_B$. The formulas for these probabilities are presented in the above order.

The first probability is

$$\boxed{p_1(k_E) = \frac{1}{\mathbb{P}\{K_A = K_B\}} \int_0^1 \mathbb{P}\{K_B = q(\ell^N(\xi))|X_A = \xi\} \cdot \mathbb{P}\{K_E = k_E|X_A = \xi\}\, d\xi} \quad (4.5)$$

where $\mathbb{P}\{K_B = k|K_A = \xi\}$ is given in (4.2), $\mathbb{P}\{K_B = K_A\}$ is given in (4.3), and

$$\mathbb{P}\{K_E = k_E|X_A\} = F_{\ell^N(x_E)}\left(g^{-1}\left(\frac{k_E - 1}{2^L}\right)\middle| X_A\right) - F_{\ell^N(x_E)}\left(g^{-1}\left(\frac{k_E}{2^L}\right)\middle| X_A\right) \quad (4.6)$$

Proof of (4.5):

Since, conditioned on X_A, the random variables X_B and X_E are independent,

$$\begin{aligned}\mathbb{P}\{K_E = k_E|K_A = K_B, X_A = \xi\} &= \frac{\mathbb{P}\{K_E = k_E \text{ and } K_A = K_B|X_A = \xi\}}{\mathbb{P}\{K_A = K_B|X_A = \xi\}} \\ &= \frac{\mathbb{P}\{K_E = k_E|X_A = \xi\} \cdot \mathbb{P}\{K_A = K_B|X_A = \xi\}}{\mathbb{P}\{K_A = K_B|X_A = \xi\}} \\ &= \mathbb{P}\{K_E = k_E|X_A = \xi\} \end{aligned} \quad (4.7)$$

Let $f_{X_A|K_A=K_B}(\xi) \triangleq \frac{d}{d\xi}\mathbb{P}\{X_A \leq \xi|K_A = K_B)$; and let $f_{X_A}(\xi) \triangleq \frac{d}{d\xi}\mathbb{P}\{X_A \leq \xi)$.

$$\begin{aligned} f_{X_A|K_A=K_B}(\xi) &\overset{(a)}{=} \frac{\mathbb{P}\{K_A = K_B|X_A = \xi\}}{\mathbb{P}\{K_A = K_B\}} f_{X_A}(\xi) \\ &\overset{(b)}{=} \frac{\mathbb{P}\{K_A = K_B|X_A = \xi\}}{\mathbb{P}\{K_A = K_B\}} \\ &\overset{(c)}{=} \frac{\mathbb{P}\{K_B = q(\ell^N(\xi))|X_A = \xi\}}{\mathbb{P}\{K_A = K_B\}} \end{aligned} \quad (4.8)$$

Here, (a) is an application of Bayes' rule; (b) follows from the uniformity of the random variable, X_A; and (c) substitutes $q(\ell^N(\xi))$ for K_A.

By the law of total probability, $p_1(k_E) = \mathbb{P}\{K_E = k_E|K_A = K_B\}$ can be written as

$$\mathbb{P}\{K_E = k_E|K_A = K_B\} = \int_0^1 \mathbb{P}\{K_E = k_E|K_A = K_B, X_A = \xi\} \cdot f_{X_A|K_A=K_B}(\xi)\, d\xi \quad (4.9)$$

Finally, by substituting the results of (4.7) and (4.8) in (4.9), we obtain (4.5). □

The second probability is

$$\boxed{p_2(k) = \frac{1}{\mathbb{P}\{K_\mathrm{A} = K_\mathrm{B}\}} \int_0^1 \mathbb{P}\{q(\ell^N(\xi)) = K_\mathrm{B} = k | X_\mathrm{A} = \xi\}\, d\xi} \tag{4.10}$$

where $\mathbb{P}\{K_\mathrm{A} = K_\mathrm{B}\}$ is given in (4.3), and

$$\mathbb{P}\{q(\ell^N(\xi)) = K_\mathrm{B} = k | X_\mathrm{A} = \xi\} = \begin{cases} \mathbb{P}\{K_\mathrm{B} = q(\ell^N(\xi))\}, & q(\ell^N(\xi)) = k \\ 0, & q(\ell^N(\xi)) \neq k \end{cases} \tag{4.11}$$

and where $\mathbb{P}\{K_\mathrm{B} = k | X_\mathrm{A} = \xi\}$ is given in (4.2).

Proof of (4.10):

Let $\tilde{K}$ denote a random variable, which takes values in the set of extended real numbers:

$$\tilde{K} = \begin{cases} K_\mathrm{A}, & K_\mathrm{A} = K_\mathrm{B} \\ \infty, & K_\mathrm{A} \neq K_\mathrm{B} \end{cases}$$

For a finite k, $\mathbb{P}\{\tilde{K} = k\}$ can be derived as follows:

$$\begin{aligned} \mathbb{P}\{\tilde{K} = k\} &\overset{(a)}{=} \int_0^1 \mathbb{P}\{\tilde{K} = k | X_\mathrm{A} = \xi\}\, d\xi \\ &\overset{(b)}{=} \int_0^1 \mathbb{P}\{q(\ell^N(\xi)) = K_\mathrm{B} = k | X_\mathrm{A} = \xi\}\, d\xi \end{aligned} \tag{4.12}$$

Here, (a) follows from the uniformity of the random variable, X_A; and (b) substitutes $q(\ell^N(\xi))$ for K_A.

For a finite k, the two events, $\{\tilde{K} = k\}$ and $\{K = k \text{ and } K_\mathrm{A} = K_\mathrm{B}\}$ are equivalent, giving:

$$\mathbb{P}\{\tilde{K} = k\} = \mathbb{P}\{K = k \text{ and } K_\mathrm{A} = K_\mathrm{B}\}$$

By applying the definition of conditional probability to the righthand side of the equation above, we obtain

$$p_2(k) = \frac{\mathbb{P}\{\tilde{K} = k\}}{\mathbb{P}\{K_\mathrm{A} = K_\mathrm{B}\}} \tag{4.13}$$

Finally, by substituting the results of (4.12) in (4.13), we obtain (4.10). □

The joint probability is

$$\boxed{\begin{aligned} p(k, k_{\mathrm{E}}) = & \frac{1}{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}}\}} \\ & \times \int_0^1 \mathbb{P}\{q(\ell^N(\xi)) = K_{\mathrm{B}} = k | X_{\mathrm{A}} = \xi\} \cdot \mathbb{P}\{K_{\mathrm{E}} = k_{\mathrm{E}} | X_{\mathrm{A}} = \xi\} \, d\xi \end{aligned}} \tag{4.14}$$

where $\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}}\}$ is given in (4.3), $\mathbb{P}\{K_{\mathrm{E}} = k_{\mathrm{E}} | X_{\mathrm{A}} = \xi\}$ is given in (4.6), and $\mathbb{P}\{q(\ell^N(\xi)) = K_{\mathrm{B}} = k | X_{\mathrm{A}} = \xi\}$ is given in (4.11).

Proof of (4.14):

$$\begin{aligned}
&\mathbb{P}\{K = k \text{ and } K_{\mathrm{E}} = k_{\mathrm{E}} | K_{\mathrm{A}} = K_{\mathrm{B}}\} \\
&\overset{(a)}{=} \int_0^1 \mathbb{P}\{K = k \text{ and } K_{\mathrm{E}} = k_{\mathrm{E}} | K_{\mathrm{A}} = K_{\mathrm{B}}, X_{\mathrm{A}} = \xi\} \cdot f_{X_{\mathrm{A}} | K_{\mathrm{A}} = K_{\mathrm{B}}}(\xi) \, d\xi \\
&\overset{(b)}{=} \int_0^1 \frac{\mathbb{P}\{K = k \text{ and } K_{\mathrm{A}} = K_{\mathrm{B}} \text{ and } K_{\mathrm{E}} = k_{\mathrm{E}} | X_{\mathrm{A}} = \xi\}}{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}} | X_{\mathrm{A}} = \xi\}} \cdot f_{X_{\mathrm{A}} | K_{\mathrm{A}} = K_{\mathrm{B}}}(\xi) \, d\xi \\
&\overset{(c)}{=} \int_0^1 \frac{\mathbb{P}\{K = k \text{ and } K_{\mathrm{A}} = K_{\mathrm{B}} | X_{\mathrm{A}} = \xi\} \cdot \mathbb{P}\{K_{\mathrm{E}} = k_{\mathrm{E}} | X_{\mathrm{A}} = \xi\}}{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}} | X_{\mathrm{A}} = \xi\}} \cdot f_{X_{\mathrm{A}} | K_{\mathrm{A}} = K_{\mathrm{B}}}(\xi) \, d\xi \\
&\overset{(d)}{=} \int_0^1 \frac{\mathbb{P}\{q(\ell^N(\xi)) = K_{\mathrm{B}} = k | X_{\mathrm{A}} = \xi\} \cdot \mathbb{P}\{K_{\mathrm{E}} = k_{\mathrm{E}} | X_{\mathrm{A}} = \xi\}}{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}} | X_{\mathrm{A}} = \xi\}} \cdot f_{X_{\mathrm{A}} | K_{\mathrm{A}} = K_{\mathrm{B}}}(\xi) \, d\xi \\
&\overset{(e)}{=} \int_0^1 \frac{\mathbb{P}\{q(\ell^N(\xi)) = K_{\mathrm{B}} = k | X_{\mathrm{A}} = \xi\} \cdot \mathbb{P}\{K_{\mathrm{E}} = k_{\mathrm{E}} | X_{\mathrm{A}} = \xi\}}{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}} | X_{\mathrm{A}} = \xi\}} \cdot \frac{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}} | X_{\mathrm{A}} = \xi\}}{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}}\}} \, d\xi \\
&\overset{(f)}{=} \frac{1}{\mathbb{P}\{K_{\mathrm{A}} = K_{\mathrm{B}}\}} \\
&\quad \times \int_0^1 \mathbb{P}\{q(\ell^N(\xi)) = K_{\mathrm{B}} = k | X_{\mathrm{A}} = \xi\} \cdot \mathbb{P}\{K_{\mathrm{E}} = k_{\mathrm{E}} | X_{\mathrm{A}} = \xi\} \, d\xi
\end{aligned}$$

Here, (a) is an application of the law of total probability; (b) is an application of Bayes' rule; (c) follows from the from the independence of X_{B} and X_{E}, conditioned on X_{A}; (d) substitutes $q(\ell^N(\xi))$ for K_{A}; and (e) follows from an application of Bayes' rule and the uniformity of the random variable, X_{A} (see (b) of (4.8)). □

Note that by marginalizing the joint probability in (4.14), we obtain the probabilities in (4.5) and (4.10). Fig. 4-2 is drawn from the analytical formula given in (4.4) and plots the predictability for $L = 2$ and $\frac{\sigma_{\mathrm{E}}}{\sigma_{\mathrm{B}}} = 2$. As expected, the predictability decreases from a value less than 1 and approaches 0 as the number of iterations and noise increase.

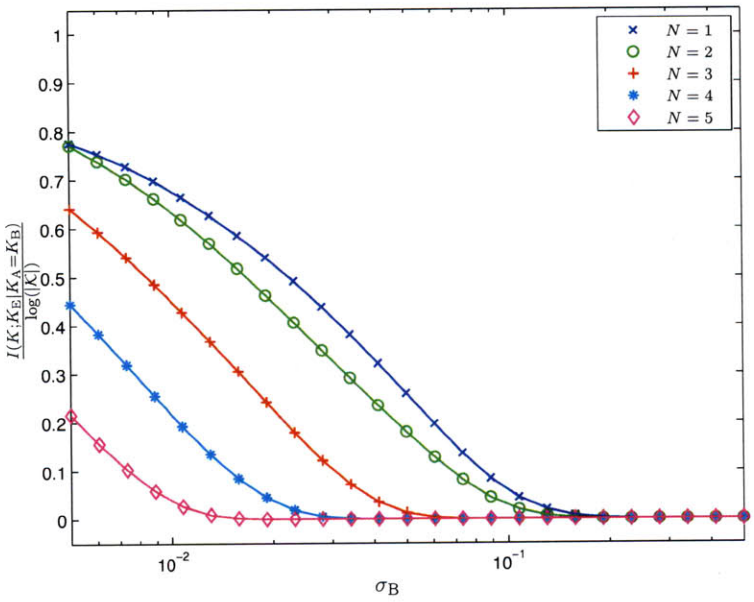


Figure 4-2: Predictability in bits plotted against σ_B for $L = 2$, $\frac{\sigma_E}{\sigma_B} = 2$, and various N.

