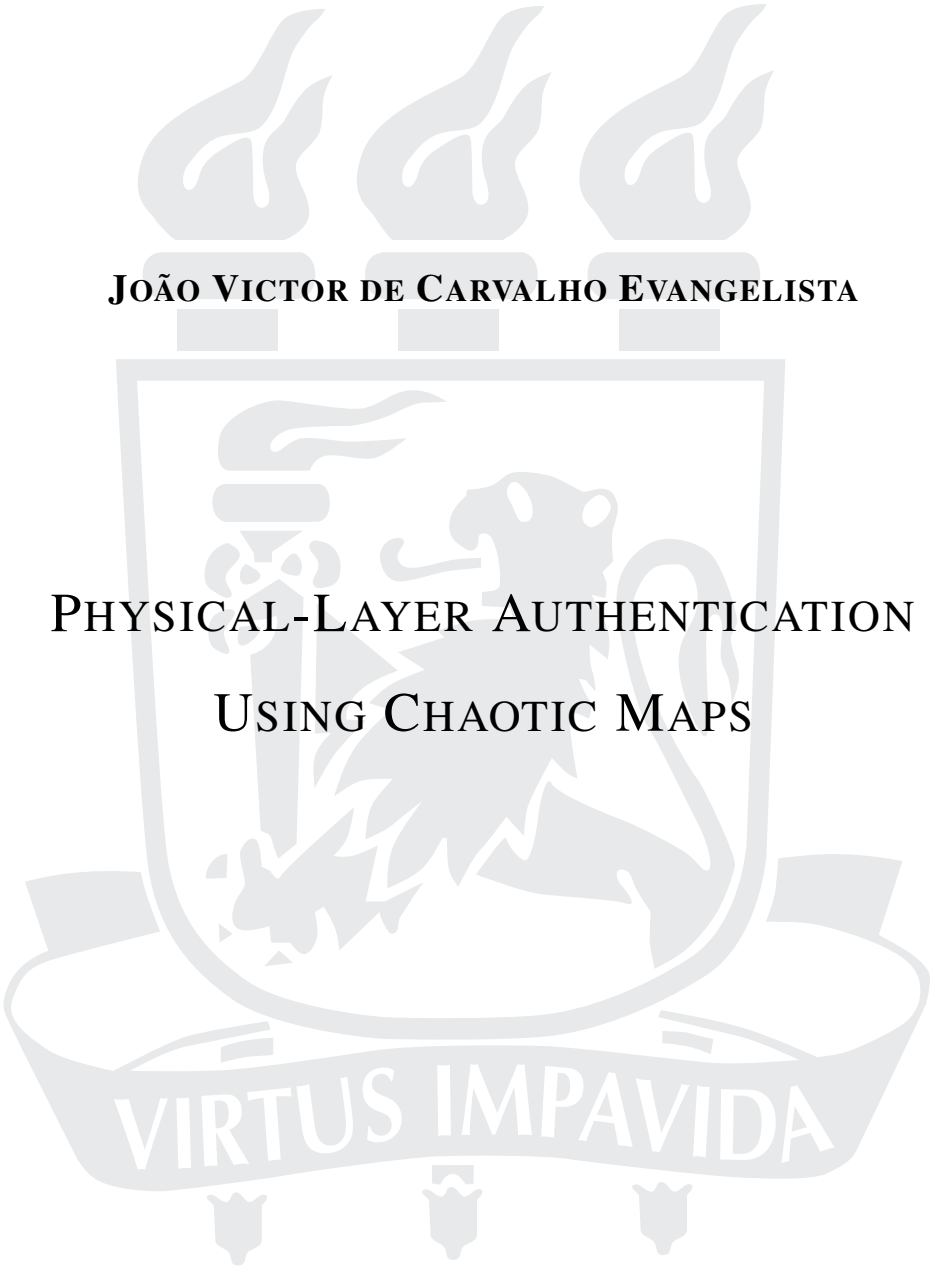
UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE TECNOLOGIA E GEOCIÊNCIAS

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA



JOÃO VICTOR DE CARVALHO EVANGELISTA

PHYSICAL-LAYER AUTHENTICATION USING CHAOTIC MAPS

Recife
2016

JOÃO VICTOR DE CARVALHO EVANGELISTA

PHYSICAL-LAYER AUTHENTICATION USING CHAOTIC MAPS

Dissertação submetida ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Pernambuco como parte dos requisitos para obtenção do grau de **Mestre em Engenharia Elétrica**.
Orientador: Prof. Daniel Pedro Bezerra Chaves.
Coorientador: Prof. Cecilio José Lins Pimentel
Área de Concentração: Comunicações

Recife
2016

Catalogação na fonte
Bibliotecária Valdicéa Alves, CRB-4 / 1260

E92p Evangelista. João Victor de Carvalho.
Physical-layer authentication Using chaotic maps/ João Victor de Carvalho Evangelista - 2016.
72folhas, Il.; e Tab.

Orientador: Prof. Dr. Daniel Pedro Bezerra Chaves.
Coorientador: Prof. Dr. Cecilio José Lins Pimentel.
.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2016.
Inclui Referências

Nota: Texto bilingue.

1. Engenharia Elétrica. 2. : Autenticação de mensagem. 3. Autenticação em camada física. 4. Mapas caóticos. 5. Probabilidade de outage. 6. Segurança incondicional. I. Chaves, Daniel Pedro Bezerra (Orientador). II. Pimentel, Cecílio José Lins(Coorientador). III. Título.

UFPE

621.3 CDD (22. ed.) BCTG/2016 - 283

Universidade Federal de Pernambuco
Pós-Graduação em Engenharia Elétrica

PARECER DA COMISSÃO EXAMINADORA DE DEFESA DE DISSERTAÇÃO DO MESTRADO ACADÊMICO DE

JOÃO VICTOR DE CARVALHO EVANGELISTA

TÍTULO

"PHYSICAL-LAYER AUTHENTICATION USING CHAOTIC MAPS"

A comissão examinadora composta pelos professores: DANIEL PEDRO BEZERRA CHAVES, DES/UFPE; CECILIO JOSÉ LINS PIMENTEL, DES/UFPE; JULIANO BANDEIRA LIMA DES/UFPE e JOSÉ SAMPAIO DE LEMOS NETO, DES/UFPE, sob a presidência do primeiro, consideram o candidato **JOÃO VICTOR DE CARVALHO EVANGELISTA** **APROVADO**.

Recife, 16 de agosto de 2016.

MARCELO CABRAL CAVALCANTI
Coordenador do PPGEE

DANIEL PEDRO BEZERRA CHAVES
Orientador e Membro Titular Interno

JOSÉ SAMPAIO DE LEMOS NETO
Membro Titular Externo

CECILIO JOSÉ LINS PIMENTEL
Coorientador e Membro Titular Interno

JULIANO BANDEIRA LIMA
Membro Titular Interno

RESUMO

A autenticação de mensagem, o que garante que uma mensagem recebida vem de seu aclamado remetente, é de fundamental importância para sistemas de comunicação seguros. Neste contexto, considera-se neste trabalho um sistema de autenticação em camada física empregando tags embutidos nas mensagens proporcionando um robusto método de autenticação. Este trabalho diverge de trabalhos anteriores na área no que se refere ao método de geração de tags. Enquanto os trabalhos anteriores utilizam métodos baseados em funções criptográficas de *hash* e na informação do estado do canal, nosso sistema emprega mapas caóticos unidimensionais para gerar os tags. Devido ao fato de que a informação sobre a condição inicial se perde ao longo de uma órbita caótica mostraremos que elas são fortes candidatas para o processo de geração de tags. Provamos que tags caóticos garantem um limitante inferior positivo na segurança incondicional do sistema. Adicionalmente, nós calculamos a probabilidade de sucesso de três tipos de ataque: de personificação, de substituição e de repetição. Para finalizar, analisamos como os parâmetros do sistema afetam essas probabilidades e algumas métricas de performance (taxa de erro por bit, probabilidade de interrupção e probabilidade de falso negativo) e os compromissos entre segurança e performance para prover um guia de projeto do sistema.

Palavras-chaves: autenticação de mensagem, autenticação em camada física, mapas caóticos, probabilidade de *outage*, segurança incondicional, taxa de erro por bit

ABSTRACT

Message authentication, which ensures that a received message comes from its acclaimed sender, is of fundamental importance for secure communication systems. We consider in this work a physical layer authentication system employing tag signals embedded in the message to provide a robust authentication method. This work diverges from previous work in the area when it comes to the tag generation method. While the previous works use methods based on cryptographic hash functions or on the channel side information our system employs unidimensional chaotic maps to generate these tags. Due to the loss of information about the initial condition of chaotic maps, we show that they are strong candidates for the tag generation process. We prove that chaotic tags provide a positive lower bound on the unconditional security of the system. Additionally, we calculate the probability of success for three possible attacks to the authentication system: impersonation, substitution and replay. Finally, we analyze how the system parameters affect these probabilities and some performance metrics (bit error rate, outage probability, probability of false negative) and explore the tradeoff between security and performance in order to provide guidelines to design the system.

Keywords: bit error rate, chaotic maps, message authentication, outage probability, physical layer authentication, unconditional security

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 The Authentication Problem

Authentication is the procedure to establish the authorship or the origin of a message. Nowadays, most people rely on digital means for communications purposes, from large corporations to regular users. In this context, message authentication plays a major role on making these communications reliable. Consider a system where two users who share a secret key (the legitimate users) are communicating with each other and an active adversary, who has read and write access to the channel, tries to disrupt the conversation by impersonating a legitimate user. The goal of the authentication system is to guarantee, based only on the common knowledge of the shared secret key, that a user is able to identify who originated the message.

Traditionally, authentication is deployed in higher layers of the network [1]. The legitimate users generate an authentication tag, which are binary sequences generated based on the secret key using a cryptographic function, and send them along with their messages. The adversary must not be able to discover the secret key by observing the tag. Most cryptographic functions rely on the hardness of a problem (computing discrete roots or elliptic curve discrete logarithms) to guarantee that. However, this hardness comes from the fact that all known algorithms to solve these problems run in super-polynomial time, so, they only provide computational security. However, if better algorithms are developed or better hardware becomes available solving these problems in feasible time may become possible. In order to provide an additional layer of security, physical layer authentication protocols that explore the stochastic properties of the communication channel were introduced [2–11]. These protocols incorporate the intrinsic probabilistic nature of the physical channel in order to provide

unconditional security [12].

1.2 Physical Layer Authentication

One approach for physical layer authentication is similar to the methods deployed in the higher layers. Authentication tags are generated, where the tags are waveforms transmitted with the messages, based on the knowledge of the shared secret key [8, 9, 11, 13]. These systems exploit the channel noise to hide the information about the key from the adversary and the main security metric is how much information the adversary has about the key. Another approach to the problem is to explore the uniqueness of the channel between the legitimate users [3–7]. In this approach the security performance is assessed based on the probability that a fraudulent message is detected.

In [3], a physical layer authentication system that uses the channel response as an identifier of the legitimate transmitter is proposed. This system relies on the fact the channels decorrelate quickly with distance. The channel is assumed to be invariant. The system can identify messages sent by the adversary when the quality of the channel between the legitimate users is better than the channel between the receiver and the adversary. A similar method is proposed in [4], however, a time-variant channel is assumed and the probability of identifying messages sent by the adversary is evaluated in an indoor channel modeled using ray tracing techniques. The problem of identifying channel between the legitimate users is modeled as a hypothesis test. Similar to [3], the low probability on detecting fraudulent messages when the legitimate channel is poor persists. An extensive analysis on how channel parameters affect the probability is developed. In [5] an adaptive threshold is proposed for the hypothesis tests, resulting in a higher probability of identifying the adversary when the channel between the legitimate users is poor. In [6] a new method of obtaining the channel response is proposed. This new method result in a higher probability of detecting the adversary for channels with small Doppler spread. While in [7], an authentication system where the legitimate receiver sends a challenge and the legitimate transmitter, who must respond this challenge correctly to be authenticated, based on the reciprocity of the phase response is proposed. An analysis of the adversary's attacking strategies is developed, however, only passive attacks are considered. In the works mentioned so far the probability of detecting the messages sent by the adversary depended on the quality of the channel between the legitimate users being better that the channel between the adversary and a legitimate user. Additionally, none of these work evaluated the probability of success of active attacks.

In [8], in a work precursor to the tag embedding methods, two methods to modify the OFDM

waveform in a way that reflect the common knowledge of the key are presented and the effects on the bit error rate are evaluated. In [9, 13] an authentication system using tag signals generated by keyed hash functions embedded in the messages is proposed and implemented. The effects of the authentication system on the bit error rate and on the outage probability are studied. The uncertainty of the key given noisy observations of the tag is used as a security metric. The resulting system has a higher equivocation if the ratio between the tag power and the noise power is low, however, when the noise power is reduced, the equivocation approaches zero. A discussion of the vulnerability of the system against attacks is developed, however, an analytic approach to the probability of success of the attacks is missing. A system that uses the knowledge of previous channel responses to design the tag waveform is proposed in [11] . This technique mitigates the effects of the authentication system on the bit error rate, but no security analysis is conducted. In comparison with authentication systems based on the channel response, those employing authentication tags are more flexible. By changing the properties of the tag signal it is possible to improve the system security at cost of message detection performance. However, the system security is still dependent on the noise power. Moreover, an analysis on different attack strategies is missing.

In this work, we propose a tag generation method that provides a lower bound in the uncertainty about the key that depends only on system parameters. Additionally we develop a detailed analytical analysis on the probability of success of attacks to the system.

1.3 Chaos Applied to Communications

Dynamical systems are described by how the system evolves with time given an initial condition. Chaotic dynamical systems are characterized by an aperiodic long-term unpredictable behavior generated by a nonlinearity. The key property of chaotic maps is their sensitivity to initial conditions. Two initial conditions separated by an infinitesimal distance produce uncorrelated long-term behaviors [14, 15]. Initially chaos theory was concerned to describe the behavior of mechanical, biological and meteorological systems, however, in 1990 Ott, Grebogy and Yorke [16] published a paper on chaos control. This paper arose an interest to the application of chaos control to modulate information in chaotic signals [17, 18]. Due to its characteristics, chaotic systems in the context of communications have been proposed as:

- ▷ Multiple access spread spectrum modulations [18].
- ▷ Coherent (Chaotic Shift Keying) [17] and non-coherent (Differential Chaotic Shift Keying)[18]

modulation schemes.

▷ Pseudo random number generation [19].

In this work we propose a novel application for chaotic unidimensional maps, we use sequences generated by such maps as authentication tags for physical layer authentication systems. The properties of chaotic maps are explored to provide security independent of the channel noise.

1.4 Objectives and Contributions

The objective of this work are:

▷ Apply the results of previous works on the probabilistic properties of chaotic systems and the information-theoretic analysis of chaotic sequences, to evaluate the information flow on chaotic sequences.

▷ To propose a physical layer authentication system that employs chaotic generated tags. To the best of our knowledge this the first time that chaotic maps are employed in physical layer authentication systems.

▷ To derive analytical expressions for the probability of success of attacks to the system.

▷ To explore the tradeoffs in the performance by varying the system parameters.

The main contributions of this work are:

▷ A method to estimate the loss of information about the initial condition of a chaotic map is given in Chapter 2.

▷ A method to generate chaotic tags is proposed in Section 3.4.

▷ An information-theoretic analysis of the conditional entropy of the key is developed and we prove that for chaotic generated tags the unconditional security of the key given observations of the tag is higher than zero even in a noiseless environment. An expression for the unconditional security of the system is given by (3.15). To the best of our knowledge this is the first work where unconditional security is obtained independently of the noise power.

▷ We consider active attacking strategies for the adversary and the probability of success of impersonation, substitution and replay attacks are given respectively by (3.23), (3.25) and (3.26).

▷ An extensive analysis on how the authentication system affects the bit error rate and the outage probability is developed, and the tradeoffs between the system parameters are evaluated.

1.5 Organization of the Dissertation

In Chapter 1 the authentication problem is qualitatively defined, a brief literature review on physical layer authentication and chaos applied to communications is presented and the objectives and contributions of this work are summarized.

In Chapter 2 basic definitions about chaos are given. A study on the evolution of probability densities under chaotic maps and on the information flow in chaotic orbits is presented.

In Chapter 3 basic concepts of security of communication systems are discussed, a novel method of chaotic tag generation is presented. The probability of impersonation, substitution and replay attacks are calculated. A study of the equivocation of the key for a chaotic generated tag is presented and the unconditional security is derived.

In Chapter 4 effects of the authentication system on the bit error rate and the outage probability are assessed and an analysis of the system tradeoffs is developed.

In Chapter 5 all the conclusions derived throughout the work are summarized and the directions for future works are presented.

CHAPTER 2

ANALYSIS OF CHAOTIC MAPS

A chaotic dynamical system is characterized by an aperiodic long-term unpredictable behavior generated by a certain nonlinearity. At a first glance it may be perplexing that a deterministic system defined by difference equations can be unpredictable. The key to understand this concept is to understand its sensitivity to initial conditions. Two initial conditions separated by an infinitesimal distance produce uncorrelated long-term behaviors [14, 15]. Due to this inherent property chaotic systems have been proposed for several applications in securing communications systems [20, 21].

In this chapter the foundations for the use of unidimensional chaotic maps as tag generators for physical layer authentication system are laid. A requirement for a good tag generation system is that it must be hard for an eavesdropper that observes the tag to figure out which key gave origin to that tag. In Section 2.1 the basic definitions of chaos are presented, in Section 2.2 a study on how a density function is affected by successive applications of a chaotic function is developed, in Section 2.3 a description on how information flows through a chaotic orbit is derived and in Section 2.4 a summary of the conclusions of this chapter are presented.

2.1 Overview of Chaotic Maps

A dynamical system consists of a set of possible states, and a rule that determines the next state depending upon the past states. In a continuous time framework the state is given by the values of the state variables and the rule is given by the differential equations governing the system. This work is concerned only with discrete time systems with their rule defined by one dimensional difference equations. Additionally, only chaotic maps which have a domain equal to it's image are of

concern. These kind of systems are called one-dimensional maps. Along this chapter the tools used to investigate such systems are described and a formal definition of chaotic one-dimensional maps is derived.