4.4 Randomness

By definition, randomness, $\frac{H(K|K_A=K_B)}{\log(|\mathcal{K}|)}$, is given by:

$$\frac{H(K|K_A = K_B)}{\log(|\mathcal{K}|)} = -\frac{1}{\log(|\mathcal{K}|)} \cdot \sum_{k\in\mathcal{K}} p_2(k) \log p_2(k) \tag{4.15}$$

where $p_2(k) = \mathbb{P}\{K = k|K_A = K_B\}$ is defined in (4.10).

Fig. 4-3 is drawn from the analytical formula given in (4.15) and plots the randomness for $L = 2$ as a function of N. Note that randomness stabilizes after two iterations of the chaotic map.

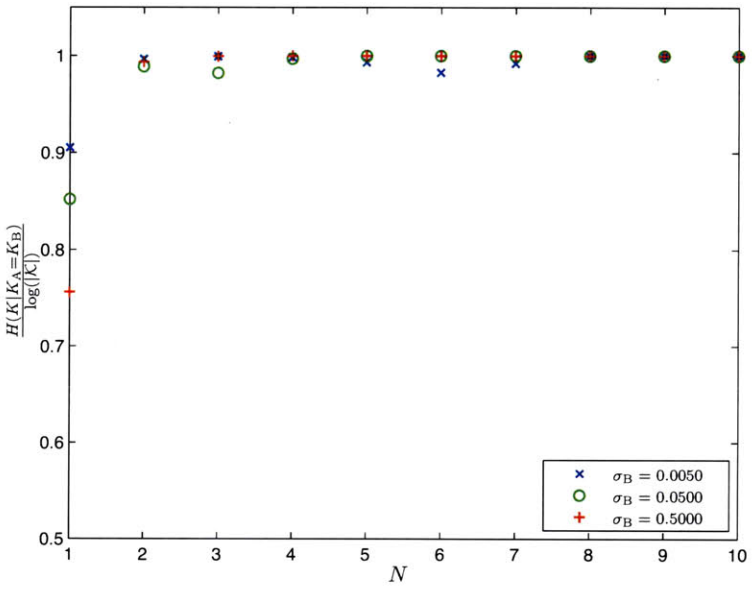


Figure 4-3: Randomness in bits plotted against the number of iterations for $L = 2$.

Chapter 5

Modified Per-Sample Scheme

It is important to note that the experiments published in [24] covered only the special case with zero eavesdroppers. Thus, the only metric that was effectively studied was reliability; neither unpredictability nor randomness was addressed in the published results. In this chapter, we present a modification to the per-sample scheme, which enables covert communication in the presence of a passive eavesdropper.

5.1 Scheme

The per-sample scheme works in the following way:

1. *In the handshaking phase:* The handshaking phase is identical to that given for the LMS. Alice and Bob send each other the same transmit signal. A schematic of the handshaking phase is given in fig. 2-1.

   (a) Alice broadcasts a signal, $p(t)$. The signal Bob receives can be modeled as $r_{\mathrm{B}}(t) = p(t) \otimes h_{\mathrm{AB}}(t) + n_{\mathrm{B}}(t)$.

   (b) Then Bob broadcasts the same transmit signal, $p(t)$; while Alice receives $r_{\mathrm{A}}(t) = p(t) \otimes h_{\mathrm{AB}}(t) + n_{\mathrm{A}}(t)$.

2. *In the key-generating phase:* Alice and Bob individually extract a key from his or her respective receive waveform. Each agent first generates decorrelated, normalized samples from his or her respective receive waveform and then computes a key from the amplitudes of these samples. Flowcharts depicting the similarities and differences

of the key-generating phases for the unmodified per-sample scheme (UPSS), the LMS, and the modified per-sample scheme (MPSS) are given in fig. 5.1.

(a-1) *For the UPSS only:*

i. Bob sends the coset assignments of his samples, where a sample's coset assignment is determined completely by the noise of the sample.

ii. Alice receives Bob's coset assignments and determines his quantized sample values from the received information; thus, Alice and Bob are able to agree on the same key bits.[1]

(a-2) *For the MPSS only:*

i. For each normalized sample, x, the agent first computes $y = s^N(x)$, where $s : [0,1] \to [0,1]$ is the binary shift map, defined as:

$$s(x) = \begin{cases} 2x, & 0 \leq x \leq 0.5 \\ 2x - 1, & 0.5 < x \leq 1 \end{cases}$$

$s^N(x)$ denotes the N-times composition function of $s(x)$, and an appropriate N is determined by the statistics of Alice and Bob's observational noise as well as Eve's estimation error.[2]

ii. For each transformed sample, y, the agent then computes $q_s : [0,1] \times \mathbb{N} \to \{1, 2, \ldots, 2^L\}$ defined as:

$$q_s(y, L) = \lceil 2^L y \rceil$$

where L denotes the number of binary key bits per sample. The quantized values for a sequence of y's are then concatenated sequentially to produce the final key.

It will be assumed that all agents operating in the network, including Eve, know the N- and L-values for the samples.

[1] It is assumed that Alice and Bob both have access to a lookup table, which maps the samples to their corresponding coset assignments.

[2] In a practical system, x is pre-quantized. However, so long as x is represented with $(L + 2^N)$-bits of precision, the analysis made in sec. 5.2 remains valid.

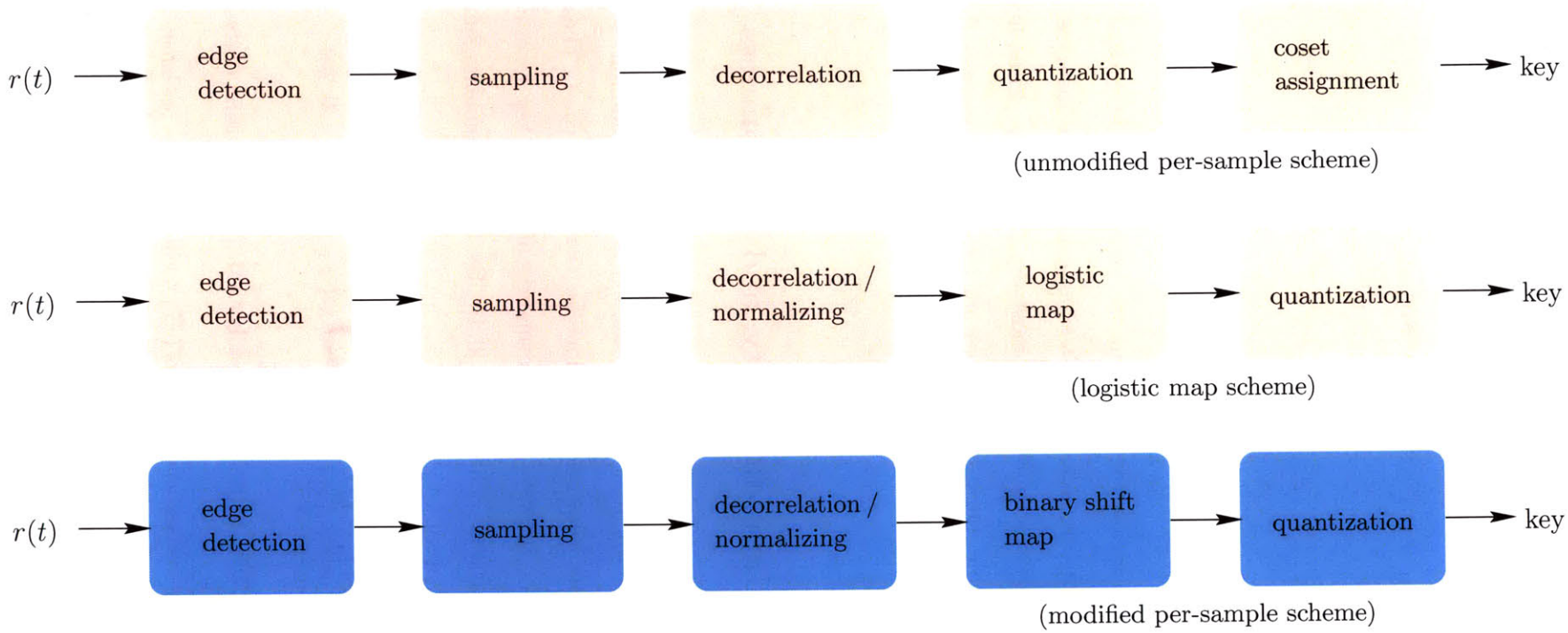


Figure 5-1: Flowcharts of the key-generating phase for the UPSS, the LMS, and the MPSS.

The rationale for step (a-2) in the MPSS is as follows. Let Alice and Bob's samples and Eve's best estimation of Alice's sample be denoted by:

$$x_{\mathrm{A}} = x_{\mathrm{A}_1} x_{\mathrm{A}_2} \ldots$$

$$x_{\mathrm{B}} = x_{\mathrm{B}_1} x_{\mathrm{B}_2} \ldots$$

$$x_{\mathrm{E}} = x_{\mathrm{E}_1} x_{\mathrm{E}_2} \ldots$$

respectively, where x_{A_i}, x_{B_i}, and x_{E_i} denote the i^{th} bits in the binary representations of x_{A}, x_{B}, and x_{E}, respectively.[3]

Alice and Bob each truncate the most and the least significant bits of each sample. Given the sample model in sec. 2.2, the most significant bits are insecure, because Eve has too much statistical knowledge of Alice's most significant bits. In addition, the least significant bits are unreliable, because Bob does not have enough statistical knowledge of Alice's least significant bits. Thus, these insecure or unreliable bits are removed from the final key.[4]

5.2 Reliability, Unpredictability, and Randomness

The results from this chapter is used in sec. 6.2 to compare the performance of the LMS against the MPSS. The reliability, the unpredictability, and the randomness for the MPSS are derived analytically, much like what was done for the LMS in ch. 4. These derivations will enable a fair comparison between the performances of the two key generation schemes.

Let X be a random variable defined over $[0, 1]$. By using arguments similar to those used in appendix A, the CDF of $s^N(X)$ at x is

$$F_{s^N(X)}(x) = \sum_{i=1}^{2^N} \left[F_X\left(\frac{i}{2^N} + \frac{x}{2^N}\right) - F_X\left(\frac{i}{2^N}\right) \right], \qquad 0 \le x \le 1 \tag{5.1}$$

where $F_X(\cdot)$ denotes the CDF of the initial distribution. Now, by using derivations similar

[3] A real number may have two binary representations (e.g., 0.1 and 0.0111... are binary representations of the same number). In such instances, we chose the binary representation, which does not terminate with an infinite sequence of 1's.

[4] Note that truncating the most significant bit of a binary number, x, is equivalent to running $s(x)$ on x, and that truncating the N most significant bits is equivalent to running $s^N(x)$ on x. The number of bits which remain in the key segment depends on the quantization parameter, L.

to those in ch. 4 and by using (5.1), we can determine the reliability for the MPSS as

$$\mathbb{P}\left\{K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\right\} = \int_0^1 \left[F_{s^N(X_\mathrm{B})}\left(\frac{q_s\left(s^N(\xi), L\right) - 1}{2^L} \middle| X_\mathrm{A} = \xi \right) - F_{s^N(X_\mathrm{B})}\left(\frac{q_s\left(s^N(\xi), L\right)}{2^L} \middle| X_\mathrm{A} = \xi \right) \right] d\xi \tag{5.2}$$

where $K_{(s,\mathrm{A})} = q_s\left(s^N(X_\mathrm{A}), L\right)$, and $K_{(s,\mathrm{B})} = q_s\left(s^N(X_\mathrm{B}), L\right)$.

Figs. A-1(b)-A-2(b) are drawn from the analytical formula given in (5.2) for $L = 2$. Figs. A-1(b) and A-2(b) plot the reliability and the *un*reliability as a function of σ_B-values, respectively.