2.1.1 Basic Definitions

Given that $x[n]$ is the value of the state variable x at discrete time n, the value of $x[n+1]$ is obtained by the forward iteration of the chaotic map given by

$$x[n+1] = f(x[n]) \text{ , for } n = 0, 1, 2, \ldots, \infty, \tag{2.1}$$

where $f : A \rightarrow A$ is a suitable nonlinear and noninvertible function. To determine the state of the system at $n+2$ we have $x[n+2] = f(x[n+1]) = f(f(x[n])) \stackrel{\triangle}{=} f^2(x[n])$, so $f^r(\cdot)$ is the r-th composition of $f(\cdot)$ with itself. So to know the value assumed by the state variable at any time we only need to know its initial condition $x[0]$. The sequence of points generated by successive applications of the map starting from point $x[0]$ is known as the trajectory or the orbit of $x[0]$ under $f(\cdot)$ and is given by the set of points $\{x[0], f(x[0]), f^2(x[0]), f^3(x[0]), ...\}$.

2.1.2 Lyapunov Exponent and the Chaotic Behavior

Chaotic maps are known to generate uncorrelated, noise-like, aperiodic real valued sequences [14, 15]. But how to distinguish a stable dynamical system from a chaotic one? The defining property of chaotic systems is that they are deeply sensitive to the initial condition of the system, meaning that infinitesimally close initial conditions generate low correlated sequence. A widely used metric to measure this sensitivity to initial conditions and determine whether the map evolves to a stable or chaotic behavior is the **Lyapunov exponent**.

Given some initial condition $x[0]$ let $x[0] + \delta_0$ be a nearby point within the map's domain, where δ_0 is infinitesimally small. Let δ_n be the separation between the output of two equal maps after n iterates, the first map having $x[0]$ as its initial condition and the second having $x[0] + \delta_0$. Assuming

there is a exponential relationship between δ_n and δ_0 we have

$$\begin{aligned} |\delta_n| &= |\delta_0|\ \exp(n\lambda_n) \\ \ln(|\delta_n|) &= \ln(|\delta_0|) + n\lambda_n \\ \lambda_n &= \frac{1}{n}\ln\left(\left|\frac{\delta_n}{\delta_0}\right|\right) \\ &= \frac{1}{n}\ln\left(\left|\frac{f^n(x[0]+\delta_0) - f^r(x[0])}{\delta_0}\right|\right) \text{ , taking the limit } \delta_0 \to 0 \\ \lambda_n &= \frac{1}{n}\ln(|(f^r(x[0]))'|), \end{aligned} \tag{2.2}$$

where $f^r(\cdot)$ is a r-fold composition of $f(\cdot)$ with itself and $(f(x))'$ denotes the first derivative of $f(x)$. By using the derivation chain rule we have that

$$(f^k(p_k))' = \prod_{i=1}^{k} f'(p_i). \tag{2.3}$$

Substituting (2.3) in (2.2) and taking the limit of n to infinity we obtain

$$\begin{aligned} \lambda &= \lim_{n\to\infty}\frac{1}{n}\ln\left(\left|\prod_{i=0}^{n-1} f'(x[i])\right|\right) \\ &= \lim_{n\to\infty}\left[\frac{1}{n}\sum_{i=0}^{n-1}\ln(|f'(x[i])|)\right]. \end{aligned} \tag{2.4}$$

If this limit exists λ is called the Lyapunov exponent [15]. As λ is the divergence rate between two sequences originated by infinitesimally close initial conditions we conclude that for chaotic maps $\lambda > 0$ while for stable systems $\lambda \leq 0$. The positive Lyapunov indicates that chaotic maps are sensitive to initial condition. Figure 2.1(a) shows two orbits of a chaotic map generated by two initial conditions separated by 10^{-6}, with initial conditions $x_1[0] = 0.1$ and $x_2[0] = 0.1 + 10^{-6}$. From this figure it is seem that after a few iterations the orbits diverge assuming completely distinct dynamical behavior. Figure 2.1(b) shows the absolute value of the difference between these two orbits.

2.2 Chaotic Generated Probability Densities

Due to the noise-like behavior of chaotic sequences it is hard to obtain useful information about the behavior of the sequences generated by a chaotic map from the observation of the time evolution. Despite being deterministic and defined by difference equations a chaotic map with uncertain initial condition can be characterized as a stochastic process, where the orbit of each initial condition under the map is a realization of the process. Thus, the set of all possible sequences is the ensemble of the process and the output after each iteration is a random variable, given that the initial condition is

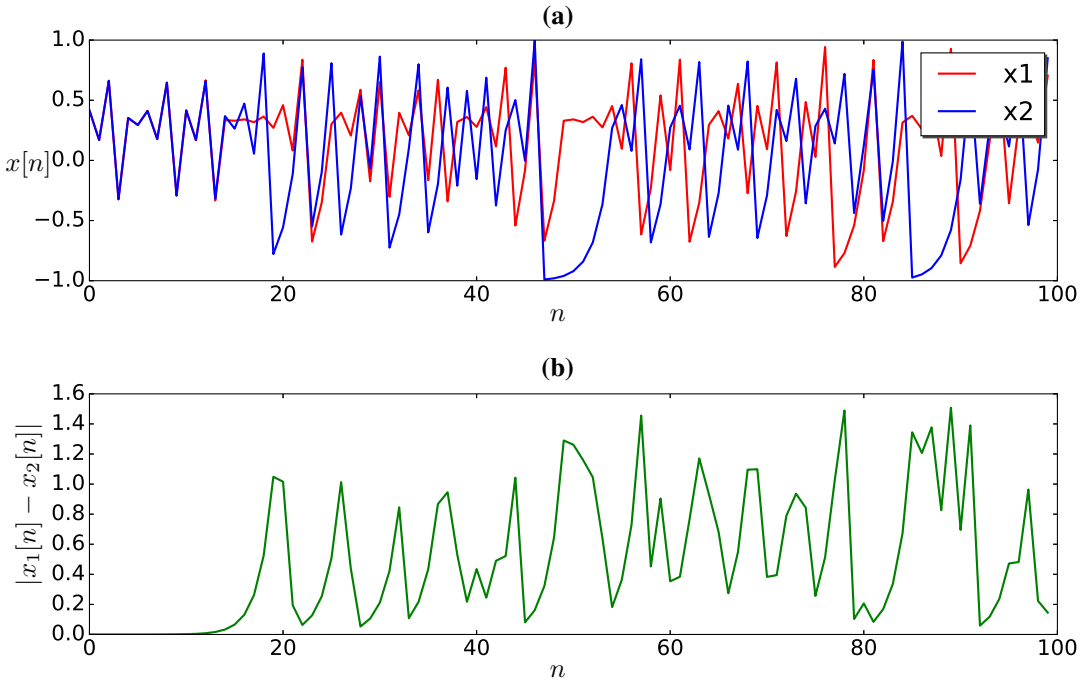


Figure 2.1: *(a) Two orbits of a chaotic map generated by two initial conditions separated by* 10^{-6} *(b). The absolute value of the difference between the distinct orbits.*

unknown. The analysis presented in this section is based on [22] and [23] and is necessary for a good understanding of the rest of the chapter.

2.2.1 Time Evolution of Chaotic Probability Densities

In order to fully characterize a chaotic map it is important to understand how the probability density function (PDF) of the initial conditions evolve after successive iterations of the map. Let $f : A \to A$ be a chaotic map and A be an one dimensional interval, if we pick an initial condition for the map from an the interval A distributed according to a PDF $p_0(x)$ it is important to know the PDFs $p_1(x), p_2(x) \cdots$ after successive iterations of the map.

In order to understand how the PDFs of the map evolve, we must establish the relationship between the PDFs of subsequent iterations $p_i(x)$ and $p_{i+1}(x)$. We define the counterdomain of an interval Δ as $f^{-1}(\Delta)$ meaning that

$$x[i+1] \in \Delta \quad \iff \quad x[i] \in f^{-1}(\Delta). \tag{2.5}$$

Thus the events that $x[i+1]$ belongs to Δ and that $x[i]$ belongs to $f^{-1}(\Delta)$ are equiprobable. Using this relationship we obtain

$$\int_{\Delta} p_{i+1}(u)du = \int_{f^{-1}(\Delta)} p_i(u)du. \tag{2.6}$$

Let $\Delta = [a, x]$ where a is a constant and x a variable, if we derive both sides of (2.6) we obtain

$$p_{i+1}(x) = Pp_i(x) = \frac{d}{dx}\int_{f^{-1}([a,x])} p_i(u)du, \tag{2.7}$$

where P is the Froebenius-Perron operator (FP operator). If $f(\cdot)$ is a monotone function we have that $f^{-1}(\Delta) = [f^{-1}(a), f^{-1}(x)]$, thus

$$p_{i+1} = Pp_i(x) = \frac{d}{dx}\int_{f^{-1}(a)}^{f^{-1}(x)} p_i(u)du = p_i(f^{-1}(x))\left|\frac{d}{dx}f^{-1}(x)\right|, \tag{2.8}$$

so $p_{i+1}(x)$ does not depend on the choice of a. The FP operator maps the infinite space of all one dimensional Lebesgue integrable functions of the interval A on itself. Each one dimensional map has its correspondent FP operator and for those which the FP operator has a fixed point (maps a density on itself) the density correspondent to the fixed point is said to be the invariant density of the map $p_*(x)$ [22]. Qualitatively this means that for any $p_0(x)$ the PDFs of the following iterations will inevitably converge to $p_*(x)$. As shown by (2.8) determining $p_{i+1}(x)$ given $p_i(x)$ involves solving a functional equation, which for most cases it is not a straight forward problem.

2.2.2 A Special Case: Markov Maps

Definition 2.2.1 – Indicator Function

Given a set Δ the indicator function is defined as

$$1_\Delta(x) = \begin{cases} 1, \textit{ if } x \in \Delta \\ 0 \textit{ otherwise.} \end{cases} \tag{2.9}$$

□

Definition 2.2.2 – Partition

Given an interval A, the set $\{A_b\}_{i=0}^{B-1}$ is a partition of A if the following holds

- ▷ $A_i \cap A_j = \emptyset$ *if* $i \neq j$.
- ▷ $A_b \subset A$, *for all* b.
- ▷ $\bigcup_{b=0}^{B-1} A_b = A$.

□

A set of chaotic maps are of special interest, the piecewise-linear, eventually expanding Markov maps [23, 24], from now on simply referred as Markov maps for the sake of simplicity. They are of special interest because it is possible to obtain their statistical properties in a closed form [25].

Definition 2.2.3 – Markov Maps

Let $f : A \to A$ be the function that define a Markov map, the following holds:

1. *There is a partition $\{A_b\}_{b=0}^{B-1}$ such that restricted to each interval A_b the map is continuous and has constant derivative. Thus $f(x)$ can be rewritten as $f(x) = \sum_{i=0}^{B-1} f_b(x)1_{A_b}(x) = \sum_{b=0}^{B-1}(d_b x + c_b)1_{A_b}(x)$, where $f_b(x) = d_b x + c_b$.*
2. *$f(A_j) = \bigcup_i A_i$.*
3. *$f(\cdot)$ has eventually expanding property, meaning that there is an integer k, such that $\inf_{x\in A} |\frac{d}{dx} f^k(x)| > 1$, where inf denotes the infimum.* □

Thus, finding the FP operator of a Markov map consists on solving the following functional equation

$$p_{i+1} = \sum_{b=0}^{B-1} \frac{p_i(f_b^{-1}(x))1_{A_b}(x)}{|d_b|} = \sum_{b=0}^{B-1} \frac{p_i\left(\frac{x-c_b}{d_b}\right)1_{A_b}(x)}{|d_b|}. \tag{2.10}$$

It is a known result from [25] that the invariant density of a Markov map is piecewise constant, so the invariant density of the map can be represented by a B-dimensional vector $\mathbf{p}_* = \begin{bmatrix} p_*^0 & p_*^1 & \cdots & p_*^{B-1} \end{bmatrix}$ where

$$p_*(x) = \sum_{b=0}^{B-1} p_*^b 1_{A_b}(x). \tag{2.11}$$

Definition 2.2.4 – Index Set

Let $\mathcal{I}_k$ be an index set, than the following holds:

$$\mathcal{I}_k = \{b | A_b \subset f(A_k)\}. \tag{2.12}$$

□

So, the problem to find the invariant density can be reduced to a finite dimensional one and the FP operator can be represented by a $B \times B$ FP matrix $\mathbf{P}$ with components

$$P_{i,j} = \begin{cases} \frac{1}{|d_j|} \text{ , if } i \in \mathcal{I}_j \\ 0 \text{ , otherwise.} \end{cases} \tag{2.13}$$

In [26] it is shown that the matrix $\mathbf{P}$ is diagonally similar to a column stochastic matrix, hence, it has the same eigenvalues as some stochastic matrix. In [27] the Froebenius theorem states that all stochastic matrix have a unitary eigenvalue, consequently so does $\mathbf{P}$, thus, determining the invariant density vector of a map consists on finding the eigenvector, denoted by $\mathbf{p}_*$, correspondent to the unitary eigenvalue

$$\mathbf{P}\mathbf{p}_* = \mathbf{p}_*. \tag{2.14}$$

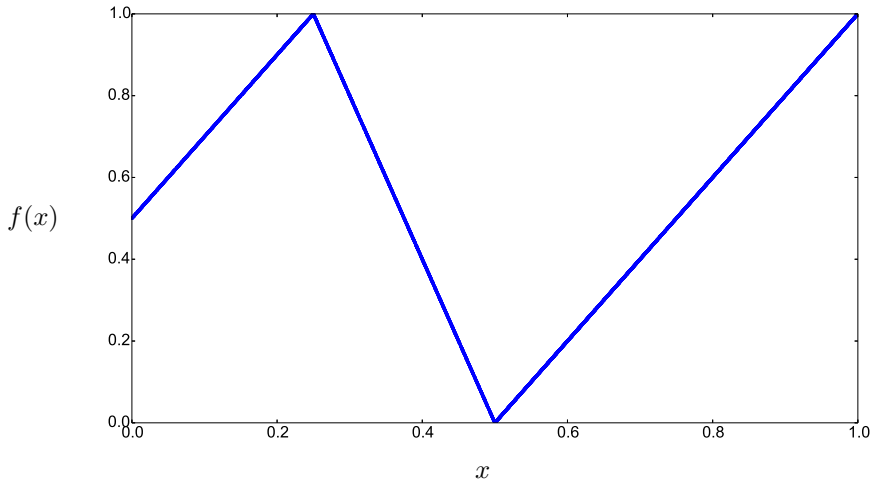


Figure 2.2: *Map given by (2.16).*

The invariant density is obtained from the vector as

$$p_*(x) = \frac{1}{\sum_{i=0}^{B-1} p_*^i |A_i|} \sum_{i=0}^{B-1} p_*^i 1_{A_i}(x), \tag{2.15}$$

where $|A_i|$ represents the length of the interval A_i.

Example

In order to illustrate the procedure consider the chaotic Markov map $f : [0,1] \to [0,1]$ given by

$$f(x) = \begin{cases} 2x + \dfrac{1}{2}, \text{, for } x \in [0, 0.25) \\ -4x + 2, \text{, for } x \in [0.25, 0.5) \\ 2x - 1, \text{, for } x \in [0.5, 1]. \end{cases} \tag{2.16}$$

In order to guarantee that the map has chaotic behavior its Lyapunov exponent must be calculated. Using a numerical method detailed in [15] we obtain $\lambda = 0.83$, which is positive, so the map is chaotic. Its curve is depicted in Figure 2.2. A suitable Markov partition for this maps is $\{[0, 0.25), [0.25, 0.5), [0.5, 1]\}$ and the correspondent index sets are $\mathcal{I}_0 = \{2\}$, $\mathcal{I}_1 = \{0, 1, 2\}$ and $\mathcal{I}_2 = \{0, 1, 2\}$. Thus, the FP matrix is

$$\mathbf{P} = \begin{bmatrix} 0 & \frac{1}{4} & \frac{1}{2} \\ 0 & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{2} \end{bmatrix}, \tag{2.17}$$

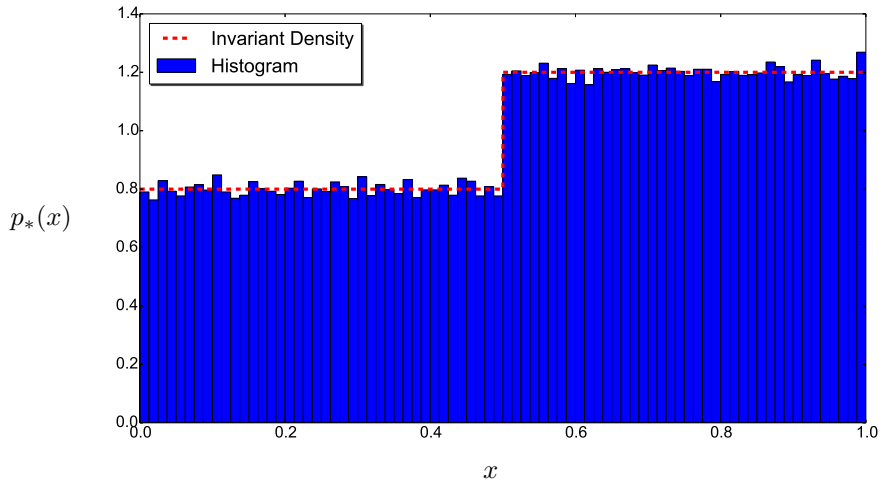


Figure 2.3: *Comparison between the normalized histogram and the analytical invariant density of the map given by (2.16).*

and the eigenvector corresponding to the unitary eigenvalue is

$$\mathbf{p}_* = \begin{bmatrix} \frac{2}{3} & \frac{2}{3} & 1 \end{bmatrix}^T . \tag{2.18}$$

Hence, the invariant density calculated by the proposed method is

$$p_*(x) = \begin{cases} \dfrac{4}{5} \text{ , for } x \in [0, 0.5) \\ \dfrac{6}{5} \text{ , for } x \in [0.5, 1]. \end{cases} \tag{2.19}$$

Figure 2.3 shows a comparison between the analytically obtained invariant density and the normalized histogram of an orbit of length 10^6.

2.2.3 Approximation of the Invariant Density for a Broader Class of Maps

The method described in Subsection 2.2.2 determines analytically the invariant density for Markov maps, the same method can be used to approximate the invariant density for any eventually expanding maps [23].

Definition 2.2.5 – Eventually Expanding Map

Given a eventually expanding chaotic map $f : A \to A$ the following holds:

1. *There is a partition $\{A_b\}_{b=0}^{B-1}$ such that restricted to any A_b, $f(\cdot)$ is monotonic, continuous and differentiable.*
2. *$\frac{1}{f'(x)}$ is of bounded variation.*

3. *$f(\cdot)$ has eventually expanding property, meaning that there is an integer k and a number $\Gamma > 1$, such that $\left|\frac{d}{dx}f^k(x)\right| > \Gamma$ wherever the derivative exists.* □

The theorem by Wong detailed in [28] guarantees that every eventually expanding map possess an invariant density. The approximation method consists in obtaining a Markov approximation for the eventually expanding map and then applying the technique presented in Section 2.2.2. The eventually expanding map domain must be partitioned by a Markov partition $\{Q_i\}$. Restricted to each interval $Q_i = [q_i, q_{i+1})$, the map $f(\cdot)$ is continuous, differentiable and monotonic. Additionally, as any Markov partitions we have that $f(Q_i) = \bigcup_j Q_j$ for all i. Then the Markov approximation $\hat{f}(\cdot)$ is given by

$$\hat{f}(x) = \sum_i \hat{f}_i 1_{Q_i}(x) = \sum_i \left(\frac{f(q_{i+1}) - f(q_i)}{q_{i+1} - q_i} + c_i \right) 1_{Q_i}(x). \tag{2.20}$$

Now an algorithm to obtain a Markov partitioning for the approximation with as many partitions as wanted is presented. First select an initial set of partition points θ_0 with three partition points determining two intervals, $Q_0 = [q_0, q_1)$ and $Q_1 = [q_1, q_2)$, such that the partitions are Markovian with respect to $f(\cdot)$, which implies that $f(q_i) \in \theta_0 \; \forall \; q_i \in \theta_0$. Then, we can obtain a larger set of partition points $\theta_1 = \theta_0 \cup f^{-1}(\theta_0)$, which is Markovian because $f(\theta_1) = f(\theta_0) \cup \theta_0$. Thus, a set of Markov partition points is obtained through the iterative equation

$$\theta_{k+1} = \theta_k \cup f^{-1}(\theta_k). \tag{2.21}$$

After obtaining an appropriate set of partition points determining (2.20) an approximate FP matrix $\hat{\mathbf{P}}$ can be obtained using (2.13) and the approximate invariant density vector $\hat{\mathbf{p}}_*$ is the eigenvector with unitary eigenvalue with respect to the transformation $\hat{\mathbf{P}}$. Finally, the approximated invariant density is obtained by direct application of (2.15).

Example

Consider the piecewise smooth chaotic map $f : [0, 1] \to [0, 1]$, from now on referred as the PWS map, given by the equation

$$f(x) = \begin{cases} \dfrac{9x}{3x+2} \text{ , for } x \in [0, 1/3) \\ \dfrac{6x-2}{x+3} \text{ , for } x \in [1/3, 1]. \end{cases} \tag{2.22}$$

The curve of the map is seem in Figure 2.4. The derivative of the PWS map is given by

$$\frac{d}{dx}f(x) = \begin{cases} \dfrac{18}{(3x+2)^2} \text{ , for } x \in [0, 1/3) \\ \dfrac{20}{(x+3)^2} \text{ , for } x \in [1/3, 1]. \end{cases} \tag{2.23}$$

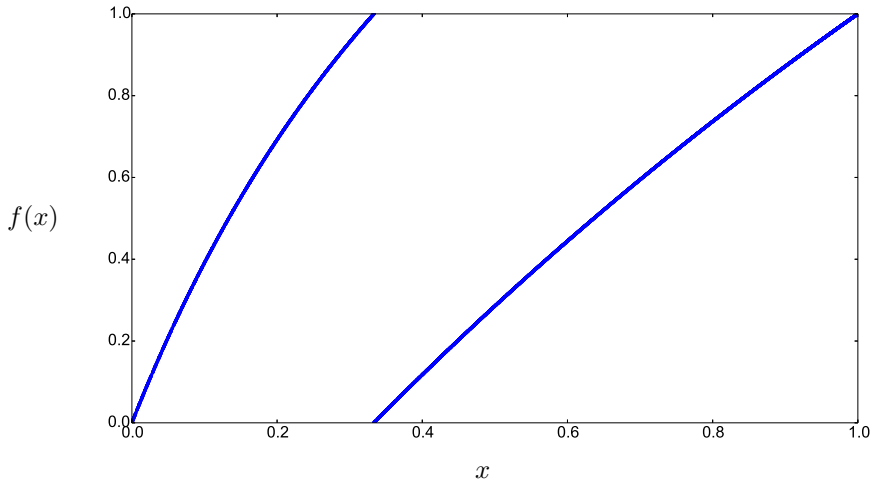


Figure 2.4: *PWS chaotic map from the example.*

Thus, confined to its domain $[0, 1]$, the map is indeed eventually expanding and its inverse derivative is of bounded variation. An obvious initial set of partition points is $\theta_0 = \{0, \frac{1}{3}, 1\}$. This set of partition points can be refined depending on how good the FP operator and the invariant density must be approximated. Figure 2.5 compares the approximation with the normalized histogram of the map for θ_2, which consists of 8 intervals, while Figure 2.6 compares the histogram with the approximation for θ_{10}, which consists of 2048 intervals. If a more accurate approximation is needed a finer set of partition points can be obtained by successive application of (2.21). It is worth noting that for a set of partition points θ_k the complexity on determining the eigenvectors of the approximate FP matrix grows exponentially with k. For example approximating the invariant density of the PWS map using θ_{15} consists on finding the eigenvalues and eigenvectors of a 65536×65536 matrix.

2.3 Information Flow on Markov Maps

In this section, chaotic maps are analyzed under an information theoretic framework, and we pose the following question: how much information about the initial condition x_0 of a chaotic map is available only by observing its r-th iterate x_r?

2.3.1 Stretching and Folding of the Phase Space

In order to understand how iterations of chaotic maps incur in an increase of the uncertainty we have to understand two phenomena inherent to these maps: the stretching and the folding of the phase space. When a region of the input is mapped on larger region of the output it means that the phase

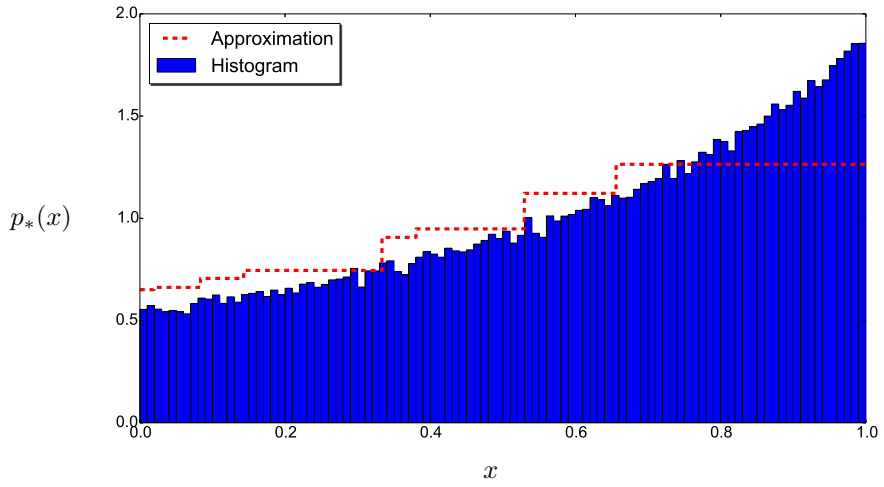


Figure 2.5: *Approximation of the invariant density of the PWS map using the set of partition points* θ_2.

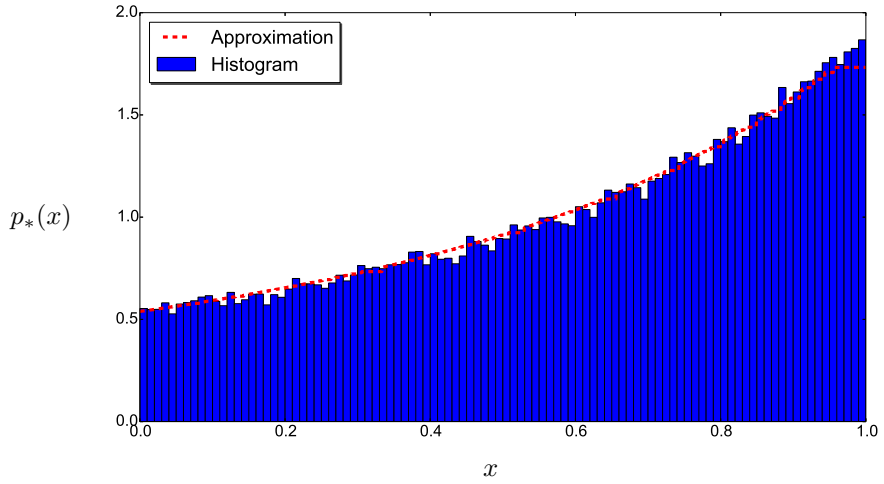


Figure 2.6: *Approximation of the invariant density of the PWS map using the set of partition points* θ_{10}.

state has been stretched. By folding of the phase space we mean the event that two or more input values map to the same output value, thus the map is not injective. By definition, chaotic maps are automorphisms, meaning that they map a region on itself. Thus, the folding of the phase space is a direct consequence from the stretching. This suggests that the stretching and the folding generate an uncertainty on the region of the initial condition that originated a certain chaotic orbit.

2.3.2 Mutual Information

Mutual information [29] measures the amount of information (usually in bits) shared between two random variables. Consider that the r-th point $x[r]$ of a chaotic orbit under $f : A \to A$ with

unknown initial condition is a continuous random variable, with PDF $p_r(x)$. We conduct a discrete analysis [30] from a partition of the function domain A in 2^K intervals $A_i = [a_i, a_{i+1})$ with $i = 0, 1, 2, \cdots, 2^K - 1$, each with length $\frac{|A|}{2^K}$. Let x_r be a discrete random variable indicating which of the intervals A_i does $x[r]$ belongs to, then we have that the probability mass function (PMF) of x_r is given by

$$P_r(m) \stackrel{\triangle}{=} \Pr(x_r = m) = \int_{A_m} p_r(x)dx, \tag{2.24}$$

for $m = 0, 1, 2, \cdots, 2^K - 1$. Thus, assuming that the PDF of the initial condition $p_0(x)$ is known, we have that

$$P_0(m) = \int_{A_m} p_0(x)dx. \tag{2.25}$$

Hence, the PDF of any iterations of the map is obtained as

$$P_r(m) = \int_{A_m} P^r p_0(x)dx, \tag{2.26}$$

where P^r is the r-th composition of the FP operator with itself. Hence, the entropy of x_r is given by

$$H(x_r) = -\sum_{m=0}^{2^K-1} P_r(m) \log_2 P_r(m). \tag{2.27}$$

The mutual information between the x_r and x_0 is given by

$$I(x_r; x_0) = H(x_r) - H(x_r|x_0). \tag{2.28}$$

The derivation of $H(x_r|x_0)$ is described next.

Derivation of $H(x_r|x_0)$

In order to evaluate the conditional entropy $H(x_r|x_0)$ we follow the approach in [30] and first consider the derivation of $H(x_1|x_0)$. Assuming that the map function $f : A \to A$ is piecewise smooth, for a large value of 2^K it is reasonable to assume that the derivative of the map in the m-th partition, $d(m)$, is constant and can be approximated to

$$d(m) \approx \frac{d}{dx} f\left(\frac{a_m + a_{m+1}}{2}\right). \tag{2.29}$$

So, an interval of length $\frac{|A|}{2^K}$ is mapped in a region of length $\frac{|A|d(m)}{2^K}$. We must evaluate the conditional entropy for two situations: $d \leq 1$ and $d > 1$.

▷ $d(m) \leq 1$: As depicted in Figure 2.7, for a fixed initial partition, the initial partition is spread to up to two partitions. Let the mapping of the initial partition cover a fraction of a partition (I) of length $\frac{|A|\epsilon}{2^K}$ and a fraction of another partition (II) of length $\frac{|A|}{2^K}(d(m) - \epsilon)$, where $0 \geq$

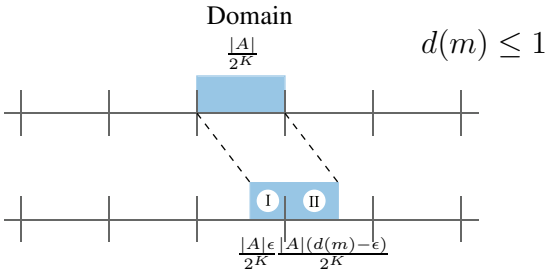


Figure 2.7: *Mapping of a partition for* $d(m) < 1$.

$\epsilon < d(m)$ is a uniformly distributed random variable, as depicted in Figure 2.7. We have that $\Pr(x[1] \in \text{I}|x_0 = m)$ is equal to $\frac{|A|\epsilon/2^K}{|A|d(m)/2^K} = \frac{\epsilon}{d(m)}$ and $\Pr(x[1] \in \text{II}|x_0 = m)$ is given by $\frac{|A|(d(m)-\epsilon)/2^K}{|A|d(m)/2^K} = 1 - \frac{\epsilon}{d(m)}$, thus

$$H(x_1|x_0 = m, \epsilon) = -\frac{\epsilon}{d(m)} \log_2 \left(\frac{\epsilon}{d(m)}\right) - \left(1 - \frac{\epsilon}{d(m)}\right) \log_2 \left(1 - \frac{\epsilon}{d(m)}\right). \tag{2.30}$$

If the conditional entropy is averaged over ϵ, and assuming that ϵ is uniformly distributed, we obtain the average conditional entropy for a fixed initial partition we have

$$H(x_1|x_0 = m) = \frac{d(m)}{2 \ln 2}. \tag{2.31}$$

▷ $d(m) > 1$: The output is spread from $\lfloor d(m) \rfloor$ up to $\lfloor d(m) \rfloor + 2$ partitions, where at least $\lfloor d(m) \rfloor - 1$ partitions are entirely covered (I) while up to two partitions are partially covered (II). Figure 2.8 depicts a few possible arrangements for $d(m) > 1$. Thus, $\Pr(x[1] \in \text{I}|x_0 = m)$ is $\frac{|A|/2^K}{|A|d(m)/2^K} = \frac{1}{d(m)}$ while the probabilities of ending in one of the partially covered partitions are $\frac{|A|\epsilon/2^K}{|A|d(m)/2^K} = \frac{\epsilon}{d(m)}$ and $\frac{|A|(d(m)-\epsilon)/2^K}{|A|d(m)/2^K} = 1 - \frac{\epsilon}{d(m)}$, where $0 \leq \epsilon < 1$ is a uniformly distributed random variable. So, the average conditional entropy for a fixed initial partition is

$$H(x_1|x_0 = m) = \frac{\lfloor d(m) \rfloor - 1}{d(m)} \log_2 \left(\frac{1}{d(m)}\right) + \frac{1}{2d(m) \ln 2}. \tag{2.32}$$

Thus the average conditional entropy after one iteration is obtained as

$$H(x_1|x_0) = \sum_{m=0}^{2^K - 1} P_0(m) H(x_1|x_0 = m), \tag{2.33}$$

where $P_0(m)$ is given by (2.25).In order to calculate $H(x_r|x_0 = m)$ we repeat the step conducted in (2.31) and (2.32) with the r-th composition of the map function with itself $f^r(\cdot)$. Applying the chain rule of derivation we can obtain a discrete approximation of $\frac{d}{dx} f^r(x)$, at the m-th partition as

$$d_r(m) = \left[\frac{d}{dx} f\left(\frac{a_m + a_{m+1}}{2}\right)\right]^r, \tag{2.34}$$

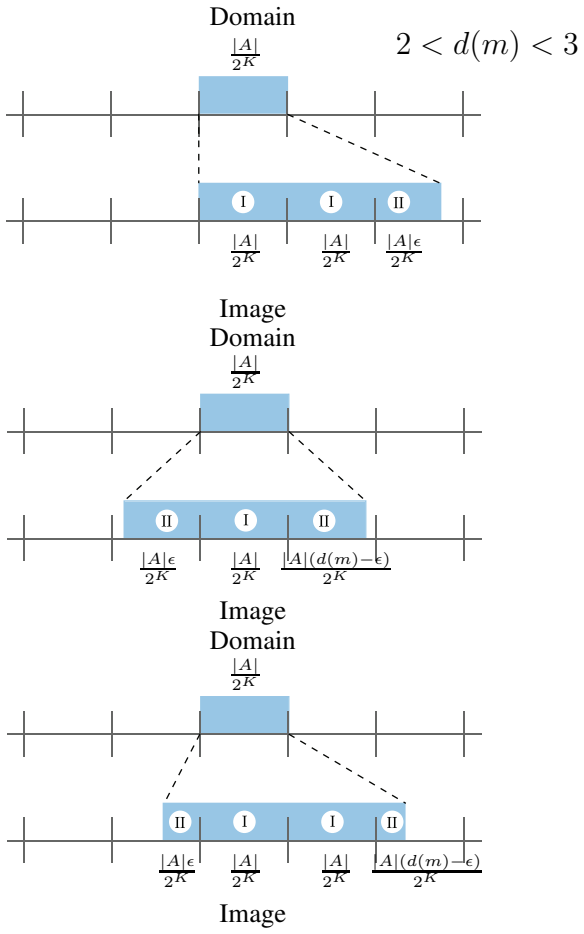


Figure 2.8: *The figure illustrates the mapping of a partition for* $2 < d(m) < 3$.

and $H(x_r|x_0 = m)$ is

$$H(x_r|x_0 = m) \begin{cases} \dfrac{d_r(m)}{2\ln 2}, & \text{if } d_r(m) \leq 1 \\ \dfrac{\lfloor d_r(m) \rfloor - 1}{d_r(m)} \log_2 \left[\dfrac{1}{d_r(m)} \right] + \dfrac{1}{2d_r(m)\ln 2}, & \text{if } d_r(m) > 1. \end{cases} \tag{2.35}$$

Thus the average conditional entropy after r iterations is obtained as

$$H(x_r|x_0) = \sum_{m=0}^{2^K-1} P_0(m) H(x_r|x_0 = m). \tag{2.36}$$

The Critical Iteration for Eventually Expanding Maps

If we consider only eventually expanding maps (see Definition 2.2.5) after a finite number of iterations k we have that $d_{k+1}(m) > d_k(m)$ due to the eventually expanding property. Hence, the conditional entropy increases with the iteration up to the critical iteration r_* when

$$H(x_{r_*}|x_0) = H(x_{r_*}), \tag{2.37}$$

therefore, $I(x_{r_*}; x_0) = 0$. A procedure to estimate the critical iteration for a eventually expanding map is proposed. As mentioned in Subection 2.2.1 calculating the FP operator is often a difficult problem, but the invariant density $p_*(x)$ can be obtained by the method described in Subsection 2.2.3, so, it is assumed that $p_r(x) = p_*(x)$ for any $r > 0$. This assumption considers that $p_0(x)$ converges to the invariant density after one iteration. Then, $P_*(x)$ and $H(x_r)$ can be obtained using (2.24) and (2.27) respectively. The conditional entropy $H(x_r|x_0)$ can be obtained using $d_r(m)$ and $P_0(m)$ in (2.36).