Conditioned on $K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})} = K_s$, the unpredictability for the MPSS is as follows:

$$\frac{I\left(K_s; K_{(s,\mathrm{E})} \middle| K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\right)}{\log(|\mathcal{K}|)} = \frac{\sum_{k\in\mathcal{K}} \sum_{k_\mathrm{E}\in\mathcal{K}} p_s(k, k_\mathrm{E}) \log\left(\frac{p_s(k,k_\mathrm{E})}{p_{(s,1)}(k_\mathrm{E}) p_{(s,2)}(k)}\right)}{\log(|\mathcal{K}|)} \tag{5.3}$$

where $p_s(k, k_\mathrm{E}) = \mathbb{P}\{K_s = k \text{ and } K_{(s,\mathrm{E})} = k_\mathrm{E} | K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\}$, $p_{(s,1)}(k_\mathrm{E}) = \mathbb{P}\{K_{(s,\mathrm{E})} = k_\mathrm{E} | K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\}$, and $p_{(s,2)}(k) = \mathbb{P}\{K_s = k | K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\}$.

By repeating the proofs for (4.5), (4.10), and (4.14) (see sec. 4.3), the joint and marginal probabilities are given by:

$$\begin{aligned}
p_{(s,1)}(k_\mathrm{E}) &= \frac{\int_0^1 \mathbb{P}\{K_{(s,\mathrm{B})} = q_s(\ell^N(\xi)) | X_\mathrm{A} = \xi\} \cdot \mathbb{P}\{K_{(s,\mathrm{E})} = k_\mathrm{E} | X_\mathrm{A} = \xi\}\, d\xi}{\mathbb{P}\{K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\}} \\
p_{(s,2)}(k) &= \frac{1}{\mathbb{P}\{K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\}} \times \int_0^1 \mathbb{P}\{q_s(s^n(\xi)) = K_{(s,\mathrm{B})} = k | X_\mathrm{A} = \xi\}\, d\xi \\
p_s(k, k_\mathrm{E}) &= \frac{1}{\mathbb{P}\{K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\}} \\
&\quad \times \int_0^1 \mathbb{P}\{q_s(s^n(\xi)) = K_{(s,\mathrm{B})} = k | X_\mathrm{A} = \xi\} \cdot \mathbb{P}\{K_{(s,\mathrm{E})} = k_\mathrm{E} | X_\mathrm{A} = \xi\}\, d\xi
\end{aligned} \tag{5.4}$$

where

$$\mathbb{P}\{q_s(s^N(\xi)) = K_\mathrm{B} = k | X_\mathrm{A} = \xi\} = \begin{cases} \mathbb{P}\{K_{(s,\mathrm{B})} = q_s(s^N(\xi))\}, & q_s(s^N(\xi)) = k \\ 0, & q_s(s^N(\xi)) \neq k \end{cases}$$

and where $\mathbb{P}\{K_{(s,\mathrm{B})} = k_\mathrm{B} | X_\mathrm{A}\}$ and $\mathbb{P}\{K_{(s,\mathrm{E})} = k_\mathrm{E} | X_\mathrm{A}\}$ are defined in terms of $F_{s^N(x)}(\cdot)$.

Figs. A-3(b)-A-7(b) are drawn from the analytical formula given in (5.3) with $L = 2$ and $\frac{\sigma_\mathrm{E}}{\sigma_\mathrm{B}} = 2$, 4, 8, 16, or 32; the figures plot the predictability over a range of σ_B-values.

Conditioned on $K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})} = K_s$, the randomness for the MPSS is given by:

$$\frac{H(K_s|K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})})}{\log(|\mathcal{K}|)} = -\frac{\sum_{k=\mathcal{K}} p_{(s,2)}(k) \log p_{(s,2)}(k)}{\log(|\mathcal{K}|)} \tag{5.5}$$

where $p_{(s,2)}(k) = \mathbb{P}\{K_s = k|K_{(s,\mathrm{A})} = K_{(s,\mathrm{B})}\}$ is defined in (5.4).

Figs. A-8(b) and A-9(b) are drawn from the analytical formula given in (5.5) for $L = 2$; the figures plot the randomness and the *un*randomness as a function of N.

Chapter 6

Numerical Results

In the first section of this chapter, we determine whether the LMS provides reliability, unpredictability, and randomness. In addition, we explain how to extend our per sample analysis to include cases where the number of samples per agent exceeds one. In the second part, we compare the performance of the LMS against that of the MPSS.

6.1 Interpretations of Eqns. 4.1, 4.4, and 4.15

The LMS can be determined to be a viable secret key agreement scheme by solving a system of inequalities. Let $\overrightarrow{\epsilon} = [\epsilon_1, \epsilon_2, \epsilon_3]$ denote the allowable error vector for the triple, $(x_{\mathrm{A}}, x_{\mathrm{B}}, x_{\mathrm{E}})$. For a fixed key segment length, L, the LMS provides reliability, unpredictability, and randomness for the allowable error, $\overrightarrow{\epsilon}$, if the following system of inequalities is met:

$$\begin{aligned} 1 - \mathbb{P}\{K_{\mathrm{B}} = K_{\mathrm{A}}\} &\leq \epsilon_1 \\ \frac{I(K; K_{\mathrm{E}} | K_{\mathrm{A}} = K_{\mathrm{B}})}{\log(|\mathcal{K}|)} &\leq \epsilon_2 \\ 1 - \frac{H(K | K_{\mathrm{A}} = K_{\mathrm{B}})}{\log(|\mathcal{K}|)} &\leq \epsilon_3 \end{aligned}$$

where $\mathbb{P}\{K_{\mathrm{B}} = K_{\mathrm{A}}\}$ is given in (4.1), $\frac{I(K;K_{\mathrm{E}}|K_{\mathrm{A}}=|kb)}{\log(|\mathcal{K}|)}$ is given in (4.4), and $\frac{H(K|K_{\mathrm{A}}=K_{\mathrm{B}})}{\log(|\mathcal{K}|)}$ is given in (4.15). Note that as N increases; reliability decreases (i.e., the probability of key agreement decreases), whereas as unpredictability and randomness increase (i.e., mutual information decreases, and entropy increases). Under the reasonable assumption that Eve's

estimation error is strictly larger than Bob's observational noise, there exists some N such that the inequalities hold for some $\overrightarrow{\epsilon} = [\epsilon_1, \epsilon_2, \epsilon_3]$. This insight suggests that for the LMS to be a viable secret key agreement scheme, there exists some bounded values of N that satisfy the error criteria.

The numerical results presented in this thesis indicate that the LMS provides reliability, unpredictability, and randomness under realistic conditions. In ultra-wide bandwidth systems, typical signal to noise ratios (SNR) range from 0 dB to 40 dB, which translates to typical values for σ_B ranging from rom 5×10^{-3} (high SNR) to 0.5 (low SNR). From figs. A-3(a)-A-7(a), and A-9(a), 3-5 iterations of the chaotic map suffice to reach acceptably small errors in unpredictability and randomness. From fig. A-1(a), even after 3-5 iterations, the probability of key agreement is still relatively high for lower σ_B-values in the typical range. Thus, the LMS is information-theoretically secure in the sense that non-zero, secret key lengths are achievable for some positive key length L and for some reasonably small, allowable errors in performance.

The per sample analysis can be extended to include cases where the number of samples per agent exceeds one. If the samples are independent, then the mutual information as well as the entropy can be scaled trivially. The challenge lies in preserving a high probability of key agreement. To that end, the decision to keep or to drop a sample as well as determining the key segment length, L, can be made on a per sample basis depending on the estimated values for x_A, σ_B, and σ_E. Furthermore, in time-variant systems, we can allow error detection and correction schemes to guarantee reliability at a cost in key rate.

6.2 Comparative Analysis

Having derived the analytical expressions for the reliability, the unpredictability, and the randomness for both the LMS (in ch. 4) and the MPSS (in sec. 5.2), we are now able to compare the two methods' performance in terms of the average achievable key length. We do this by fixing ϵ_2, ϵ_3, L, and the ratio, $\frac{\sigma_E}{\sigma_B} > 1$. From figs. A-8(a) and A-8(b), the entropy of the shared key stabilizes to near the maximum entropy after about two iterations of $\ell(x)$ for the LMS, and about two iterations of $s(x)$ for the MPSS. We, therefore, assume that an acceptable level of uniformity in the shared key is reached in all conditions where $N \geq 2$. Based on the mutual information values given in figs. A-3(a)-A-7(a) and A-3(b)-A-7(b), a

threshold of 10^{-4} is chosen for ϵ_2.

For both the LMS and the MPSS, we determine M, the maximum of 2 (i.e., the number of iterations needed to satisfy the randomness condition) and the minimum number of iterations necessary to reduce the mutual information to 10^{-4} (i.e., the chosen threshold for mutual information). We then calculate the corresponding average key length (after M iterations) over a range of σ_{B}-values for $\left(L, \frac{\sigma_{\mathrm{E}}}{\sigma_{\mathrm{B}}}\right) \in \{1,2\} \times (2,4,8,16,32)$.

Fig. 6-1 below depicts the average key length for $L = 2$ and $\frac{\sigma_{\mathrm{E}}}{\sigma_{\mathrm{B}}} = 8$ using the LMS and the MPSS, respectively. Note that for the typical range of observational noise, $\sigma_{\mathrm{B}} \in [5 \times 10^{-3}, 0.5]$, the LMS generally outperforms the MPSS. (Similar plots with different $\left(L, \frac{\sigma_{\mathrm{E}}}{\sigma_{\mathrm{B}}}\right)$-pairs are provided in figs. A-10(a)-A-14(a) at the end of appendix A.)

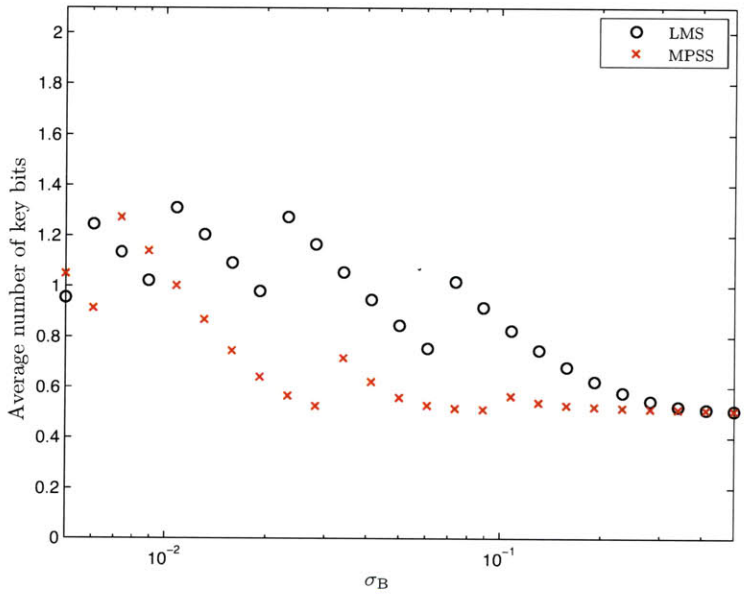


Figure 6-1: Comparative analysis for $\epsilon_2 = 10^{-4}$ and $\frac{\sigma_{\mathrm{E}}}{\sigma_{\mathrm{B}}} = 8$ for $L = 2$.

Chapter 7

Conclusion and Recommendations

A key generation scheme is proposed and its performance analyzed. The method, the LMS, is applicable for use on wireless networks because it does not require devices to engage in computationally intensive algorithms. In addition, the method is shown to achieve reliability from the perspective of the communication agents, as well as unpredictability and randomness from the perspective of an eavesdropper. Lastly, the performance of the LMS is compared against that of an existing technique. Results from a comparative analysis indicate that the proposed method generally yields a greater number of reliable, unpredictable, and random key bits than the existing technique under the same conditions. These results bring us closer towards realizing information-theoretically secure cryptosystems.

However, more research should be conducted to understand the practicality of the LMS. In order to truly understand whether the LMS is a competitive technique for secure communications, a thorough proof-of-concept study to tackle the challenging problem of how to realistically model Eve's best estimation of Alice's sample should be conducted. In addition, pre-processing techniques for producing decorrelated and normalized samples from receive waveforms should be developed and analyzed for standard channel models. Finally, it may be of interest to determine the achievable secret key rate by utilizing the LMS for various coherence times and to extend the results of this thesis to include multiple malicious and / or colluding eavesdroppers.