2.3.3 Motivating Examples

The techniques presented so far are applied to two different chaotic maps, the tent map and the PWS map. For both maps we consider that

$$p_0(x) = \begin{cases} \dfrac{1}{|A|} \text{ , for } x \in A \\ \\ 0 \text{ , otherwise.} \end{cases} \tag{2.38}$$

Tent Map

The tent map has this name because its curve is shaped like a tent as shown in Figure 2.9. The tent map $f : [-1, 1] \to [-1, 1]$ is given by

$$f(x) = \begin{cases} 2x + 1, & \text{for } x \in [-1, 0) \\ \\ 1 - 2x, & \text{for } x \in [0, 1] \end{cases} \tag{2.39}$$

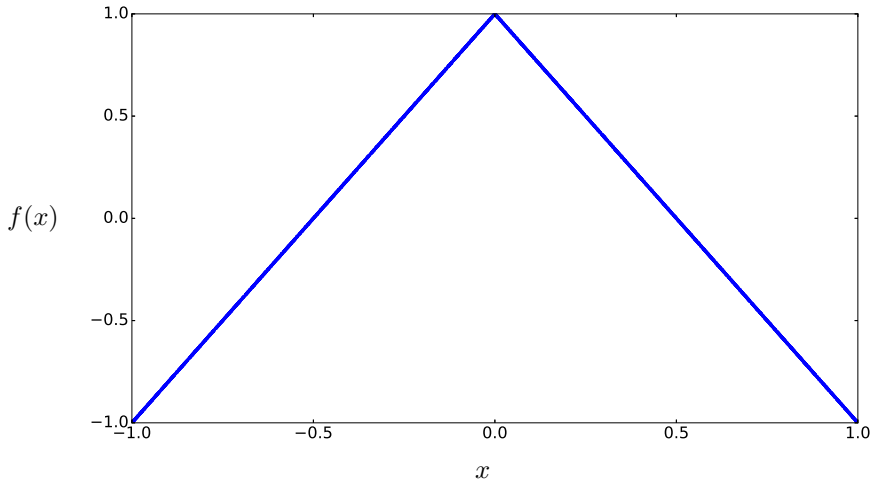


Figure 2.9: *Tent map.*

The tent map has a constant absolute derivative $|\frac{d}{dx}f(x)| = 2$ and a Lyapunov exponent $\lambda = \ln(2)$. Its FP matrix is equal to

$$\mathbf{P} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}. \tag{2.40}$$

The eigenvector correspondent to the unitary eigenvalue is

$$\mathbf{p}_* = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \end{bmatrix} \tag{2.41}$$

Hence, its invariant density is

$$p_*(x) = \begin{cases} \dfrac{1}{2}, & \text{for } x \in [-1, 1] \\ 0, & \text{otherwise.} \end{cases} \tag{2.42}$$

The mean of a point of the orbit of the tent map is given by

$$E[x[n]] = 0, \tag{2.43}$$

where $E[\cdot]$ denotes the expected value, while the variance is given by

$$E[x[n]^2] = \frac{1}{3}. \tag{2.44}$$

As the uniform invariant density is a fixed point of the FP operator of the tent map the PMF of the output point of the orbit is also uniform. Hence, the entropy of the r-th iteration is given by

$$H(x_r) = \log_2(2^K) = K \text{ bits}. \tag{2.45}$$

Table 2.1: *Mutual information between the r-th iteration and the initial condition of the tent map for $K = 8$.*

r	$I(x_r\|x_0)$
0	8
1	7.14
2	6.32
3	5.28
4	4.20
5	3.13
6	2.08
7	1.04
8	0

The derivative of the r-fold composition of the map with itself is $\left|\frac{d}{dx}f^r(x)\right| = 2^r$. Thus, using (2.36)

$$H(x_r|x_0) = \begin{cases} \dfrac{2^r-1}{2^r}\log_2[2^r] + \dfrac{1}{2^{r+1}\ln 2}, & \text{for } r < K \\ K, & \text{for } r \geq K \end{cases} \tag{2.46}$$

Therefore, the mutual information between the K-th iteration of the tent map x_K and the x_0 is equal to zero, so $r_* = K$. Table 2.1 shows the evolution of the mutual information of the tent map for $K = 8$.

PWS Map

The PWS map is defined in Section 2.2.3. As shown in Section 2.2.3 the invariant density of this class of maps can be approximated by $\hat{p}_*(x)$. $H(x_r)$ is readily obtained with (2.27) if we consider $P_r(m) = P_*(m)$ for $r \geq 1$.

The map derivative is given by

$$\frac{d}{dx}f(x) = \begin{cases} \dfrac{18}{(3x+2)^2}\text{ , for } x \in [0, 1/3) \\ \dfrac{20}{(x+3)^2}\text{ , for } x \in [1/3, 1]. \end{cases} \tag{2.47}$$

The discrete approximation of the derivative is obtained using (2.29) and is used to calculate the conditional entropy with (2.36). Table 2.2 shows the evolution of the mutual information of the PWS map for $K = 8$. Hence, for the PWS map $r_* = 10$.

2.3.4 Monte Carlo Simulation

In order to validate the model proposed in Section 2.3.2 a Monte Carlo simulation [31] of the information flow of the tent map is realized. We assume that $K = 8$, thus the map domain is divided

Table 2.2: *Mutual information between the r-th iteration and the initial condition of the PWS map for $K = 8$.*

r	$I(x_r\|x_0)$
0	8
1	7.22
2	6.53
3	5.62
4	4.69
5	3.73
6	2.77
7	1.82
8	0.88
9	0.033
10	0

in 256 partitions. According to the analysis developed at Section 2.3.3 it is expected that the mutual information of the tent map and the PWS map will go to zero for the 8th iterate and the 10th iterate respectively.

The conditional probability distributions of the 1st to the 12th iterate of the tent map and the PWS map are estimated by iterating 256000 randomly selected initial conditions within each of the 256 initial partitions.

Figure 2.10 shows $I(x_r; x_0)$ versus r for every iteration of the tent map until the 12th iteration and compares it with the predicted result in Table 2.1. As seem in the picture the simulation results are consistent with the theoretical predictions.

In Figure 2.11, a similiar comparison is shown for the PWS map. From observing the figure we conclude that the mutual information is zero starting from the 10th iteration, which corresponds to the prediction.

2.4 Conclusion

The important conclusions we draw from this chapter are:

▷ The sequences generated by chaotic maps are extremely sensitive to variations in the initial condition.

▷ The sequences generated by a Markov map originate a Markov process.

▷ It is possible to obtain the invariant probability density in closed form for Markov maps. The tent

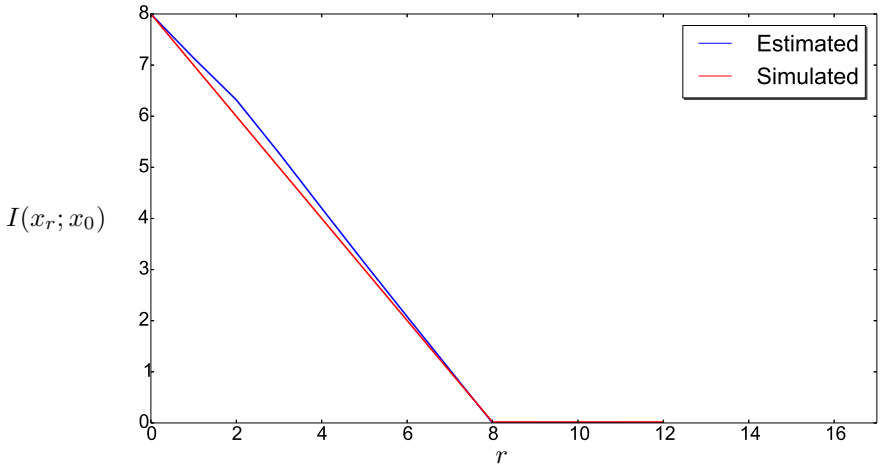


Figure 2.10: *Comparison between the Monte Carlo simulation of the information flow and the predicted result up to the* 12*th iterate for the tent map with* $K = 8$*.*

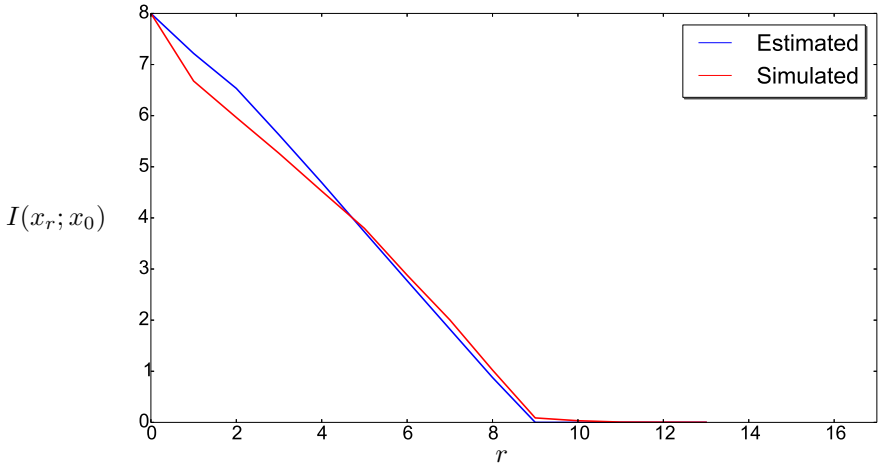


Figure 2.11: *Comparison between the Monte Carlo simulation of the information flow and the predicted result up to the* 12*-th iterate for the PWS map with* $K = 8$*.*

map specifically is uniformly distributed.

▷ The FP operator of eventually expanding piecewise smooth maps can be approximated and consequently its invariant distribution can be approximated.

▷ The mutual information between the initial condition and the r-th iteration goes to 0 due to the folding and stretching properties of chaotic maps.

▷ Given the FP operator of a map it is possible to accurately estimate for which iteration all the information on the initial condition is lost.

CHAPTER 3

MESSAGE AUTHENTICATION

In this chapter, we discuss the importance of authentication in the context of secure communications. Then, we introduce to the reader to a few traditional authentication methods widely described in the literature [32, 33]. The need of increasing layers of security in communication systems is discussed and how physical layer authentication methods are a promising solution to satisfy the need for extra security. We assume a system that employs tags, which are signals that are generated based on the knowledge of a secret key, to perform the authentication of the messages and a novel method to generate those tags using chaotic maps is presented. The unconditional security of the system is quantified, considering an information-theoretic approach, and a positive lower bound to the security is derived, which is an advance in comparison to systems employing tags generated by hash functions [9]. Finally, we define security in the context of physical layer authentication and evaluate the probability of a successful attack to the system considering the proposed tag generation method.

3.1 Secure Communications

Depending on the application a communication system has several security goals, but they frequently require [32, 33]

- **Confidentiality**: A third party must not be able to have access to the information sent between two communicating nodes.
- **Integrity**: The communicating nodes must be able to verify that the content of the received message is not adultered.

▷ **Authentication**: The communicating nodes must be able to verify the identity of the node that sent a specific message.

In this work, we restrict our efforts to the authentication goal. So, all the methods proposed in this chapter have the sole purpose of guaranteeing that a communicating node accepts data packets from trusted nodes and is able to detect if transmitted data was somehow tampered by an untrusted third party with a high level of reliability. The ITU-T Recommendation X800 [34], *Security Architecture for OSI* defines a systematic approach to identify the security needs and strategies of a system. The recommendation focus on three aspects of security:

▷ **Security Attacks**: Any action that might compromise one or more of the security goals.

▷ **Security Services**: A service provided by a layer of the network that guarantees the security goals are effectively achieved and are protected from possible security attacks.

▷ **Security Mechanisms**: The procedures designed to detect, prevent or recover from an attack. Several security mechanisms implement a security service.

In this work we are concerned with the authentication security service. We start by discussing the core security mechanisms for authentication and then we discuss the possible security attacks to the system and present supplemental security mechanisms to specifically counter each considered threat.

3.2 Authentication Methods

Conceptually the problem of determining the authenticity of a message or an user can be viewed as asking a questions and accepting the user or the message depending on the answer to this question. Suitable questions to be asked are:

▷ **What do you know?** This is the knowledge factor which is regarded to some information that only the authentic user should know. It can be a password or the answer to a personal question.

▷ **What do you have?** This is the possession factor, this method is probably the one being used for the longest time and it is regarded to something that only the authentic user should possess. It can be a club membership card, a signed document or a token.

▷ **What you are?** This is the inherence factor and it is concerned to some characteristic of the authentic user that is inherently unique to him. It can be a voice recognition system, a fingerprint reader or an iris scanner.

In order to achieve higher security instead of asking a single question multiple questions could be asked. This model is called **multifactor authentication** (MFA).

3.2.1 The Scenario

In this section the users considered in the authentication system model are presented and their roles and capabilities are detailed. We consider a classical scenario in the study of cryptography where three users sharing a common insecure channel, as depicted in Figure 3.1. These users are:

- ▷ **Alice**: Is a legitimate user of the system, meaning that she employs the proposed authentication protocol. She sends message packets of length L with a superimposed tag to Bob. The tag depends on a secret key shared with Bob.
- ▷ **Bob**: Is a legitimate user of the system, meaning that he employs the proposed authentication protocol. He receives message packets of length L, recover them and based on the detection or not of a legitimate tag he decides to accept or to reject the messages.
- ▷ **Eve**: Is a malicious user of the system, where we assume the Kerckhoff's hypothesis [12], which implies that Eve is aware of every possible detail of the authentication scheme, except for the secret key. She is considered an active adversary, her goal is to disrupt the communication between Alice and Bob. She is able to eavesdrop the packets sent by Alice and to send malicious packets to Bob.

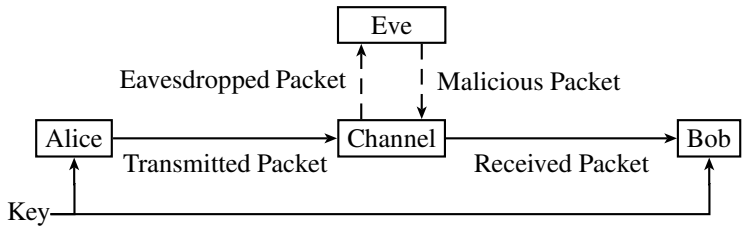


Figure 3.1: *The classical three users scenario of communications over an unsecure channel.*

3.2.2 Message Authentication Functions

A widely used method to verify the authenticity of messages [35] consists in using a generator function $g(\cdot)$ that takes two inputs, the message packet to be sent $\mathbf{s}$ and a secret key shared between the legitimate users $\mathbf{k}$ and returns a message authentication code or tag $\mathbf{t} = g(\mathbf{s}, \mathbf{k})$. The transmitter sends the message along with the tag to the receiver, that recover the message as $\hat{\mathbf{s}}$ and verifies if the locally generated tag $\hat{\mathbf{t}} = g(\hat{\mathbf{s}}, \mathbf{k})$ matches the received one. Traditionally two approaches are used:

- ▷ **Message Authentication Codes** [36]: $g(\cdot)$ is a hash function that maps a pair of message and key of any length into a fixed sized value used as a tag. This tag is appended to the transmitted message, as the receiver has the secret key he is able to decode the message and apply the hash function using his own key and verifying if the locally generated tag matches the received one.
- ▷ **Message Encryption** [12, 37]: $g(\cdot)$ is a ciphering function and the cipher text as whole is used as an authenticator.

3.2.3 Physical Layer Authentication

The authentication protocol usually takes place in higher layers of the network [1, 33]. However, complying with the MFA methodology, there is a trend to extend the authentication process to additional protocols deployed in the lower layers, more specifically in the physical layer. Higher layers authentication methods are usually computationally secure, meaning that its security relies on the hardness of solving a problem in superpolynomial time [32]. This reliance may incur in a frailty as soon as more powerful computers (e.g. quantum computers) or faster solving algorithms are available. On the other hand, physical layer authentication system benefit from the stochastic nature of wireless communication channels, making it possible to achieve unconditional security, meaning that despite the computational power of the adversary he simply does not have enough information to compromise the system security. Thus, in this work a physical layer authentication system which shares similarities with [9] is proposed employing a novel method to generate tags based on chaotic maps.

In the physical layer two ways to send the tag to the receiver are described in the literature

- ▷ **Time Division Multiplexing (TDM)** [38] This method consists on allocating different time slots for the message and for the tag.
- ▷ **Tag Embedding** [39] This method consists in allocating different power to the message and to the tag, summing them up and then sending it as a single transmitted packet.

For the TDM method, as the message and the tag are sent in separate time frames, hence it is easier to recover both the message and the tag as they do not interfere with each other. However, the number of information bits per packet is reduced. On the other hand, for the tag embedding method, it is harder to recover the tag as the power allocated to the tag is only a fraction of the power allocated for the TDM method. On the bright side, there is no reduction on the information bits per packet, also, it is harder for the adversary to detect the tag. Figure 3.2 illustrates the timing of the transmitted

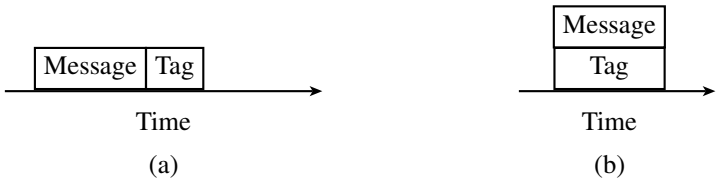


Figure 3.2: ***(a)*** *The packet allocation for the TDM method* ***(b)*** *The packet allocation for the tag embedding method.*

packet for both methods. In this work, the tag embedding approach is chosen because, as shown in subsequent sections, the different power allocation characteristic of the method shall be used as a security mechanism to comply with a security goal.

3.3 Security Attacks

In this section, the possible security attacks to the authentication system are detailed. Following a similar approach to [9, 37] we consider three attacks: impersonation, substitution and replay. We consider that $\mathbf{s}$ and $\mathbf{t}$ are two vectors of length L denoting the transmitted message and the transmitted tag, respectively, and that $\mathbf{k}$ is a binary vector of length K denoting the secret key, where K is larger than L.

3.3.1 Impersonation Attack

The impersonation or masquerade attack consists on a non-authorized user from the network (Eve in our model) inserting messages on the channel impersonating Alice, an authorized node. Consider that Eve observes a tag message pair $(\mathbf{s}, \widetilde{\mathbf{t}})$, where $\widetilde{\mathbf{t}}$ denotes a noisy version of the tag. So, based on the knowledge acquired on this observation, Eve estimates the key used to generate the tag and sends a fraudulent pair $(\mathbf{s}', \mathbf{t}')$. The probability that an impersonation attack is successful (when $\mathbf{t}'$ is a legitimate tag for $\mathbf{s}'$) is denoted by P_I, which is the probability of determining the key.

3.3.2 Substitution Attack

The substitution attack consists on intercepting a legitimate tag message pair $(\mathbf{s}, \widetilde{\mathbf{t}})$ and altering the content of the message. Eve is successful if she is able to find a fraudulent message $\mathbf{s}'$ different from $\mathbf{s}$ that yields to the same tag. The probability that a substitution attack is successful is denoted by P_S.

3.3.3 Replay Attacks

The replay attack consists on storing a legitimate tag message pair and then retransmitting it to Bob in the future. The probability that a replay attack is successful is denoted by P_R.

3.4 Chaotic Tag Generation and Security Mechanisms

The choice of the tag generator function $g(\cdot)$ is of fundamental importance to achieve a secure authentication system. The tag vector is the output of $g(\cdot)$, given the transmitted message and the secret key as inputs, and is used by the receiver to determine the authenticity of the message. As described in Subsection 3.2.2, $g(\cdot)$ is typically a keyed hash function or a ciphering function. In this dissertation, a function based in chaotic maps is proposed.

The tag is taken to be an orbit of fixed length generated by the chaotic map. As explained in Subsection 2.1.2, due to the sensitivity of chaotic maps to the initial conditions, infinitesimally close initial conditions yield to diverging orbits. We take advantage of this property by using the secret key and the transmitted message to determine the initial condition, and from it generate the tag.

The set of all the possible initial conditions $\mathcal{X}_0$ is given by

$$\mathcal{X}_0 = \{X_0^i\}_{i=0}^{2^K-1}, \tag{3.1}$$

and is known by all users of the communication system. Similarly, we have that

$$\mathcal{X}_n \stackrel{\triangle}{=} \{f^n(x) | \forall\, x \in \mathcal{X}_0\}, \tag{3.2}$$

where $\mathcal{X}_n$ is the set of all possible n-th iterations.

Let $M(\cdot)$ be a one to one mapping between all the K long binary vectors and the elements of $\mathcal{X}_0$. Then, the initial condition $x[0]$ is given by

$$x[0] = M(\mathbf{k} \oplus \mathbf{s} || \mathbf{t}_s), \tag{3.3}$$

where $\mathbf{t}_s$ is the time stamp vector of length equal to $K - L$, $\oplus$ is the XOR operation and $||$ denotes the concatenation between two vectors. The time stamp vector plays an important role in preventing replay attacks as detailed in Subsection 3.4.4. The key vector is drawn from a uniformly distributed PMF, thus, the vector resulting from the XOR operation is completely random, so the initial condition of the map is also a random variable with PMF given by

$$P(x[0] = x) = \begin{cases} \dfrac{1}{2^K}, & \forall\, x \in \mathcal{X}_0 \\ 0\,, & \text{otherwise}\,. \end{cases} \tag{3.4}$$

As shown in Subsection 2.3.2 skipping points of the orbit decreases the information about the initial condition, so, by skipping the first σ points of the orbit the system designer limits the maximum amount of information that can be obtained about the initial condition, and consequently about the key, by observing the tag. Hence, instead of transmitting the first L points of the orbit as a tag, the proposed system skips the first σ points of the orbit, where σ is the skip parameter and $\sigma < K$. With $x[0]$ determined by the key, the transmitted message and the time stamp vector, the tag is taken as a finite orbit of length L of $x[0]$ under $f(\cdot)$, and is given by

$$\mathbf{t} = \begin{bmatrix} x[\sigma] & x[\sigma+1] & \cdots & x[\sigma+L-1] \end{bmatrix} \tag{3.5}$$

where $x[\sigma] \stackrel{\triangle}{=} f^{\sigma}(x[0])$.

3.4.1 Unconditional Security

As explained in Subsection 3.2.1, we evaluate the security of the authentication system assuming the Kerckhoff's hypothesis [12], so all the security of the system relies on the fact that the attacker knows every possible detail of the authentication procedure, but the secret key. Additionally, we assume unconditional security [12], meaning that the adversary has no computational constraint and has unconstrained access to the communication channel.

The security of a system is quantified by how uncertain is the key given the assumptions mentioned above. The conditional entropy [29] of the key given a noiseless observation of a legitimate message and tag $H(\mathbf{k}|\mathbf{s},\mathbf{t})$ is used to quantify the unconditional security of the authentication system [9, 12, 40].

Let $f : A \to A$ be the chaotic map used for tag generation. Consider the conditional entropy $H(x[0],\mathbf{k}|\mathbf{s},\mathbf{t})$, using the chain rule of entropy [29] we have that

$$H(x[0],\mathbf{k}|\mathbf{s},\mathbf{t}) = H(x[0]|\mathbf{k},\mathbf{s},\mathbf{t}) + H(\mathbf{k}|\mathbf{s},\mathbf{t}) = H(\mathbf{k}|x[0],\mathbf{s},\mathbf{t}) + H(x[0]|\mathbf{s},\mathbf{t}). \tag{3.6}$$

As the initial condition is a function of the message and the key, $H(x[0]|\mathbf{k},\mathbf{s},\mathbf{t}) = 0$. Similarly, as the key is completely determined by the message and by the initial condition, $H(\mathbf{k}|x[0],\mathbf{s},\mathbf{t}) = 0$. Moreover, we have that

$$H(x[0],\mathbf{s}|\mathbf{t}) = H(x[0]|\mathbf{s},\mathbf{t}) + H(\mathbf{s}|\mathbf{t}) = H(\mathbf{s}|x[0],\mathbf{t}) + H(x[0]|\mathbf{t}), \tag{3.7}$$

as $\mathbf{s}$ is independent of $\mathbf{t}$ and $x[0]$, we have that $H(\mathbf{s}|\mathbf{t}) = H(\mathbf{s})$ and $H(\mathbf{s}|x[0],\mathbf{t}) = H(\mathbf{s})$. Thus, $H(x[0]|\mathbf{s},\mathbf{t})$ is equal to $H(x[0]|\mathbf{t})$. So, the conditional entropy of the key can be rewritten as

$$H(\mathbf{k}|\mathbf{s},\mathbf{t}) = H(x[0]|\mathbf{t}). \tag{3.8}$$

Given that $x[\sigma]$ is known, the knowledge of any $x[i]$, for $i > \sigma$, gives no additional information about the initial condition. Thus, (3.8) can be rewritten as

$$H(\mathbf{k}|\mathbf{s}, \mathbf{t}) = H(x[0]|x[\sigma]). \tag{3.9}$$

Furthermore, in order to be chaotic, $f(\cdot)$ must be non-invertible, so, the inverse mapping of the chaotic map $f^{-1}(\cdot)$ is a one-to-many association between the domain and the image, meaning that $f^{-1}(\cdot)$ maps an input point to multiple points. As the first σ points of the orbit are not transmitted, this introduces an uncertainty on which initial condition generated the observed orbit.

Definition 3.4.1 – Preimage Set

Let $f : A \to A$ be a chaotic map and y a point in A. The i-th preimage set of y under $f(\cdot)$ is

$$\mathcal{S}_i(y) = \{x|f^i(x) = y\} \tag{3.10}$$

□

In this work, we restrict our analysis to maps with constant binary preimages, so the cardinality of the i-th preimage set depends only on i and is given by

$$|\mathcal{S}_i(y)| = 2^i, \forall\, y \in A. \tag{3.11}$$

This is not a severe restriction as there are several maps that attend the restriction, such as the tent map [41], the tanh map [42], the logistic map [15], among others.

As the unconditional security in (3.6) is given by $H(x[0]|x[\sigma])$, it is necessary that the knowledge of $x[\sigma]$ leaves some uncertainty about $x[0]$. Thus, multiple initial conditions must lead to the same σ-th iteration, and consequently to the same tag. In order to guarantee this, the set $\mathcal{X}_0$ must be carefully chosen, as discussed next. Firstly, $2^{K-\sigma}$ points in A are arbitrarily selected for the set of possible σ-th iterations, $\mathcal{X}_\sigma$. Then $\mathcal{X}_0$ is given by

$$\mathcal{X}_0 = \{x|x = f^{-\sigma}(y), \forall\, y\ \mathcal{X}_\sigma\}. \tag{3.12}$$

Given this method of generation of $\mathcal{X}_0$, we have that 2^σ initial conditions generate the same tag. Thus, the conditional probability of $x[0]$ given $x[\sigma]$ is

$$P(x[0] = x|x[\sigma] = y) = \begin{cases} \dfrac{1}{2^\sigma}\,, & \text{if } x \in \mathcal{S}_\sigma(y) \\ 0\,, & \text{otherwise.} \end{cases} \tag{3.13}$$

It is possible to calculate the conditional entropy in (3.9), with the conditional probability in

(3.13), as

$$\begin{aligned} H(\mathbf{k}|\mathbf{s},\mathbf{t}) &= H(x[0]|x[\sigma]) \\ &= -\sum_{j=0}^{2^{K-\sigma}-1} P(x[\sigma]=X_\sigma^j)\times \\ &\sum_{i=0}^{2^K-1} P(x[0]=X_0^i|x[\sigma]=X_\sigma^j)\log_2 P(x[0]=X_0^i|x[\sigma]=X_\sigma^j). \end{aligned} \tag{3.14}$$

So the unconditional security is given by

$$H(\mathbf{k}|\mathbf{s},\mathbf{t}) = H(x[0]|x[\sigma]) = \sigma. \tag{3.15}$$

From this analysis, we conclude that the chaotic generated tags provide a positive unconditional security, that depends only on the skip parameter σ.

3.4.2 Security Mechanisms Against Impersonation Attacks

Impersonation attack effectiveness rely on the knowledge the attacker has about the secret key. As the secret key is never transmitted, all the knowledge the attacker is able to obtain is from observing the tag message pairs sent between the legitimate users. Assuming that the attacker is able to correctly recover the message, the security against impersonation attacks can be measured by the difficulty of estimating the initial condition that originated the tag. Two security mechanisms are identified to decrease the information about the initial condition. Firstly, all the observations made by the attacker are noisy, so, the transmitter is able to increase the uncertainty on the observation of the tag, due to the noise, by reducing the power allocated to the tag. Instead of $\mathbf{t}$ the attacker observes

$$\widetilde{\mathbf{t}} = \mathbf{t} + \mathbf{w}, \tag{3.16}$$

where $\mathbf{w}$ is a vector representing additive white Gaussian noise. Secondly, as explained in Subsection 3.4.1, Alice skips the first σ points of the orbit. Hence, Eve observes

$$\widetilde{\mathbf{t}} = \Big[x[\sigma] + w_0, \quad \cdots, \quad x[\sigma+L-1] + w_{L-1}\Big]. \tag{3.17}$$

In order to calculate the probability that an impersonation attack is successful, P_I, it is necessary to obtain how much information the attacker has about the initial condition given noisy observations of the tag. This value is given by the conditional entropy of the initial conditional given a noisy observation of the tag, $H(x[0]|\widetilde{x}_\sigma^{\sigma+L-1})$, where $\widetilde{x}_\sigma^{\sigma+L-1}$ denotes the sequence $\widetilde{x}[\sigma], \widetilde{x}[\sigma+1], \cdots, \widetilde{x}[\sigma+L-1]$, and each $\widetilde{x}[i]$ is a random variable denoting the value of $f^i(x[0]) + w_{\sigma-i}$. We consider next the calculation of $H(x[0]|\widetilde{x}_\sigma^{\sigma+L-1})$.

Firstly, consider the conditional entropy $H(x[0], x[\sigma]|\widetilde{x}_{\sigma}^{\sigma+L-1})$. Using the chain rule for entropies [29] we have that

$$\begin{aligned} H(x[0], x[\sigma]|\widetilde{x}_{\sigma}^{\sigma+L-1}) &= H(x[\sigma]|x[0], \widetilde{x}_{\sigma}^{\sigma+L-1}) + H(x[0]|\widetilde{x}_{\sigma}^{\sigma+L-1}) \\ &= H(x[0]|x[\sigma], \widetilde{x}_{\sigma}^{\sigma+L-1}) + H(x[\sigma]|\widetilde{x}_{\sigma}^{\sigma+L-1}). \end{aligned} \tag{3.18}$$

As $x[0]$ completely determines $x[\sigma]$ we have that

$$H(x[\sigma]|x[0], \widetilde{x}_{\sigma}^{\sigma+L-1}) = 0. \tag{3.19}$$

Furthermore, given that $x[\sigma]$ is known, the knowledge of $\widetilde{x}_{\sigma}^{\sigma+L-1}$ gives no additional information about $x[0]$, thus,

$$H(x[0]|x[\sigma], \widetilde{x}_{\sigma}^{\sigma+L-1}) = H(x[0]|x[\sigma]). \tag{3.20}$$

Substituting the results of (3.19) and (3.20) into (3.18) we obtain the conditional entropy of the initial condition given the noisy observation of the tag as

$$\begin{aligned} H(x[0]|\widetilde{x}_{\sigma}^{\sigma+L-1}) &= H(x[0]|x[\sigma]) + H(x[\sigma]|\widetilde{x}_{\sigma}^{\sigma+L-1}) \\ &= \sigma + H(x[\sigma]|\widetilde{x}^{\sigma+L-1}), \end{aligned} \tag{3.21}$$

where (3.21) comes from (3.15). In $H(x[\sigma]|\widetilde{x}_{\sigma}^{\sigma+L-1})$ the uncertainty about $x[\sigma]$ arises from the noise in the observations of the tag, if the channel is noiseless, then $H(x[\sigma]|\widetilde{x}_{\sigma}^{\sigma+L-1}) = 0$. On the other hand, for a fixed σ, we have that $H(x[0]|x[\sigma])$ is constant regardless of the channel noise. As detailed in Section 1.2, all the other physical layer authentication schemes relied on the adversary either making noisy observations or having a channel worse than the one between the legitimate users. In comparison with these works, the tag generation method proposed in this chapter provides a lower bound on the conditional entropy of the key given a legitimate tag even in a noiseless channel. As $H(x[0]|\widetilde{x}_{\sigma}^{\sigma+L-1}) \leq H(x[0]) = K$ [29], we have that

$$\sigma \leq H(x[0]|\widetilde{x}_{\sigma}^{\sigma+L-1}) \leq K. \tag{3.22}$$

So the conditional entropy of at least $H(x[0]|x[\sigma])$ is guaranteed and an extra level of security is provided by the noise inherent to the channel, measured by $H(x[\sigma]|\widetilde{x}_{\sigma}^{\sigma+L-1})$.

The conditional entropy $H(x[0]|\widetilde{x}_{\sigma}^{\sigma+L-1})$ indicates how many bits of the initial condition are uncertain given the noisy observation of the tag. Thus, assuming the attacker uses the optimal method to estimate the key, the probability of a successful impersonation attack is given by

$$P_I = 2^{-H(x[0]|\widetilde{x}_{\sigma}^{\sigma+L-1})}. \tag{3.23}$$

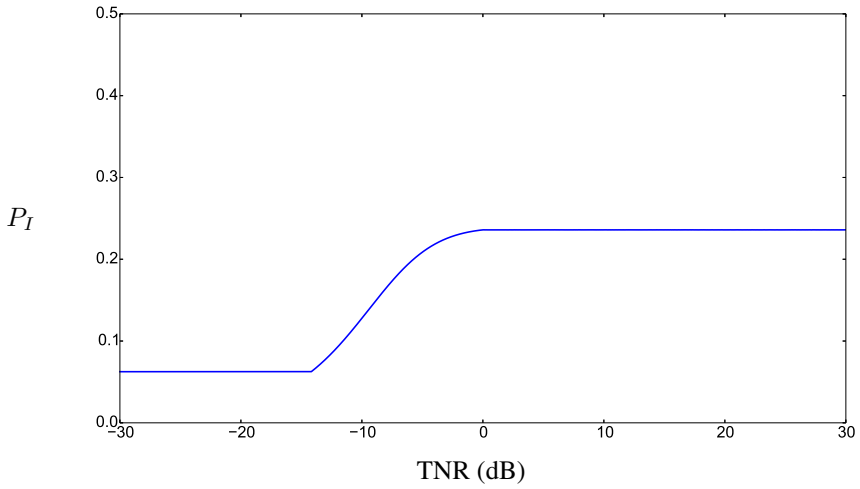


Figure 3.3: *Probability of a successful impersonation attack for a tag generated by the tent map with* $L = 3$*,* $K = 4$ *and* $\sigma = 2$*.*

From (3.22), we have that P_I is bounded by

$$2^{-K} \leq P_I \leq 2^{-\sigma}, \tag{3.24}$$

so, the designer is able to control the maximum probability of success of an impersonation attack by tuning the system parameters.

Example

In order to illustrate the probability P_I of the chaotic tag generation process and the extra uncertainty due to the Gaussian noise an example is presented where the tent map, defined by (2.39), is used to generate the tag for $K = 4$, $\sigma = 2$ and $L = 3$. For the simulation, the adversary is assumed to observe the noisy tag signal with finite resolution.