Appendix A

CDF of N Logistic Map Transforms

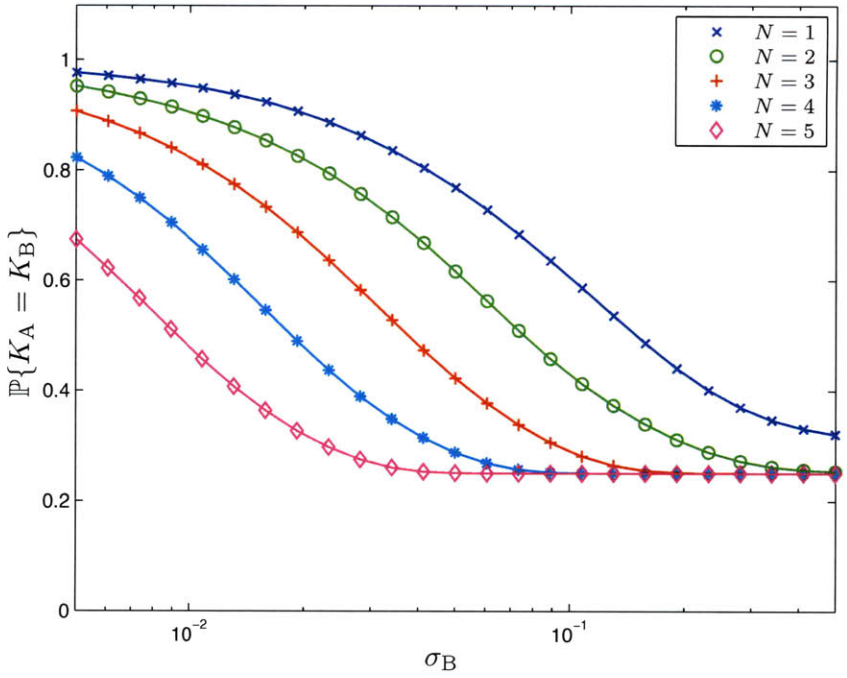
In this section, we derive the formula for the cumulative density function (CDF) of $\ell^N(X)$, given any random variable, X, defined over $[0,1]$ and with arbitrary CDF, F_X, given in analytical form. We first introduce a linear map, $t(x)$, which is easier to analyze than $\ell : [0,1] \rightarrow [0,1]$ defined as $\ell(x) = 4x(1-x)$ (our quadratic map). Our general approach will be to derive the formula for the CDF of $t^N(X)$ and then derive the formula for the CDF of $\ell^N(X)$ by performing the appropriate transformations between the linear and quadratic domains.

Definition A.0.1 *Let $t : [0,1] \rightarrow [0,1]$ denote the tent map given by:*

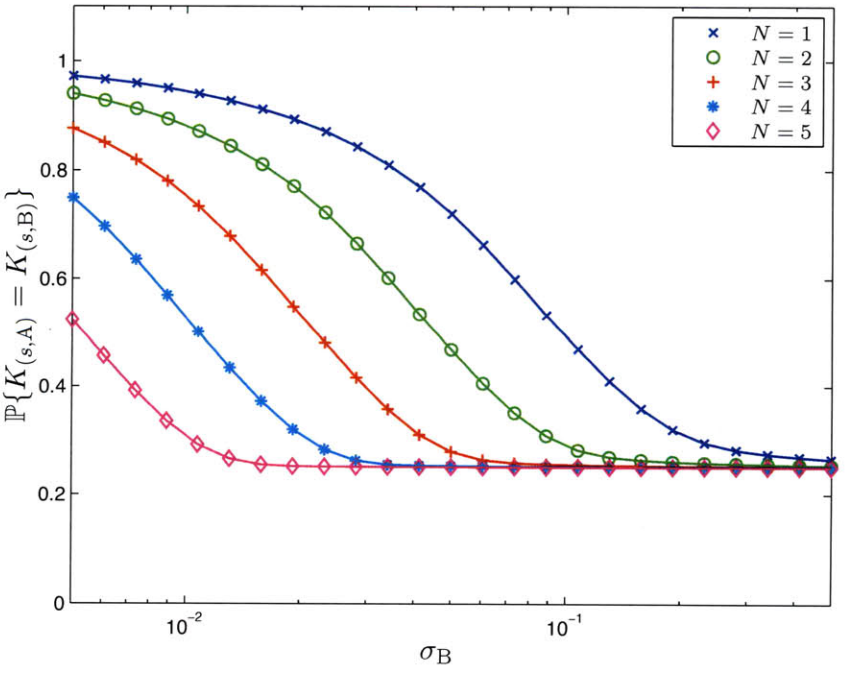
$$t(x) = \begin{cases} 2x, & 0 \leq x \leq 0.5 \\ -2x+2, & 0.5 < x \leq 1 \end{cases}$$

The tent map is a mathematical description of the quintessential example of a chaotic system: the kneading of dough [26]. In one iteration of the tent transform, an initial distribution is evenly stretched to twice its original width and then folded over in the middle; thus, the CDF of the distribution after one iteration at an arbitrarily point, $x \in [0,1]$, is equivalent to the measure of the original distribution from 0 to $\frac{x}{2}$ plus the measure of the original distribution from $\left(1 - \frac{x}{2}\right)$ to 1.

By generalizing this insight, the formula for the CDF at the N^{th} iteration is as follows. The formula for the CDF of $t^N(X)$ at x is as follows.

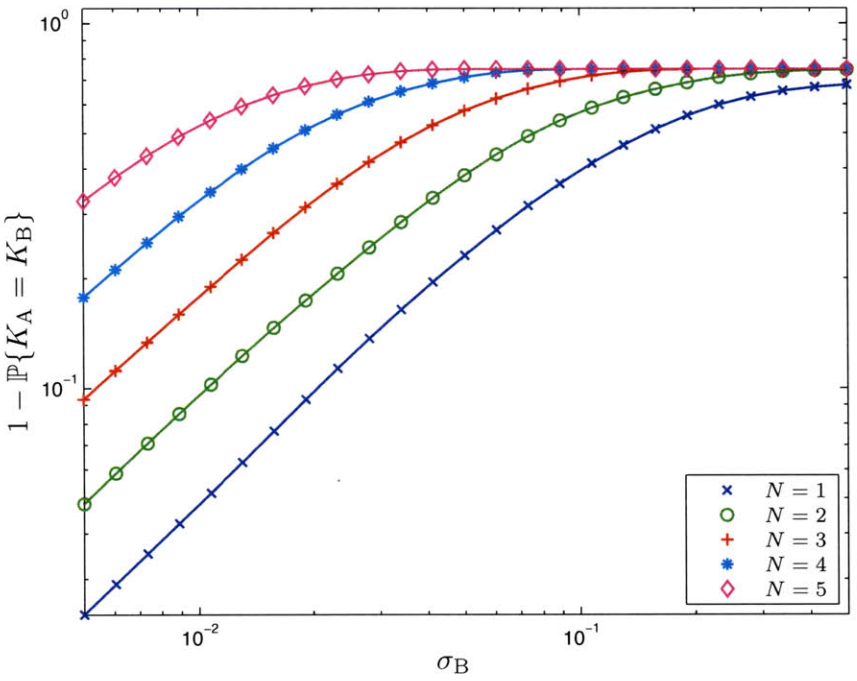


(a) Logistic Map Scheme

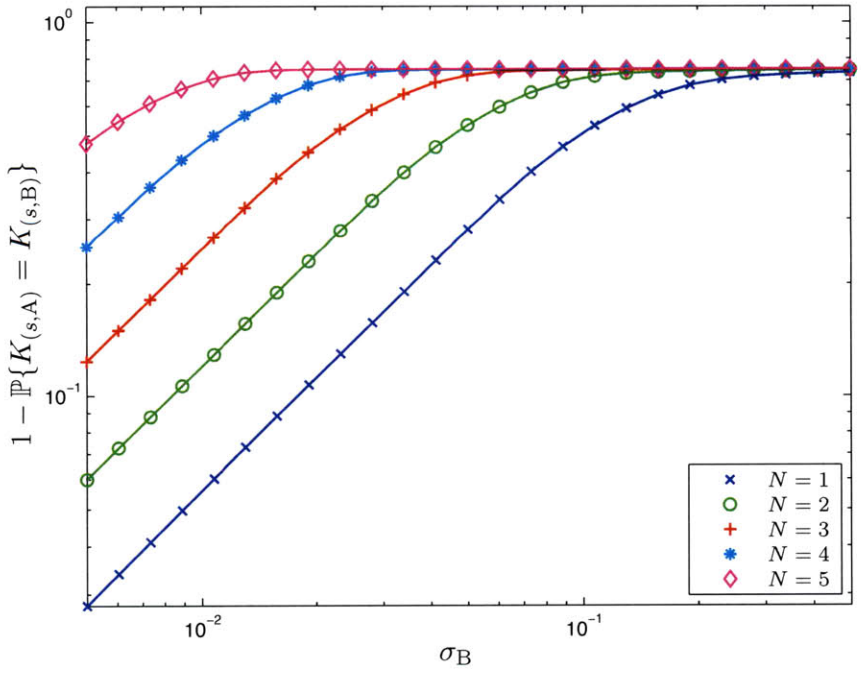


(b) Modified Per-Sample Scheme

Figure A-1: Reliability plotted against σ_{B} for $L = 2$ and various N. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

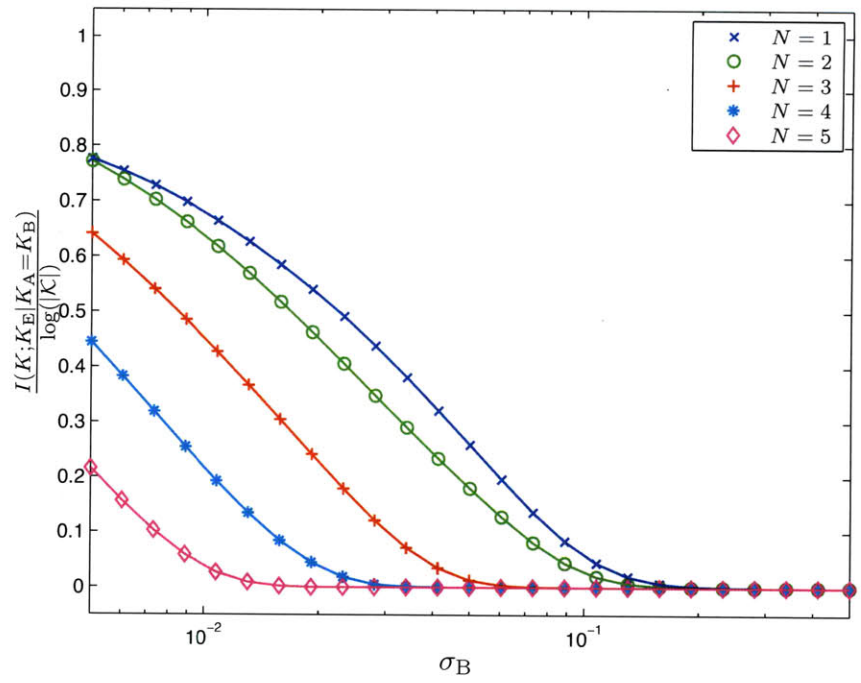


(a) Logistic Map Scheme

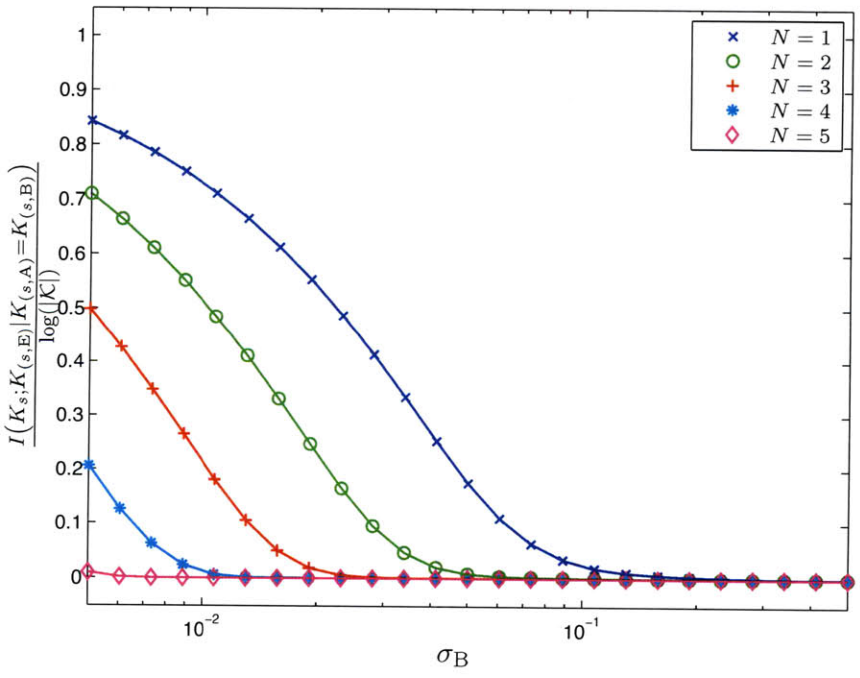


(b) Modified Per-Sample Scheme

Figure A-2: *Un*reliability plotted against σ_{B} for $\underline{L = 2}$ and various N. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

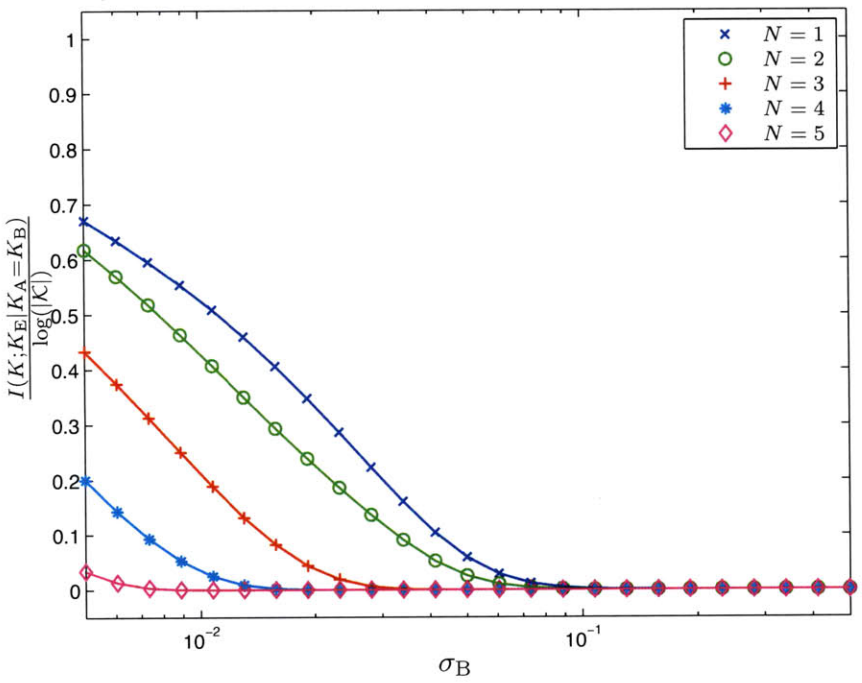


(a) Logistic Map Scheme

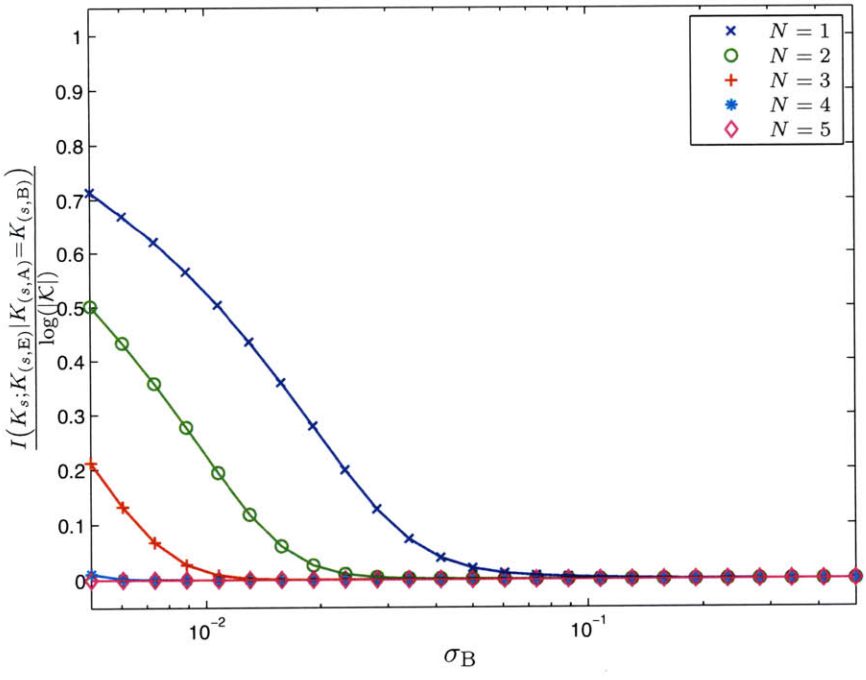


(b) Modified Per-Sample Scheme

Figure A-3: Predictability in bits plotted against σ_B for $L = 2$, $\frac{\sigma_E}{\sigma_B} = 2$, and various N. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

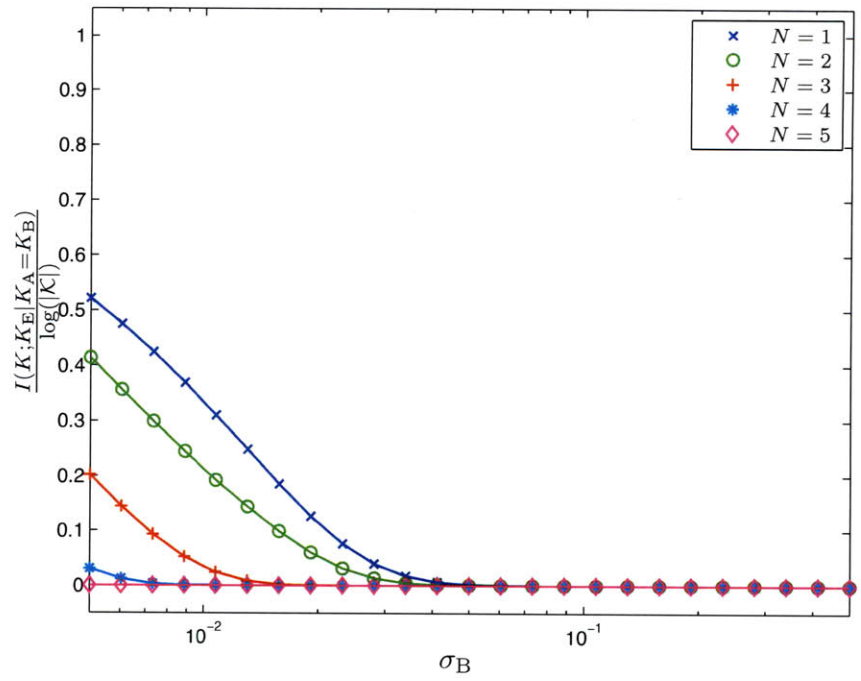


(a) Logistic Map Scheme

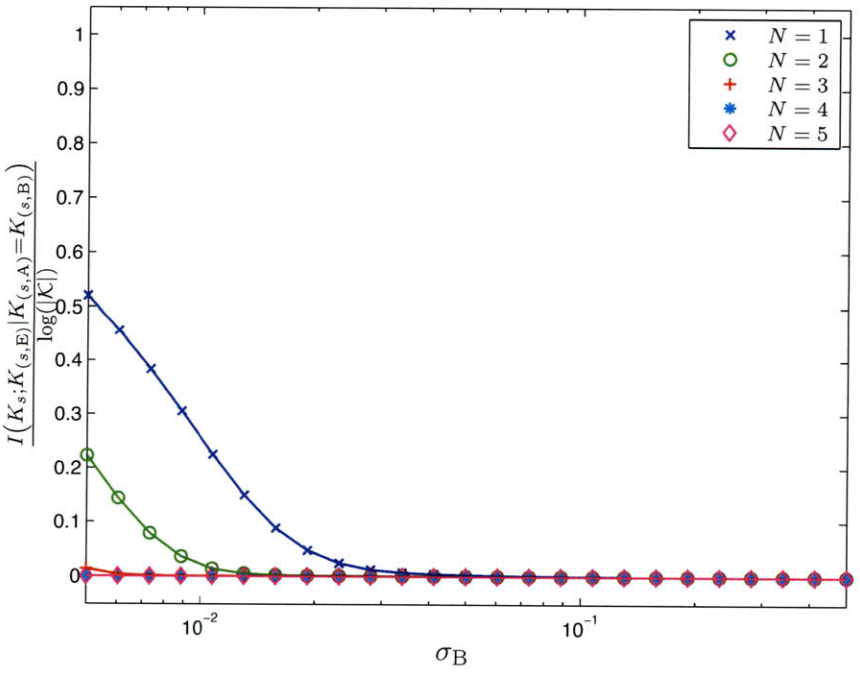


(b) Modified Per-Sample Scheme

Figure A-4: Predictability in bits plotted against σ_B for $L = 2$, $\frac{\sigma_E}{\sigma_B} = 4$, and various N. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

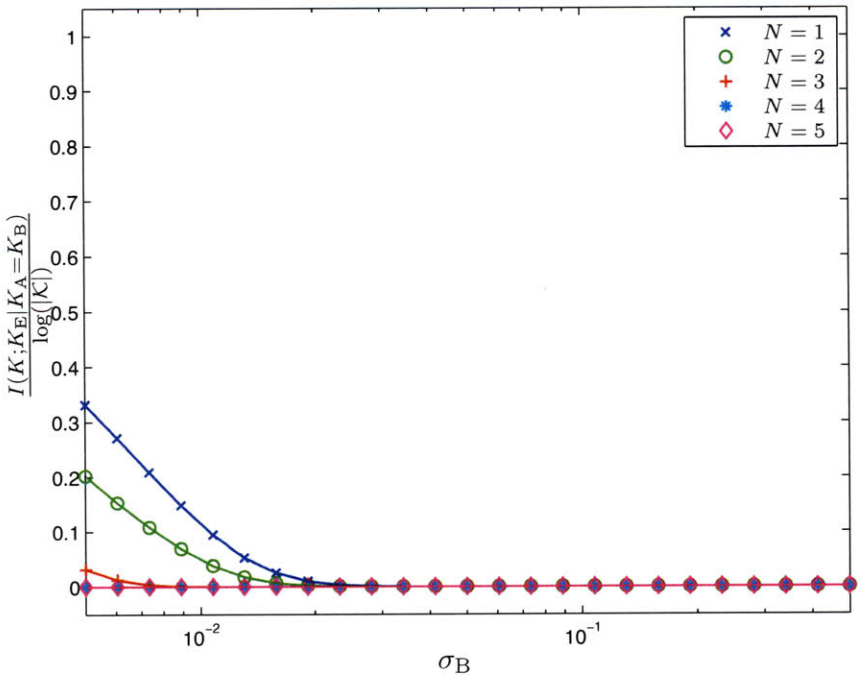


(a) Logistic Map Scheme

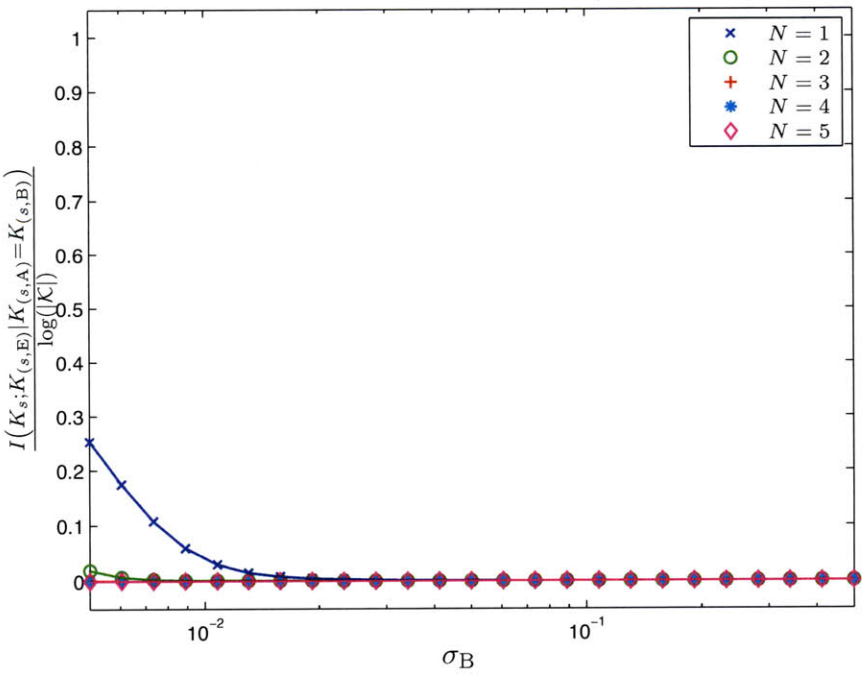


(b) Modified Per-Sample Scheme

Figure A-5: Predictability in bits plotted against σ_B for $L = 2$, $\frac{\sigma_E}{\sigma_B} = 8$, and various N. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