First, we introduce a new measure, the tag-to-noise ratio (TNR) [9]. The TNR is the ratio in decibels between the tag power and the noise power. Figure 3.3 shows the probability of a successful impersonation attack versus the TNR. It is possible to conclude that for low values of TNR the noise provides an extra security against impersonation attacks while for high values of TNR P_I tends to $2^{-\sigma}$. Thus, in comparison with the system proposed in [9] and implemented in [13], the tag generation method proposed in this work has a lower bound on the conditional entropy.

3.4.3 Security Mechanisms Against Substitution Attacks

The security against substitution attacks depend on the hardness of finding distinct messages that generate the same tag [32, 33]. As explained in Subsection 3.3.2, for a substitution attack to be successful the adversary must send a fraudulent message that results in the same tag of the intercepted signal. So, in order to be resistant against such attacks the tag generation function needs to fulfil two requirements:

- ▷ **Preimage resistance**: A function $g(\cdot)$ is preimage resistant if given a tag $\mathbf{t}$ it is computationally hard to find a message such that $g(\mathbf{s}, \mathbf{k}) = \mathbf{t}$.
- ▷ **Second preimage resistance**: A function $g(\cdot)$ is second preimage resistant if given a message $\mathbf{s}_1$ it is computationally hard to find a message $\mathbf{s}_2$ such that $g(\mathbf{s}_1, \mathbf{k}) = g(\mathbf{s}_2, \mathbf{k})$.

Consider a tag generation function using the method described in Section 3.4 using the chaotic function $f : A \to A$. Given a tag, the attacker is able to calculate all the possible initial conditions that generated the tag. However, without knowing the secret key all possible messages could have generated the tag with equal probability. Hence, the probability of success of a substitution attack is equal to the probability of randomly picking a message that result in the intercepted tag. Thus, in order to be secure against substitution attacks, the tag generation method must be second preimage resistant.

As mentioned in Subection 3.4.1, multiple initial conditions generate the same tag. Hence, given a tag $\mathbf{t}$, every point $x \in \mathcal{S}_\sigma(x[\sigma])$ generates the same orbit under $f(\cdot)$ from the σ iteration onwards. Considering only chaotic maps with constant binary preimage, there are 2^σ initial conditions resulting in the same tag and 2^K possible initial conditions. Thus, selecting a random message, the probability that the resulting tag is equal to the intercepted one, which means that the substitution attack is successful, is given by

$$P_S = 2^{K-\sigma}. \tag{3.25}$$

The skip parameter σ and the key length K must be carefully selected to ensure that $P_S \approx 0$, guaranteeing resistance to substitution attacks.

Figure 3.4 illustrates how K and σ affect P_S. Given a value for K and a requirement on the maximum P_S it is possible to determine the maximum value of σ that can be selected without compromising the security against substitution attacks.

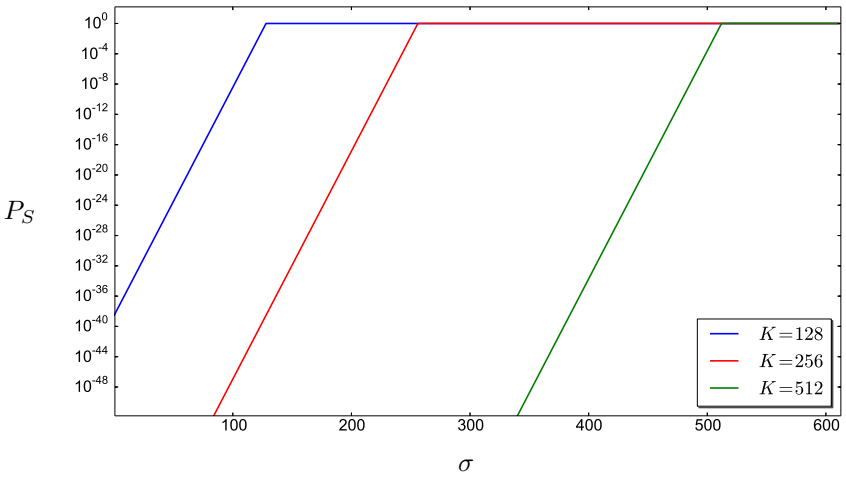


Figure 3.4: *Probability of a successful substitution attack for a tag generated by the tent map, for three values of* K.

Security Tradeoff Between Impersonation and Substitution Attacks

In (3.24), we established an upper bound on the probability that an impersonation attack is successful. This upper bound decreases with σ. On the other hand, the probability that a substitution attack is successful, given by (3.25), increases with σ. Thus, a compromise between the impersonation security and the substitution security must be made.

To illustrate this tradeoff, consider a tag generated by the tent map using a $K = 256$. Figure 3.5 shows the probability of success of an impersonation attack P_I and substitution attack P_S versus σ.

Given a maximum tolerable probability of accepting a fraudulent message η, the plot in Figure 3.5 is useful to determine if the security requirement is achievable and for which values of σ. If an horizontal line at η is drawn in the plot, the x coordinate of the crossing points between this line and the P_S and P_I curves indicates the range of allowed values of σ that satisfy the security requirements. In this figure, we considered $\eta = 10^{-20}$, what results in the range $66 \leq \sigma \leq 189$.

3.4.4 Security Mechanisms Against Replay Attacks

The time stamp $\mathbf{t}_s$ is a binary counter, starting at zero, that increments for every transmitted packet. As given by (3.3), the initial condition depends on $\mathbf{t}_s$, so if the same message is transmitted in different moments they yield to a different tag. The key reuse factor (KRF) is the number of times that the same message can be transmitted without resulting in the same tag. As the time stamp vector has length $K - L$, we have that KRF $= 2^{K-L}$. So, the probability of success of a replay attack is

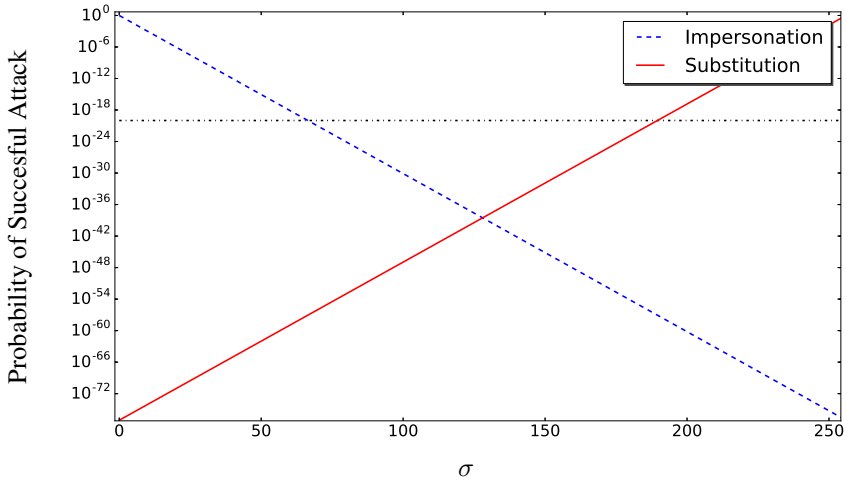


Figure 3.5: *Tradeoff between the probability of a successful impersonation attack and the probability of succes of a substitution attack, for* $K = 256$.

given by

$$P_R = \begin{cases} 0\,, & \text{if dec}(\mathbf{t}_s) \leq \text{ KRF} \\ 1\,, & \text{otherwise,} \end{cases} \tag{3.26}$$

where dec$(\cdot)$ maps a binary vector into the correspondent integer. So, an increase in the value of $K - L$ increases the amount of time that a key can be reused without being vulnerable to a replay attack.

3.5 RF Transmitter Blockchain

Figure 3.6 illustrates the RF blockchain diagram of the transmitter employing the chaotic authentication protocol. Both the message and the key are inputs to the chaotic circuit and together they determine a initial condition to the orbit generated by the circuit from a finite set. The output of the chaotic circuit is an analog signal modulated with the same carrier frequency as the digital message. That's where the tag generation procedure differ from chaotic tag generation from hash functions, the input to the chaotic function is digital while it's output is analog. The modulated signals are multiplied by the scale factors ρ_s and ρ_t, and summed before going through a power amplifier (PA) and then finally transmitted through an antenna. From the circuit blocks presented in the blockchain the chaotic circuit is the most unusual one on traditional RF circuits, and that might raise questions about the feasibility of such tag generation method. However, there are plenty circuit implementations described in the literature that could be applied at the chaotic circuit block, in [41, 43] an

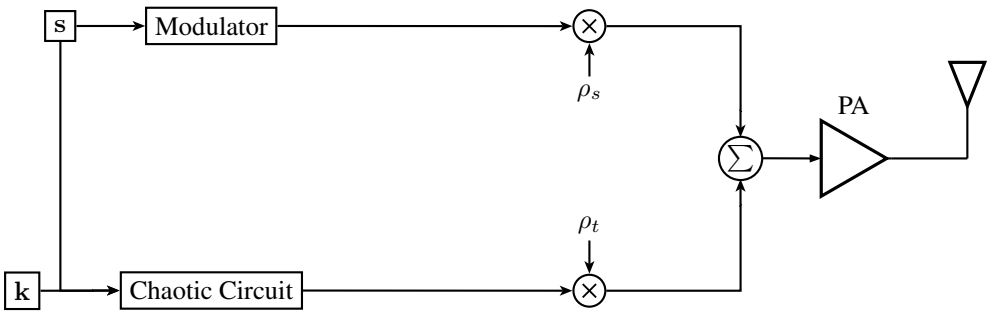


Figure 3.6: *RF blockchain of the transmitter employing the chaotic physical authentication protocol.*

implementation of the zigzag tent map, a variation of the tent map, is available with a variability analysis considering variations in the process, voltage and temperature of the devices. In [44] the implementation of the tent map and the tailed tent map are considered evaluating the impact of imperfections on the invariant density. In [45] a circuit implementation of the biological neuron is used to reproduce the dynamical behavior of any one dimensional chaotic map. In [46] a current mode implementation of the logistic map is proposed, manufactured and tested. Thus, it's safe to assume that there are many options available for the circuit designer to implement the chaotic block.

3.6 Conclusions

The most important conclusions from this chapter are:

- ▷ Authentication is an important security goal for communication systems.
- ▷ Physical Layer Authentication has emerged as an important strategy to add an extra security layer in the context of multifactor authentication and cross layer design of communication systems.
- ▷ Transmitting the authentication tag embedded in the message does not affect the transmission rate, but lowers the transmitted power allocated to the message.
- ▷ For a suitable selection of parameters chaotic maps can be used instead of hash functions to generate secure authentication tags.
- ▷ There are two security mechanisms against impersonation attacks, the power ration between the tag signal and the noise of the wireless channel and the loss of information about the initial condition of the map after σ iterations which is the lower bound on the conditional entropy about the initial condition.

- ▷ The security mechanism against substitution attack is to choose an appropriate value for the skip parameter σ in order to minimize the probability of a success of a substitution attack.
- ▷ For a sufficiently long key it is possible to select a skip parameter that satisfies the requirements that P_I and P_S to be lesser than a maximum failure rate η.
- ▷ The security mechanism against the replay attack is to make the initial condition dependent on a varying time stamp, so the initial condition is not repeated for the same message for KRF transmissions.
- ▷ There are several circuit implementations of chaotic maps described in the literature, which makes the chaotic tag generation process even more relevant.

CHAPTER 4

PERFORMANCE OF CHAOTIC TAGS

In this chapter the performance of the physical layer authentication protocol using embedded chaotic tags described in Chapter 3 is evaluated. We consider a three node communication system consisting of Alice, the legitimate transmitter, Bob, the legitimate receiver, and Eve, the active attacker. At first, a formal description of the communication system employing chaotic physical layer authentication is given. The authentication problem is modeled as a hypothesis test. Then, two performance aspects are evaluated, the bit error rate and the outage probability. We investigate how the power allocation between the message and the tag affects both metrics in comparison with a system employing no authentication. Afterwards, the tradeoffs between the system parameters are explored and the design requirements to determine the parameters are identified. For all the simulations in this chapter we use the tent map (defined in Chapter 2) as the tag generator function.

4.1 Channel Model

The authentication protocol studied in this work is designed to operate in a wireless channel and in this section the wireless channel model adopted and the assumptions made throughout the chapter are discussed and justified. A signal transmitted through a wireless channel is affected by multipath propagation and by the Doppler effect. For the channel model adopted the following assumptions are made:

▷ The period of the transmitted symbol T_S is at least an order of magnitude larger than the delay

spread, so the frequency response of the channel is flat for each symbol, only varying on its magnitude for different symbols. This kind of channel is called a flat fading channel.

- ▷ The period to send L symbols, where L is the length of the transmitted packet, is at least an order of magnitude lesser than the coherence time of the channel, so the channel is considered to be static during a packet transmission. This kind of channel is called a slow fading channel.
- ▷ There is no dominant line of sight propagation path, so the channel gain for the i-th packet h^i is Rayleigh distributed with unitary second moment ($E[(h^i)^2] = 1$, where $E[\cdot]$ denotes the expected value of a random variable). The channel gain changes between packets is an independent and identically distributed (i.i.d.) Rayleigh process.
- ▷ We consider a receiver with channel side information (CSI), hence, the value of h^i is known at the receiver and both the receiver and the transmitter know the distribution of h^i.

4.2 System Signals

In this section the system definitions are presented. We consider a BPSK modulator, where the i-th modulated message of length L is given by a row vector $\mathbf{s}^i = \begin{bmatrix} s_0^i & s_1^i & \dots & s_{L-1}^i \end{bmatrix}$, such that s_l^i are equally probable symbols belonging to the alphabet $\{-1, +1\}$. As justified in Section 4.1, we assume a block Rayleigh slow flat-fading channel in additive white Gaussian noise, so that the fading gains are constant within a block of length L and vary independently from block to block.

4.2.1 Tag Generation Process

The chaotic map generates a tag for the i-th transmitted message which is denoted by the row vector $\mathbf{t}^i = \begin{bmatrix} t_0^i & t_1^i & \dots & t_{L-1}^i \end{bmatrix}$, such that $t_l^i \in [-1, +1]$. Each vector element t_{l+1}^i is a function of t_l^i according to the chosen chaotic map and only L iterations after the first σ are transmitted as detailed in Subsection 3.4.2. The legitimate transmitter uses the shared key and the sent message as inputs to the function $M(\cdot)$ to determine the initial condition of the map.

4.2.2 Transmission and Reception

The i-th tagged transmitted signal vector is given by $\mathbf{x}^i = \rho_s \mathbf{s}^i + \rho_t \mathbf{t}^i$, where ρ_s and ρ_t determines the relative energy allocation between the message and the tag, respectively, where the energy of the message and the tag are, respectively, $E_s = L$ and $E_t = LE[(t_k^i)^2]$. The special case $\rho_s = 1$ and $\rho_t = 0$ corresponds to an untagged signal ($\mathbf{x}^i = \mathbf{s}^i$). From now on the untagged system is referred as

the reference system. Thus, for the transmitted signal energy to be equal for a tagged and an untagged signal we have that

$$\rho_t^2 = \frac{1-\rho_s^2}{E[(t_k^i)^2]}. \tag{4.1}$$

The received signal is given by

$$\mathbf{y}^i = h^i\mathbf{x}^i + \mathbf{w}^i = h^i(\rho_s\mathbf{s}^i + \rho_t\mathbf{t}^i) + \mathbf{w}^i. \tag{4.2}$$

where $\mathbf{w}^i = \begin{bmatrix} w_1^i & w_2^i & \cdots & w_L^i \end{bmatrix}$ is a vector of i.i.d. Gaussian random variables with zero mean and variance $\sigma_w^2 = N_0/2$.

The channel signal to noise ratio γ^i is the ratio between the transmitted power and the noise power. The signal to noise ratio for the i-th packet is a random variable and is given by

$$\gamma^i = \frac{(h^i)^2}{\sigma_w^2}, \tag{4.3}$$

and has exponential PDF given by

$$p(\gamma) = \frac{1}{\bar{\gamma}}\exp(-\frac{\gamma}{\bar{\gamma}}), \tag{4.4}$$

where $\bar{\gamma}$ is the average signal to noise ration (SNR) and is given by

$$\bar{\gamma} = \frac{1}{\sigma_w^2}. \tag{4.5}$$

The message to interference ratio (MIR) γ_s^i, is a random variable that represents the ratio between the message power and the interference power at the receiver for the i-th packet and is given by

$$\gamma_s^i = \frac{(h^i)^2\rho_s^2}{(h^i)^2\rho_t^2 + \sigma_w^2} = \frac{\gamma^i\rho_s^2}{\gamma^i\rho_t^2 + 1}. \tag{4.6}$$

It is important to differentiate the signal to noise ratio from the MIR, the SNR is the ratio between the total transmitted power (both message and tag power) and the noise power, while the MIR is the ratio between the power allocated to the message and the interference power (noise power plus power allocated to the tag). The second metric is the tag to noise ratio (TNR), which is the ratio between the average power allocated to the tag and the noise power and is given by

$$\text{TNR} = \frac{\rho_t^2 E[(t_k^i)^2]}{\sigma_w^2}. \tag{4.7}$$

The diagram in Figure 4.1 shows the vectors transmitted and received by each node of the communication system, where $\widetilde{s}$ represents the fraudulent messages sent by Eve.