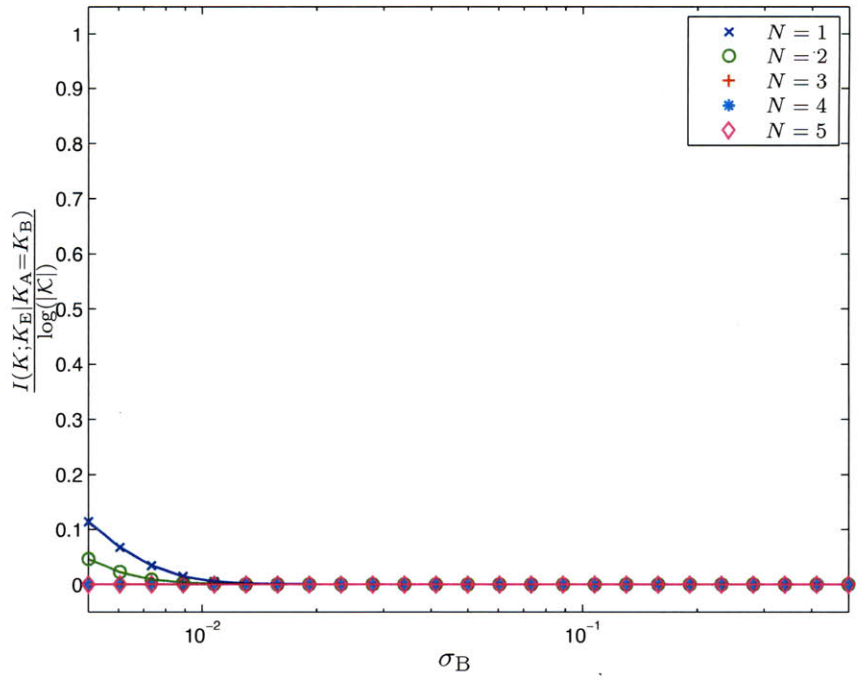


(a) Logistic Map Scheme

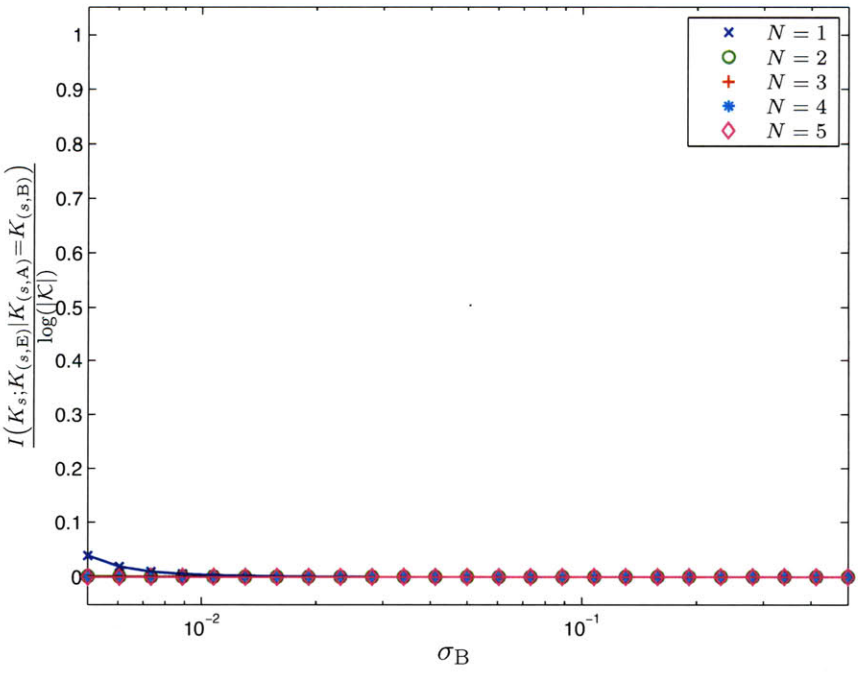


(b) Modified Per-Sample Scheme

Figure A-6: Predictability in bits plotted against σ_B for $L = 2$, $\frac{\sigma_E}{\sigma_B} = 16$, and various N. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

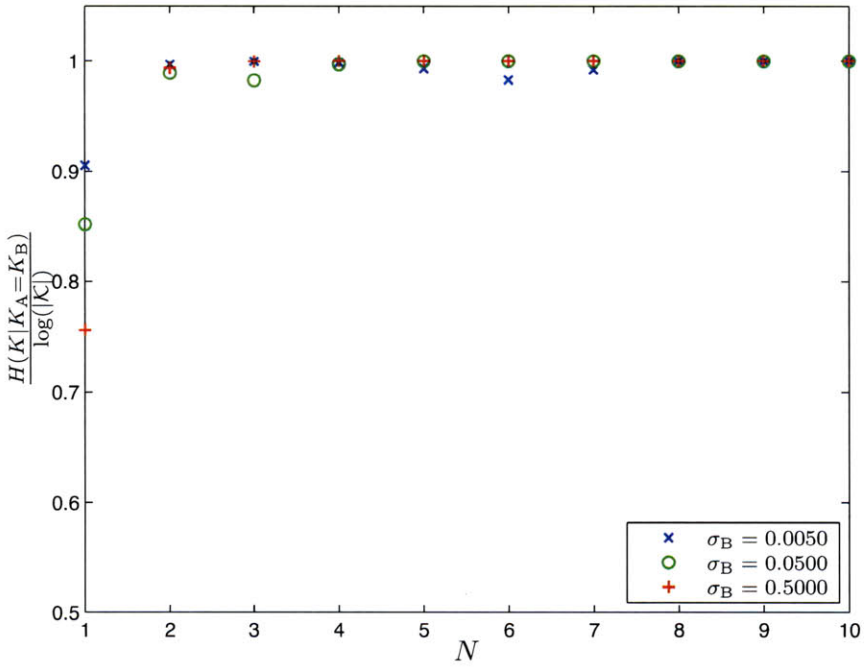


(a) Logistic Map Scheme

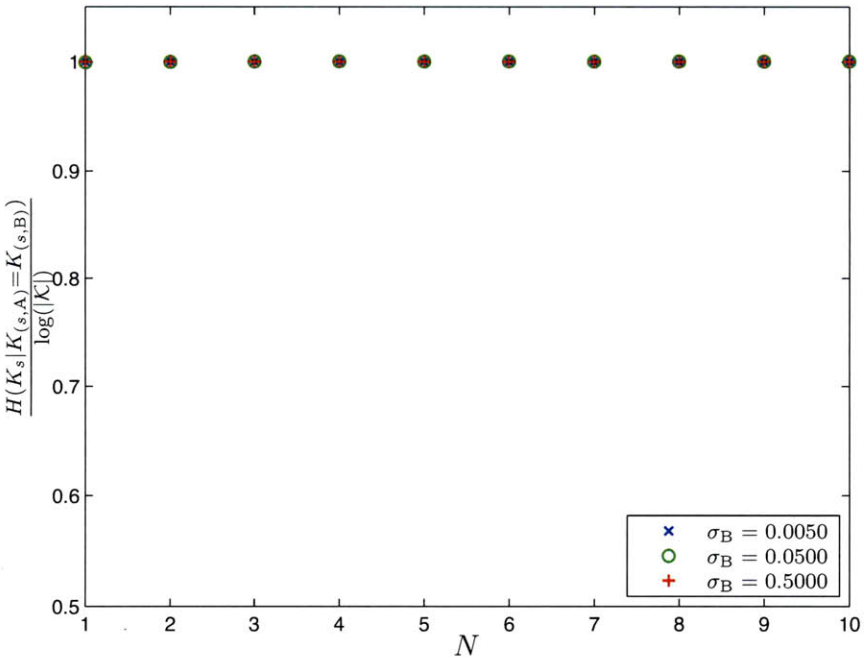


(b) Modified Per-Sample Scheme

Figure A-7: Predictability in bits plotted against σ_B for $L = 2$, $\frac{\sigma_E}{\sigma_B} = 32$, and various N. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

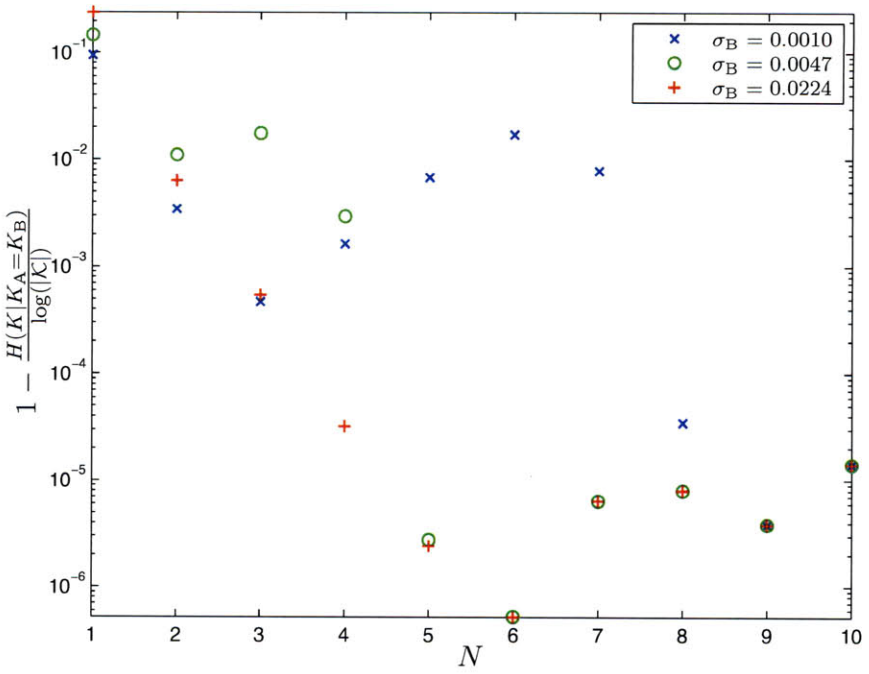


(a) Logistic Map Scheme

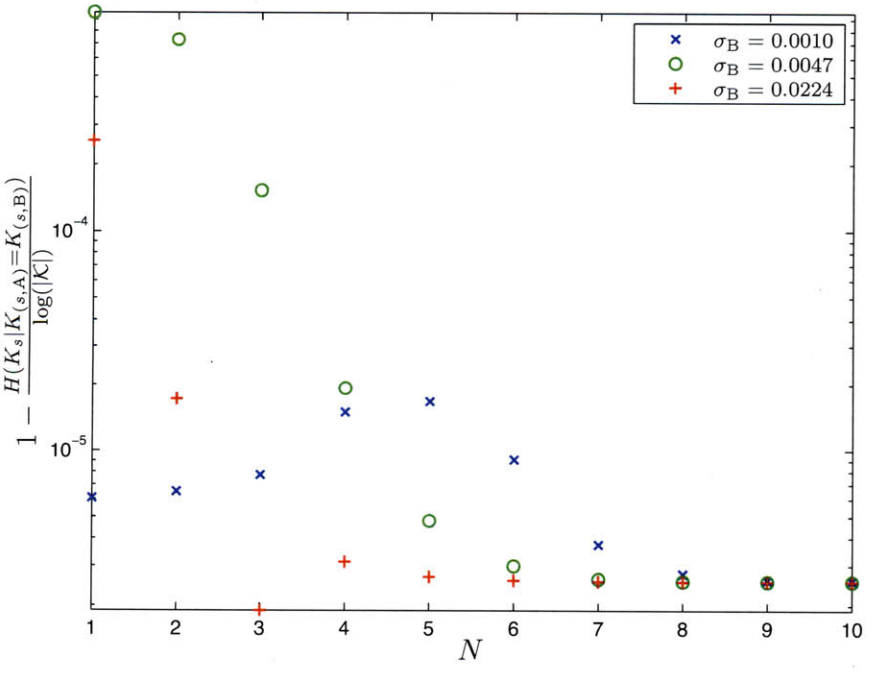


(b) Modified Per-Sample Scheme

Figure A-8: Randomness in bits plotted against the number of iterations for $\underline{L = 2}$. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

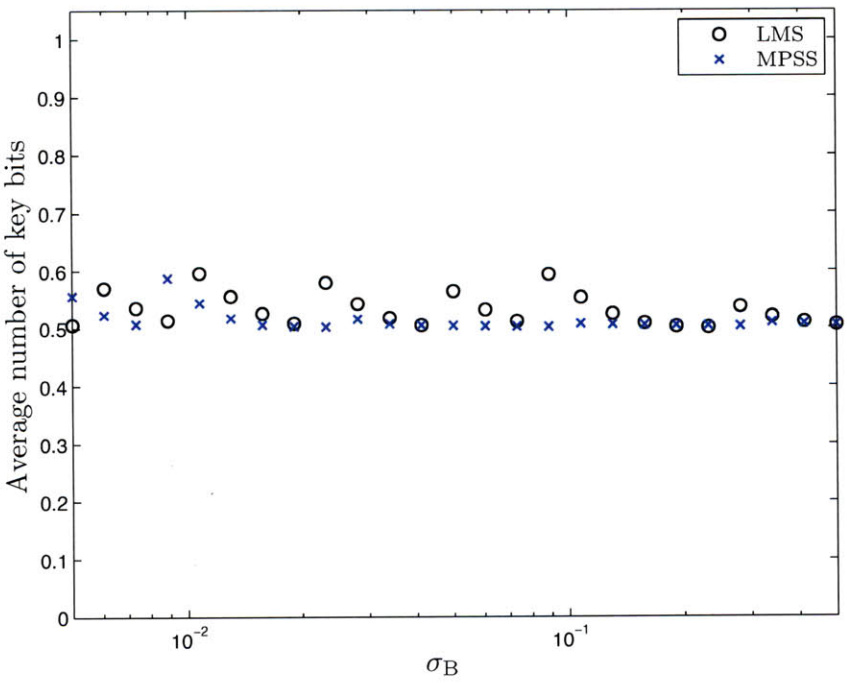


(a) Logistic Map Scheme

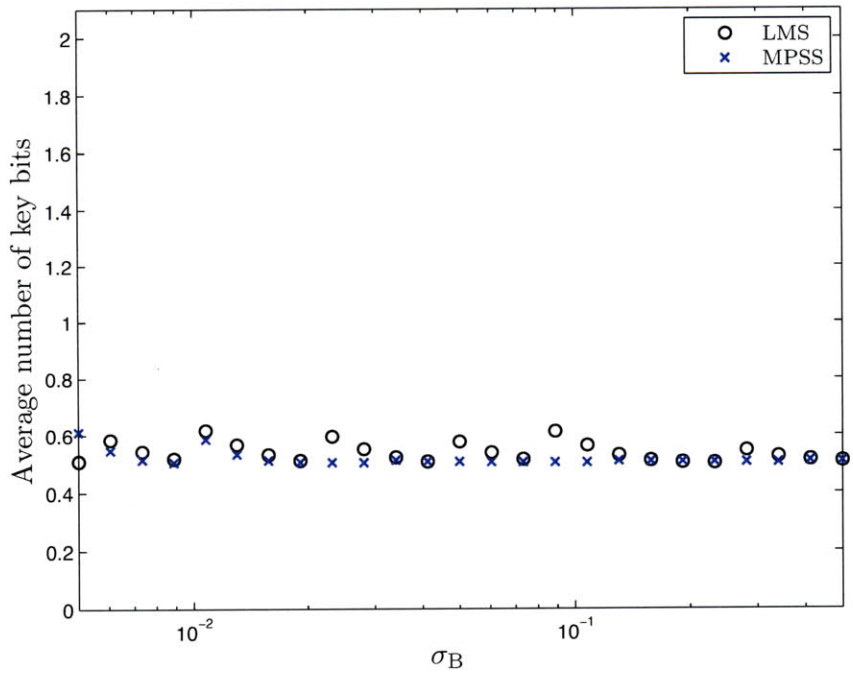


(b) Modified Per-Sample Scheme

Figure A-9: *Un*randomness in bits plotted against the number of iterations for $\underline{L = 2}$. Figs. (a) and (b) depict the results for the LMS and the MPSS, respectively.

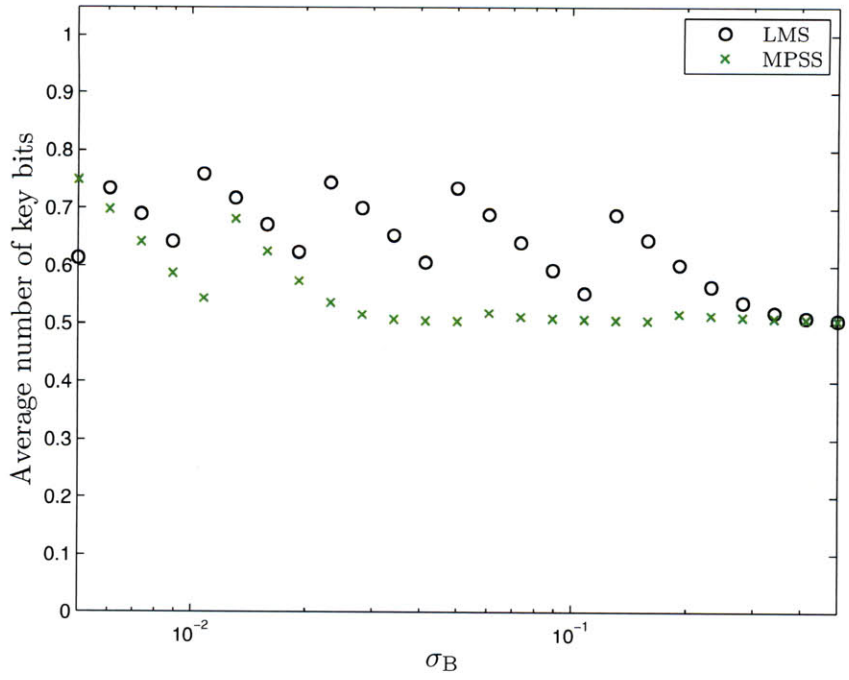


(a) $L = 1$

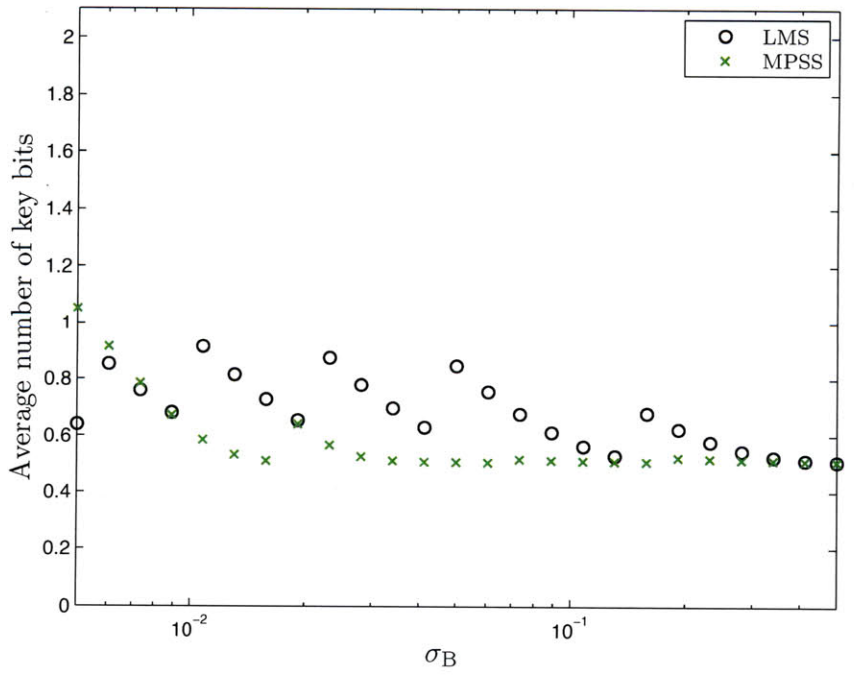


(b) $L = 2$

Figure A-10: Comparative analysis for $\epsilon_2 = 10^{-4}$ and $\frac{\sigma_E}{\sigma_B} = 2$. Figs. (a) and (b) depict the results for $L = 1$ and $L = 2$, respectively.

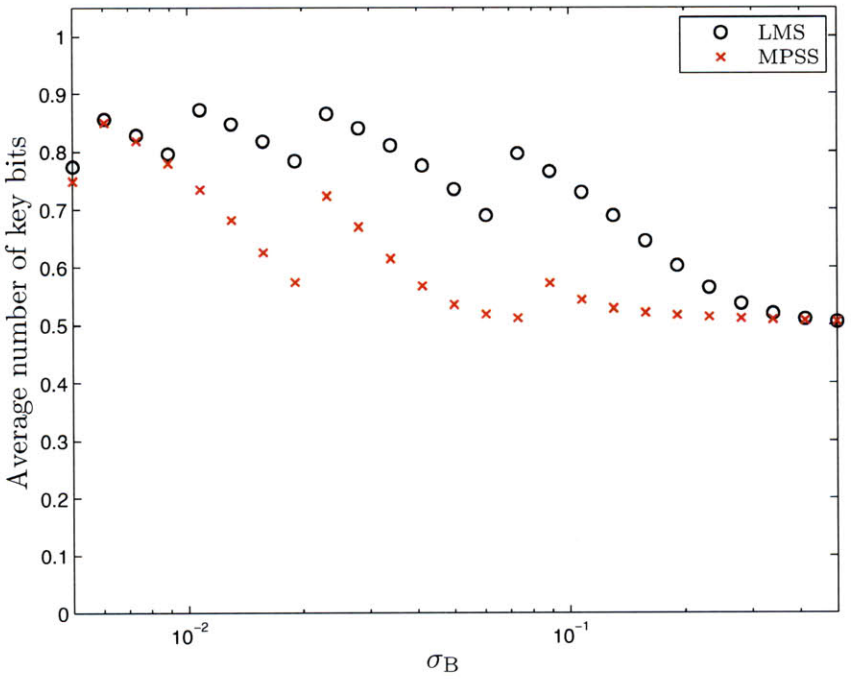


(a) $L = 1$

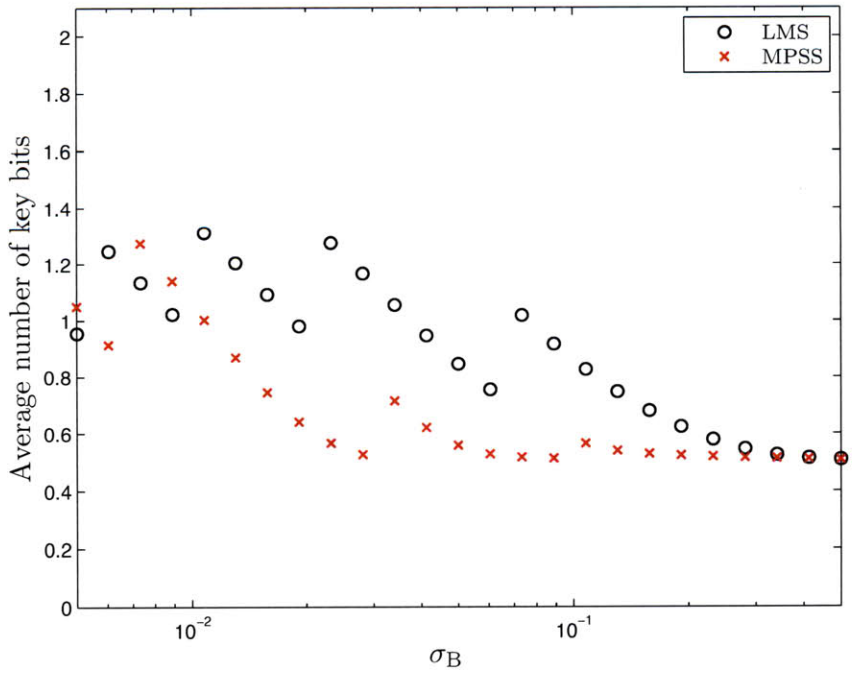


(b) $L = 2$

Figure A-11: Comparative analysis for $\epsilon_2 = 10^{-4}$ and $\frac{\sigma_E}{\sigma_B} = 4$. Figs. (a) and (b) depict the results for $L = 1$ and $L = 2$, respectively.