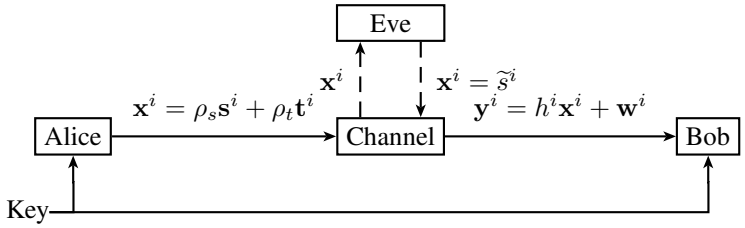


Figure 4.1: *The classical three users scenario of communications over an unsecure channel detailing the vectors transmitted and received by each user.*

4.2.3 The Hypothesis Testing

In this work, we model the authentication procedure as a hypothesis test problem [37]. The tag recovered at the receiver is a noisy version of the transmitted one, so, instead of performing a bitwise comparison between the bits of the recovered tag and the locally generated tag, a correlation is realized between them, resulting in the packet decision statistic τ^i. This decision statistic is chosen as a correlation to explore a property of sequences generated by chaotic maps. These sequences have a high autocorrelation but a low cross-correlation between sequences generated by different initial conditions [23]. The chosen statistic for the i-th transmitted packet is

$$\tau^i = \frac{\frac{\mathbf{y}^i}{h^i} - \rho_s \mathbf{s}^i}{\rho_t} \cdot \mathbf{t}^i, \tag{4.8}$$

where the operator $\cdot$ is the inner product between two vectors. We consider two hypothesis

$$\begin{aligned} \mathcal{H}_0 &: \text{ The tag is not present,} \\ \mathcal{H}_1 &: \text{ The tag is present.} \end{aligned} \tag{4.9}$$

Thus, we have two conditional PDFs $p_{\tau^i|\mathcal{H}_0}(\tau)$ and $p_{\tau^i|\mathcal{H}_1}(\tau)$. It is possible to obtain an expression for τ^i conditioned to the hypothesis $\mathcal{H}_0$

$$\tau^i|\mathcal{H}_0 = \left(\frac{1-\rho_s}{\rho_t}\right) \mathbf{s}^i \cdot \mathbf{t}^i + \frac{\mathbf{w}^i \cdot \mathbf{t}^i}{h^i \rho_t}, \tag{4.10}$$

and conditioned to the hypothesis $\mathcal{H}_1$

$$\tau^i|\mathcal{H}_1 = |\mathbf{t}^i|^2 + \frac{\mathbf{w}^i \cdot \mathbf{t}^i}{h^i \rho_t}. \tag{4.11}$$

For each packet, the vector $\mathbf{t}^i$ is deterministic, so, $\tau^i|\mathcal{H}_0$ and $\tau^i|\mathcal{H}_1$ are the sum of scaled Gaussian random variables, thus both random variables are Gaussian. We define

$$v^i \triangleq \frac{\mathbf{w}^i \cdot \mathbf{t}^i}{h^i \rho_t}, \tag{4.12}$$

Table 4.1: *Conditional probabilities of the hypothesis test.*

True \ Decision	$\mathcal{H}_0$	$\mathcal{H}_1$
$\mathcal{H}_0$	$1-\alpha$	α
$\mathcal{H}_1$	β	$1-\beta$

which is a zero mean Gaussian random variable with variance

$$\sigma_{v_i}^2 = \frac{LE[(t_k^i)^2]\sigma_w^2}{\rho_t^2|h^i|^2} = \frac{LE[(t_k^i)^2]}{\rho_t^2\gamma^i}. \tag{4.13}$$

Thus we have that

$$\begin{aligned} E[\tau^i|\mathcal{H}_0] &= 0 \\ E[(\tau^i|\mathcal{H}_0)^2] &= \sigma_{v_i}^2, \end{aligned} \tag{4.14}$$

and

$$\begin{aligned} E[\tau^i|\mathcal{H}_1] &= |\mathbf{t}^i|^2 \\ E[(\tau^i|\mathcal{H}_1 - E[\tau^i|\mathcal{H}_1])^2] &= \sigma_{v_i}^2. \end{aligned} \tag{4.15}$$

Figure 4.2 depicts the normalized histogram obtained from a Monte Carlo simulation of the distributions of τ^i for both hypothesis, for the tent map with TNR $= -10$ dB and $L = 1024$. It is possible to see that both distributions have the characteristic bell shape, but different mean.

When realizing an hypothesis test two types of errors can be committed: Deciding for $\mathcal{H}_1$ when the correct hypothesis is actually $\mathcal{H}_0$ (type I error or false positive), or deciding for $\mathcal{H}_0$ when the correct hypothesis is $\mathcal{H}_1$ (type II error or false negative). Table 4.1 shows the probability of committing each type of error, where α denotes the probability of false positive and β is the probability of false negative. The main goal in an authentication system is to detect a fraudulent message (with no tag present), thus, the major concern is with false positives. So, a packet decision threshold for the i-th packet τ_0^i is chosen such that

$$\tau^i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \tau_0^i, \tag{4.16}$$

where τ_0^i is selected with the constraint that α must be less than a tolerable failure probability η. So, to determine τ_0^i we must limit the probability of false positive to

$$\alpha = \Pr(\tau^i > \tau_0^i|\mathcal{H}_0) = \int_{\tau_0^i}^{\infty} p_{\tau^i|\mathcal{H}_0}(\tau)d\tau < \eta, \tag{4.17}$$

as $p_{\tau^i|\mathcal{H}_0}(\tau)$ is Gaussian distributed with zero mean, we have that

$$\tau_0^i = \arg\min Q\left(\frac{\tau^i}{\sigma_{v_i}^2}\right) < \eta, \tag{4.18}$$

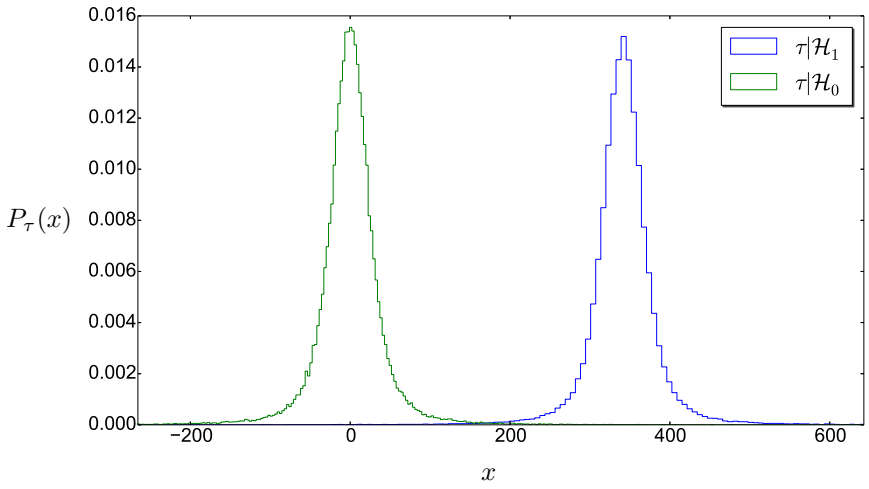


Figure 4.2: *Normalized histogram obtained from a Monte Carlo simulation of the distributions of τ^i for both hypothesis, for the tent map with TNR $= -10$ dB and $L = 1024$.*

where $Q(\cdot)$ is the tail probability of the standard Gaussian distribution [47].

With the probability of false positive limited to η the probability of false negative is given by

$$\beta = \Pr[\tau^i < \tau_0^i | \mathcal{H}_1] = \int_{-\infty}^{\tau_0^i} p_{\tau^i|\mathcal{H}_1}(\tau) d\tau. \tag{4.19}$$

4.2.4 Message Recovery

To recover the messages a maximum a priori (MAP) decoder is used [47]. As discussed in Section 4.2 the n-th received bit of the i-th packet is $y_n^i = h^i x_n^i + w_n^i$, where h^i and w_n^i are as defined in 4.2.2. The signal x_n^i has a hybrid constellation, which is the superposition of an analog and a digital signal. The performance of the message recovery is typically measured by [48]:

- ▷ **The outage probability (P_{out})**: Is the probability that the MIR falls below a threshold γ_0.
- ▷ **The average bit error probability (BER) ($\bar{P}_b$)**: The average bit error probability is the probability that a bit is wrongly decoded by the receiver.

The outage probability is given by

$$P_{\text{out}} = \int_{-\infty}^{\gamma_0} p(\gamma_s) d\gamma_s. \tag{4.20}$$

For the case of the reference system, the performance metrics are well known and are given by [48, 49]

$$P_{\text{out}}^r = 1 - \exp\left(\frac{\gamma_0}{\bar{\gamma}}\right), \tag{4.21}$$

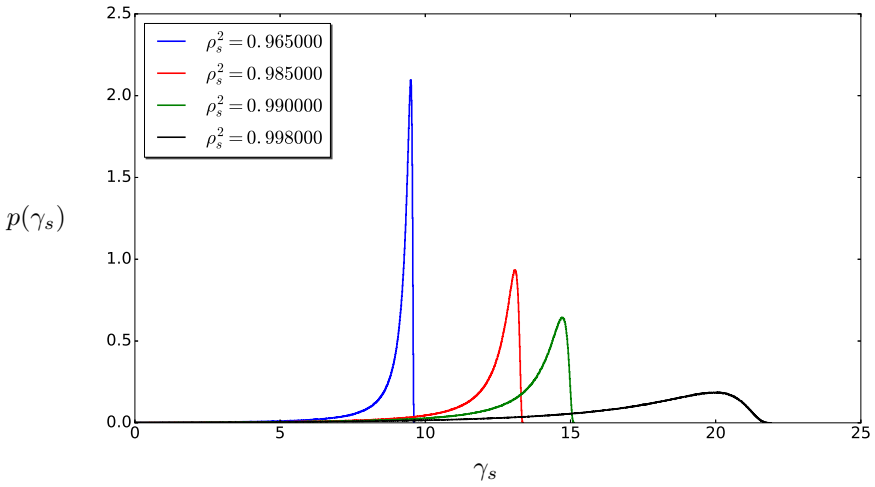


Figure 4.3: *PDF of the MIR with* $\gamma_0 = 6$ *dB and* $P^r_{out} = 0.05$.

$$\bar{P}_b^r = \frac{1}{2}\left[1 - \sqrt{\frac{\bar{\gamma}}{1+\bar{\gamma}}}\right]. \tag{4.22}$$

Additionally we can obtain the necessary SNR for a fixed outage probability by inverting (4.21) which gives

$$\bar{\gamma} = \frac{-\gamma_0}{\ln(1 - P^r_{\text{out}})}. \tag{4.23}$$

In order to evaluate the deviations on the performance of sending a tagged message, a Monte Carlo simulation is realized. The simulated PDF of the MIR for $\gamma_0 = 6$ dB is shown in Figure 4.3 for four different values of ρ_s^2. As seem in the figure, when less power is allocated to the message the likelihood of a lower MIR increases.

We consider a system without authentication designed to operate with a reference outage probability $P^r_{\text{out}} = 0.05$ and we simulate the outage probability if the authentication system is employed for different values of γ_0. The result of the simulation is shown in Figure 4.4. When ρ_s^2 is close to 1 the probability of outage becomes equal to the reference outage probability, but when ρ_s^2 decreases the outage probability increases. It is worth noting that the probability deteriorates faster with the decrease of ρ_s^2 for higher values of γ_0.

A Monte Carlo simulation is used to determine the BER for different values of ρ_s^2. In Figure 4.5 this probabilities are compared with the BER given by (4.22). For a high value of ρ_s^2 (e.g. $\rho_s^2 > 0.985$), the BER is really close to the reference system, however as the power allocated to the message decreases the BER deteriorates significatively.

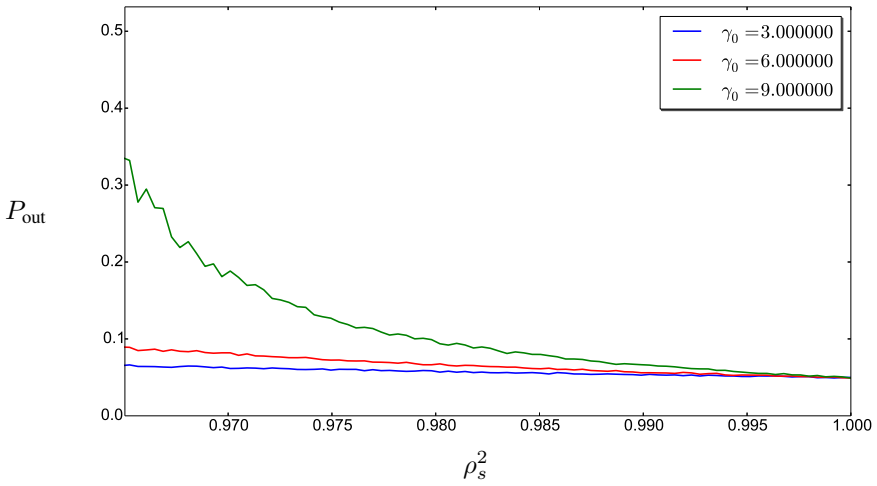


Figure 4.4: *Monte Carlo simulation of the outage probability of system employing embedded authentication tags for* $P_{out}^{r} = 0.05$.

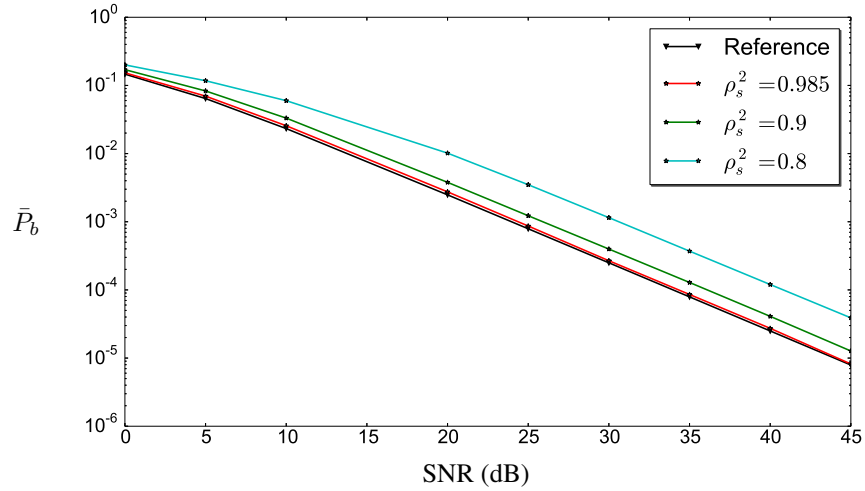


Figure 4.5: *Comparison of the bit error rate of systems employing authentication and the reference system for different values of* ρ_s^2.

4.3 System Design Parameters and the Tradeoffs Involved

So far several parameters of the system have been presented and several performance requirements have been discussed. The system tradeoffs are addressed in this section.

Firstly, the system parameters and the system requirements are summarized and a brief discussion on how each performance metric is affected by each parameter is presented. Secondly, we explain how the performance metrics relate to each other and which compromises must be made in order to

achieve a feasible set of parameters that attend the needs of the user.

4.3.1 System Parameters and Requirements

The physical layer authentication system employing chaotic tags presented in this work has the following parameters:

- ▷ **The Power Allocation**: The power of the transmitted signal is split between the message (ρ_s^2) and the tag (ρ_t^2) and both are sent together in the wireless channel. There is a constraint in the power allocation that $\rho_s^2 + \rho_t^2 = 1$.
- ▷ **The Key Length**: The length of the secret key (K).
- ▷ **The Packet Length and the Time Stamp Length**: The packet length (L) is the length of the transmitted vector. The time stamp length ($K - L$) is the length of the time stamp vector $\mathbf{t}_s$.
- ▷ **Skip Parameter**: The skip parameter (σ) indicates how many iterations of the chaotic map are skipped in the tag generation process.
- ▷ **Failure Threshold**: The failure threshold η is the maximum tolerable probability of authenticating an untagged message. The attacker is considered successful if the probability that a fraudulent message is authenticated is equal or higher than η.

In this work, we consider the following security requirements:

- ▷ **Security Against Impersonation Attacks**: The probability of a successful impersonation attack P_I must be less than η. This probability is affected by K and σ.
- ▷ **Security Against Substitution Attacks**: The probability of a successful substitution attack P_S must be less than η. This probability is affected by K and σ.
- ▷ **Security Against Replay Attacks**: The probability of a successful replay attack P_R must be less than η. This probability is affected by K and L.
- ▷ **Probability of False Positive**: False positive consists in authenticating a message that does not contain a legitimate tag. The probability that this error occurs must be less than η. The probability is affected by ρ_s, ρ_t, by the chaotic map used and by the SNR.
- ▷ **Probability of False Negative**: False negative consists in not authenticating a message that contains a legitimate tag. Ideally, the probability that such error occur would be zero. The probability is affected by L, ρ_s, ρ_t, by the chaotic map used and by the SNR.

Additionally, there are two message recovery metrics considered in this work:

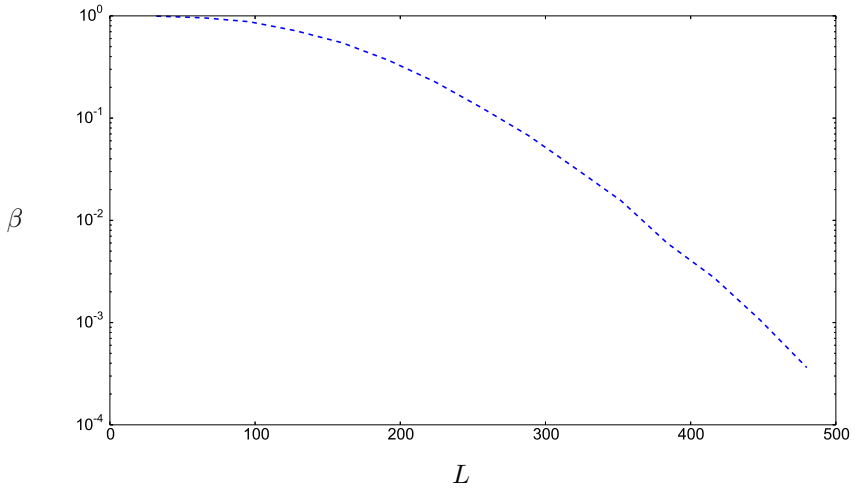


Figure 4.6: *The probability of false negative with* $K = 512$*, SNR* $= 10$ *dB,* $\rho_s^2 = 0.985$ *and* $\eta = 10^{-7}$.

▷ **Outage Probability**: This metric is affected by ρ_s, ρ_t and by the SNR.

▷ **Bit Error Probability**: This metric is affected by ρ_s, ρ_t and by the SNR.

4.3.2 False Negative Versus Key Reuse

The probability of false negative is given by (4.19). The threshold is established based on a constraint on the type I error probability as given by (4.17), hence, it depends only on $\tau^i|\mathcal{H}_0$. If L is increased, with every other parameter fixed, the mean of $\tau^i|\mathcal{H}_1$ increases, and consequently β decreases. As explained in Subsection 3.4.4 the legitimate users can use the same key 2^{K-L} times without compromising the security of the system against replay attacks. So, by increasing L, for a fixed K the number of times a key can be reused decreases exponentially. Figure 4.6 shows how the probability of false negative changes for a varying L, considering that the tag is generated by the tent map with a 512 bits long key, SNR $= 10$ dB, $\rho_s^2 = 0.985$ and for $\eta = 10^{-7}$. The designer has to make a compromise between the tolerable probability of false negative and the number of times the key can be reused. As there are not any security restrictions on the probability of false negative nor on the key reuse factor any value of L can be chosen depending on the designer needs.