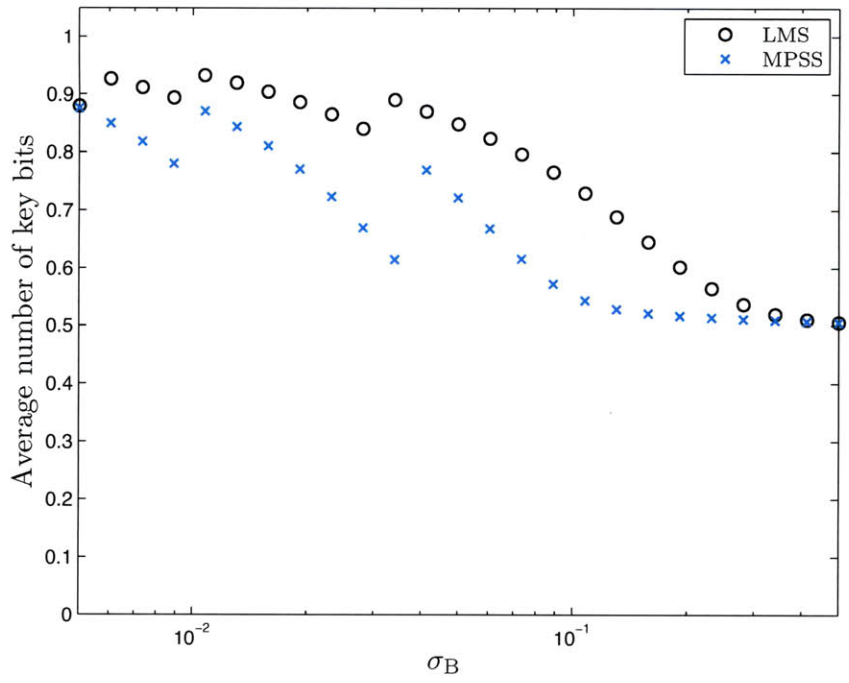


(a) $L = 1$

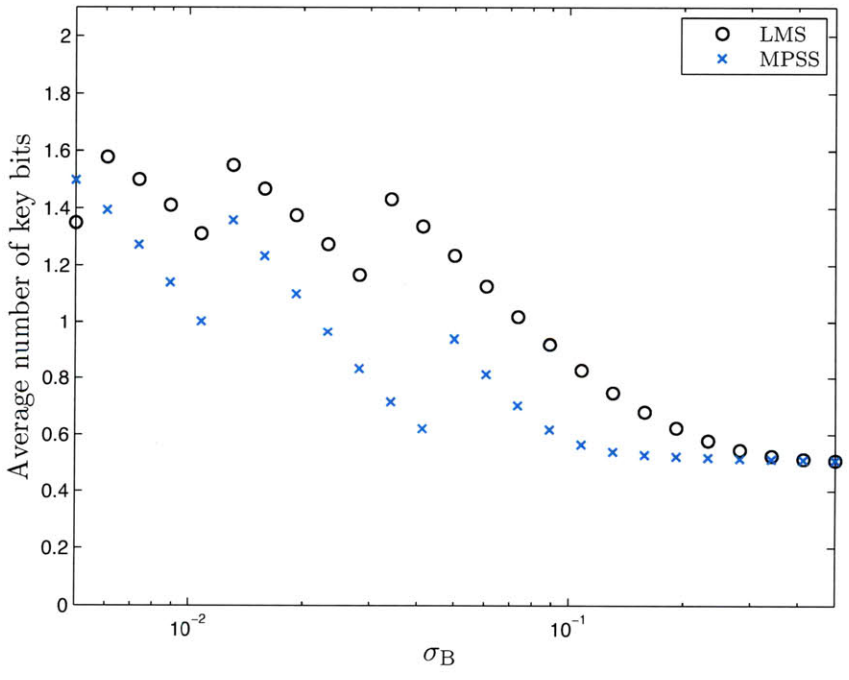


(b) $L = 2$

Figure A-12: Comparative analysis for $\epsilon_2 = 10^{-4}$ and $\frac{\sigma_E}{\sigma_B} = 8$. Figs. (a) and (b) depict the results for $L = 1$ and $L = 2$, respectively.

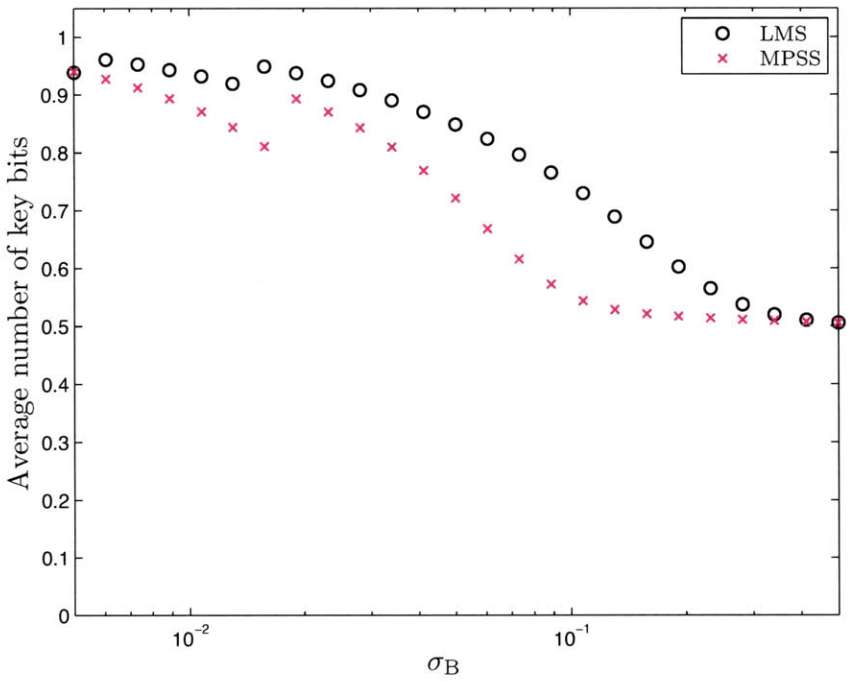


(a) $L = 1$

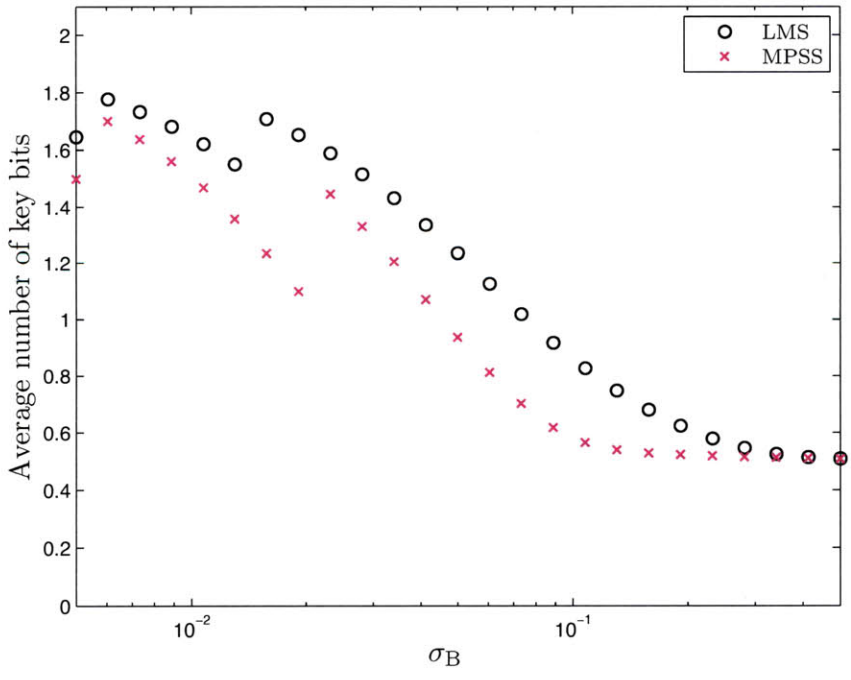


(b) $L = 2$

Figure A-13: Comparative analysis for $\epsilon_2 = 10^{-4}$ and $\frac{\sigma_E}{\sigma_B} = 16$. Figs. (a) and (b) depict the results for $L = 1$ and $L = 2$, respectively.



(a) $L = 1$



(b) $L = 2$

Figure A-14: Comparative analysis for $\epsilon_2 = 10^{-4}$ and $\frac{\sigma_E}{\sigma_B} = 32$. Figs. (a) and (b) depict the results for $L = 1$ and $L = 2$, respectively.

Bibliography

[1] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[2] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, 2008.

[3] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," *Proc. 2008 IEEE Symp. on Security and Privacy*, pp. 129–142, 2008.

[4] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci. Int.*, vol. 28, no. 2, pp. 270–299, 1983.

[5] D. Dolev and A. Yao, "On the security of public key schemes," *Proc. IEEE 22nd Annual Symp. on Found. of Comp. Sci.*, pp. 350–357, 1981.

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[7] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[8] ——, "The strong secret key rate of discrete random triples, in communication and cryptography – two sides of one tapestry," *Kluwer Academic Publishers*, pp. 271–285, 1994.

[9] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *Eurocrypt 2000, Lecture Notes in Computer Science*, vol. 1807, pp. 351+, 2000. [Online]. Available: citeseer.ist.psu.edu/maurer00informationtheoretic.html

[10] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[11] M. Z. Win and R. A. Scholtz, "Impulse radio: How it works," *IEEE Commun. Lett.*, vol. 2, no. 2, pp. 36–38, Feb. 1998.

[12] ——, "Ultra-wide bandwidth time-hopping spread-spectrum impulse radio for wireless multiple-access communications," *IEEE Trans. Commun.*, vol. 48, no. 4, pp. 679–691, Apr. 2000.

[13] ——, "Characterization of ultra-wide bandwidth wireless indoor communications channel: A communication theoretic view," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 9, pp. 1613–1627, Dec. 2002.

[14] D. Cassioli, M. Z. Win, and A. F. Molisch, "The ultra-wide bandwidth indoor channel: from statistical model to simulations," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 6, pp. 1247–1257, Aug. 2002.

[15] A. F. Molisch, D. Cassioli, C.-C. Chong, S. Emami, A. Fort, B. Kannan, J. Karedal, J. Kunisch, H. Schantz, K. Siwiak, and M. Z. Win, "A comprehensive standardized model for ultrawideband propagation channels," *IEEE Trans. Antennas Propag.*, vol. 54, no. 11, pp. 3151–3166, Nov. 2006, special issue on *Wireless Communications.*

[16] A. F. Molisch, "Ultrawideband propagation channels-theory, measurements, and modeling," *IEEE Trans. Veh. Technol.*, vol. 54, no. 5, pp. 1528–1545, Sep. 2005.

[17] A. Ridolfi and M. Z. Win, "Ultrawide bandwidth signals as shot-noise: a unifying approach," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 4, pp. 899–905, Apr. 2006.

[18] J.-Y. Lee and R. A. Scholtz, "Ranging in a dense multipath environment using an UWB radio link," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 9, pp. 1677–1683, Dec. 2002.

[19] W. Suwansantisuk, M. Z. Win, and L. A. Shepp, "On the performance of wide-bandwidth signal acquisition in dense multipath channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 5, pp. 1584–1594, Sep. 2005, special section on *Ultra-Wideband Wireless Communications–A New Horizon.*

[20] W. Suwansantisuk and M. Z. Win, "Multipath aided rapid acquisition: Optimal search strategies," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 174–193, Jan. 2007.

[21] Z. N. Low, J. H. Cheong, C. L. Law, W. T. Ng, and Y. J. Lee, "Pulse detection algorithm for line-of-sight (LOS) UWB ranging applications," *IEEE Antennas Wireless Propag. Lett.*, vol. 4, pp. 63–67, 2005.

[22] D. Dardari, C.-C. Chong, and M. Z. Win, "Threshold-based time-of-arrival estimators in UWB dense multipath channels," *IEEE Trans. Commun.*, vol. 56, no. 8, pp. 1366–1378, Aug. 2008.

[23] Z. Zhang, C. L. Law, and Y. L. Guan, "BA-POC-Based ranging method with multipath mitigation," *IEEE Antennas Wireless Propag. Lett.*, vol. 4, pp. 492–495, 2005.

[24] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, pp. 364–375, Sep. 2007.

[25] J. R. Foerster, "Channel modeling sub-committee report (final)."

[26] D. S. Heinz-Otto Peitgen, Hartmut Jürgens, *Chaos and Fractals: New Frontiers of Science*, 1st ed. New York: Springer-Verlag, 1992.