4.3.3 False Negative Versus Message Recovery Performance

In Subsection 4.3.2 the possibility of decreasing β by increasing L is evaluated. However, as the decision threshold τ_0^i choice also depends on σ_{v_i}, as shown in (4.18), another way to decrease β would be to decrease σ_{v_i}. As seem in (4.13), σ_{v_i} can be decreased by increasing the power allocated

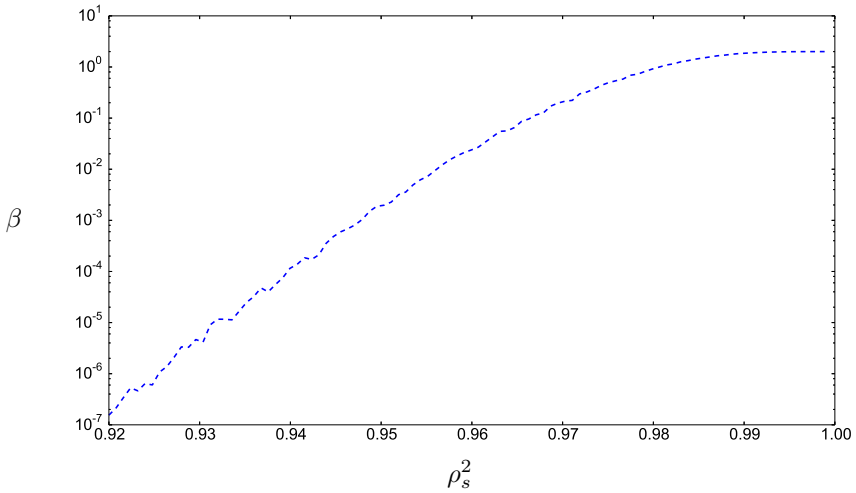


Figure 4.7: *Probability of false negative versus* ρ_s^2*, with* $\eta = 10^{-7}$*,* $L = 128$ *and* $P_{out}^r = 0.05$*.*

to the tag, with all the other parameters fixed. Due to the restriction that $\rho_s^2 + \rho_t^2 = 1$, by increasing ρ_t^2 we have to decrease ρ_s^2. As seem in Section 4.2.4, both message recovery metrics considered in this work strongly depend on the value of ρ_s^2. Figures 4.5 and 4.4 show the simulated BER and the outage probability versus ρ_s^2 considering $P_{out}^r = 0.05$. We can conclude from this figure that both metrics deteriorate with a decrease in ρ_s^2.

In order to assess the effects of changing the power allocation between the message and the tag has in the probability of false negative, in the BER and in the outage probability a simulation of the system is realized considering $\eta = 10^{-7}$, $L = 128$ and $P_{\text{out}}^r = 0.05$. Figures 4.7, 4.8 and 4.9 show the probability of false negative, the bit error rate and the outage probability versus ρ_s^2, respectively. From observing the figures, we conclude that an increase in ρ_s^2 results in an improvement in the BER and in the outage probability, but deteriorates the probability of false negative. As the BER is not as nearly as sensitive to ρ_s^2 a recommended design methodology is to find a value of ρ_s^2 that yields to a probability of outage and false negative adequate to the system requirements.

4.3.4 Transmission Rate Versus Probability of Outage

As explained in Section 4.1 the transmitter does not know the channel gain, thus, he is unaware of the current MIR. The capacity of a communication channel is a theoretical upper bound on the maximum transmission rate for which is possible to establish communications with a negligible probability of error [29]. The capacity of the channel is given by

$$C = B \log_2(1 + \gamma_s), \tag{4.24}$$

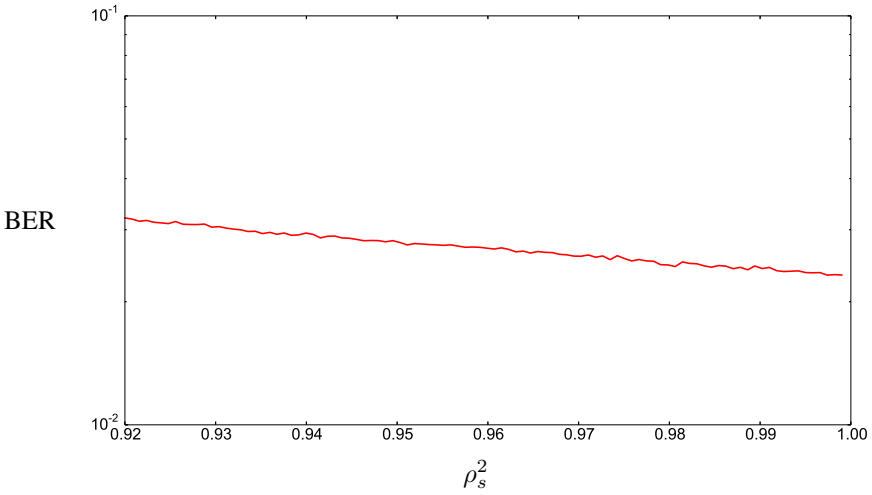


Figure 4.8: *Bit error rate versus* ρ_s^2*, with* $P_{out}^r = 0.05$.

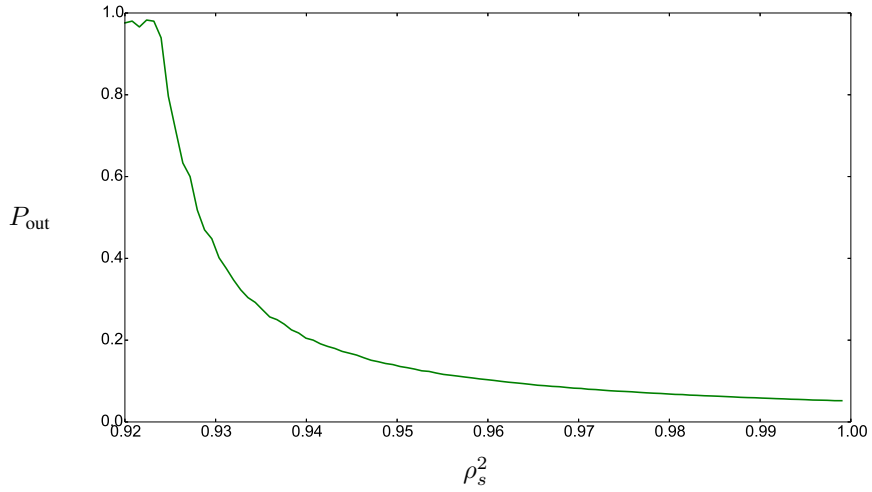


Figure 4.9: *Probability of false negative versus* ρ_s^2*, with* $P_{out}^r = 0.05$.

where B is the bandwidth of the channel. As the transmitter does not know the current MIR he chooses a fixed transmission rate equal to the channel capacity for a $\gamma_s = \gamma_0$. If the transmitter chooses a high value for γ_0 he is able to transmit at a higher rate, however, the probability that he is transmitting at a rate above the capacity increases as well. There is clearly a compromise on the tolerable probability of outage and the transmission rate. Figure 4.10 shows the curve of the channel capacity normalized by the channel bandwidth on the left vertical axis while the right vertical axis shows the probability of outage for γ_0 varying between 3 dB and 12 dB. So, the system designer has the flexibility to choose a value for γ_0 that results in a tolerable probability of outage according to the system requirements and maximizing the transmission rate giving this constraint.

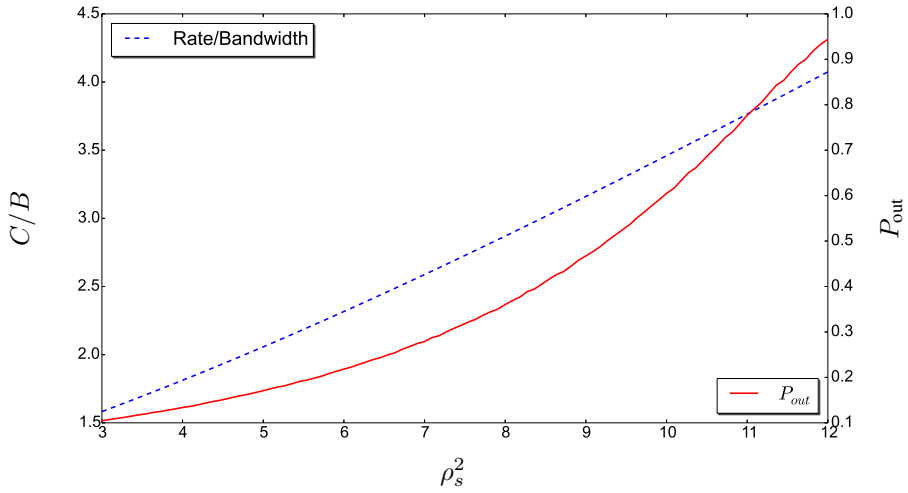


Figure 4.10: *The curves show how γ_0 influences the probability of outage and the capacity of the system.*

4.4 Conclusions

Based on the results of the simulations analyzed in this chapter we can conclude that:

- ▷ The use of an authentication tag deteriorates the bit error rate and the outage probability of the system. However, the system designer is able to tune several parameters in order to achieve a tolerable message recovery performance without compromising the system security.
- ▷ Increasing the length of the message packet reduces the probability of false negative, but decreases the key reuse factor.
- ▷ Increasing the power allocated to the tag reduces the probability of false negative, but increases the BER and the probability of outage.
- ▷ Increasing γ_0 results in a higher transmission rate, but increases the probability of outage.

CHAPTER 5

CONCLUSIONS

This chapter summarizes the contributions made by this work and point for directions for future works in this area.

A minor contribution of this work is to condensate information on how the density evolve in an orbit and how the information flows under a chaotic map. Most of this knowledge is spread out in publications on physics and mathematical journals, but in this work they are presented together from an engineering point of view.

One of the contributions of this paper is to propose a method to determine when in a chaotic orbit the information about the initial condition of a chaotic eventually expanding map is lost. The method uses the derivation chain rule to obtain the derivative of the r-th composition of the map function with itself and the value of the derivative within each partition dictates how the information is spread after each iteration.

Another contribution is the proposition of a novel method to generate physical layer authentication tags based on chaotic functions. While most of the physical layer authentication methods depend on the noise power the method proposed in this work has a lower bound on the information leaked about the secret key even in a noiseless channel. The work also present a comprehensive analysis of the effectiveness of the authentication tags in securing the system and how it affects the message recovery performance. We consider the probability of success of three types of attacks and how to select the system parameters in order to minimize these probabilities and all the tradeoffs involved. The availability of circuits that implement the dynamics of chaotic maps also contributes to the relevance of the proposed method.

5.1 Publications

▷ **Journal Publications**

– C. Souza, J. Evangelista, D.P.B. Chaves, C. Pimentel, "Spectral Analysis of a Chaotic Map Based on the Hyperbolic Tangent Function," *J. of Commun. and Inform. Syst.*, vol. 31, p. 100-107, 2016.

▷ **Conference Publications**

– J. Evangelista, D.P.B. Chaves, C. Pimentel, "Chaotic map sequence as fingerprint for physical authentication system," in *6th Int. Conf. on Nonlinear Science and Complexity, 2016,* Sao Jose dos Campos, p. 73-74, May 2016

5.2 Future Works

Four paths are identified for future directions using this work as starting point.

First, to propose a new method to estimate how the information about the initial condition is lost that covered a broader class of maps. Additionally, a method that did not rely on the assumption that the input density converges to the invariant density after one iteration is desired. Furthermore, a method to obtain the invariant density for a generic map must be developed.

Second, the performance of chaotic tags is only evaluated for slow block fading channels, so it is important to verify how different channel models affect the message recovery performance and the security to attacks of the authentication tag.

Third, to implement a fully digital solution using methods to generate binary sequences from chaotic maps orbits [41, 43]. As the chaotic orbit depends on the initial condition of the map the analog solution presented in this work would need the input to the chaotic circuit to have little to no noise if implemented in real life. In comparison, a fully digital system would not have rigorous noise constraints.

Finally, chaotic signals are spread spectrum, so it is important to evaluate the effect of filtering and bandwidth limited electronic devices would have on the performance of the authentication system.

ABOUT THE AUTHOR

The author was born in Recife on June 21st of 1992. He received his B.Sc degree in Electronics Engineering from the Federal University of Pernambuco in 2015. His research interest include Cryptography, Information theory, Wireless Communications and Signal Processing.

Address: Rua da Harmonia 460
Recife - PE
Brasil

e-mail: jvce92@hotmail.com

Esta dissertação foi diagramada usando LaTeX 2_ε[1] pelo autor.

[1] LaTeX 2_ε é uma extensão do LaTeX. LaTeX é uma coleção de macros criadas por Leslie Lamport para o sistema TeX, que foi desenvolvido por Donald E. Knuth. TeX é uma marca registrada da Sociedade Americana de Matemática ($\mathcal{AMS}$). O estilo usado na formatação desta dissertação foi escrito por Dinesh Das, Universidade do Texas. Modificado por Renato José de Sobral Cintra (2001) e por Andrei Leite Wanderley (2005), ambos da Universidade Federal de Pernambuco. Sua úlltima modificação ocorreu em 2010 realizada por José Sampaio de Lemos Neto, também da Universidade Federal de Pernambuco.

BIBLIOGRAPHY

[1] A. Tanenbaum, *Computer Networks*. Englewood Cliffs, NJ: Prentice Hall, fourth ed., 2002.

[2] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. New York, NY: Cambridge University Press, first ed., 2011.

[3] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing Wireless Systems via Lower Layer Enforcements," in *Proc. of the 5th ACM Workshop on Wireless Security (WiSe'2006)*, (New York, NY, USA), pp. 33–42, ACM, 2006.

[4] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, Jul 2008.

[5] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Military Commun. Conf. (MILCOM'2011)*, pp. 538–542, Nov 2011.

[6] S. V. Vaerenbergh, Ó. González, J. Via, and I. Santamaría, "Physical layer authentication based on channel response tracking using Gaussian processes," in *Proc. of IEEE Int. Conf. on Acoust., Speech, and Signal Process. (ICASSP '14), 2014*, pp. 2410–2414, May 2014.

[7] X. Wu and Z. Yang, "Physical-Layer Authentication for Multi-Carrier Transmission," *IEEE Commun. Lett.*, vol. 19, pp. 74–77, Jan 2015.

[8] J. E. Kleider, S. Gifford, S. Chuprun, and B. Fette, "Radio frequency watermarking for OFDM wireless networks," in *Proc. of IEEE Int. Conf. on Acoust., Speech, and Signal Process. (ICASSP '04), 2004*, vol. 5, pp. 397–400, May 2004.

[9] P. Yu, J. Baras, and B. Sadler, "Physical-Layer Authentication," *IEEE Trans. Inf. Forens. Security*, vol. 3, pp. 38–51, Mar 2008.

[10] P. L. Yu and B. M. Sadler, "MIMO Authentication via Deliberate Fingerprinting at the Physical Layer," *IEEE Trans. Inf. Forens. Security*, vol. 6, pp. 606–615, Sep 2011.

[11] N. Goergen, W. Lin, K. Liu, and T. Clancy, "Extrinsic Channel-Like Fingerprinting Overlays Using Subspace Embedding," *IEEE Trans. Inf. Forens. Security*, vol. 6, pp. 1355–1369, Dec 2011.

[12] J. L. Massey, *Lecture Notes on Applied Digital Information Technology II*.

[13] P. L. Yu, G. Verma, and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Commun. Mag*, vol. 53, pp. 48–53, Jun 2015.

[14] K. T. Alligood, T. Sauer, and J. A. Yorke, *Chaos : an introduction to dynamical systems*. New York, NY: Springer, 1996.

[15] S. H. Strogatz, *Nonlinear dynamics and chaos : with applications to physics, biology, chemistry, and engineering*. Cambridge, MA: Westview Press, second ed., 2014.

[16] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Lett.*, vol. 64, pp. 1196–1199, Mar 1990.

[17] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos. I . Fundamentals of digital communications," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 44, pp. 927–936, Oct 1997.

[18] F. C. Lau and C. K. Tse, *Chaos-Based Digital Communications*. Berlin, Germany: Springer-Verlag, first ed., 2003.

[19] A. Beirami and H. Nejati, "A Framework for Investigating the Performance of Chaotic-Map Truly Random Number Generators.," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 60, no. 7, pp. 446–450, 2013.

[20] L. Kocarev and S. Lian, *Chaos-based Cryptography*. Berlin, Germany: Springer-Verlag, first ed., 2011.

[21] L. Kong, G. Kaddoum, and M. Taha, "Performance analysis of physical layer security of chaos-based modulation schemes," in *IEEE 11th Int. Conf. on Wireless and Mobile Computing, Networking and Commun. (WiMob), 2015*, pp. 283–288, Oct 2015.

[22] A. Lasota and M. C. Mackey, *Probabilistic Properties of Deterministic Systems*. New York, NY: Cambridge University Press, first ed., 1985.

[23] S. H. Isabelle, *A signal processing framework for the analysis and application of chaos* . PhD thesis, MIT, Massachussets, 1995.

[24] S. H. Isabelle and G. W. Wornell, "Statistical properties of one-dimensional chaotic signals," in *Proc. of IEEE Int. Conf. on Acoust., Speech, and Signal Process. (ICASSP '95), 1995*, vol. 2, pp. 1352–1355, May 1995.

[25] A. Boyarsky and M. Sacrowsky, "On a class of transformations which have unique absolutely continuous invariant measures," *Trans. of the Amer. Math. Soc.*, vol. 255, pp. 243–262, 1979.

[26] N. Friedman and A. Boyarsky, "Matrices and Eigenfunctions Induced by Markov Maps," *Linear Algebra Applicat.*, vol. 38, pp. 141–147, Jun 1981.

[27] H. Minc, *Nonnegative matrices*. New York, NY: Wiley, first ed., 1988.

[28] S. Wong, "Some Metric Properties of Piecewise Monotonic Mappings of the Unit Interval," *Trans. of the Amer. Math. Soc.*, vol. 246, pp. 493–500, 1978.

[29] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY: Wiley, second ed., 2006.

[30] R. Metzler, Y. Bar-Yam, and M. Kardar, "Information flow through a chaotic channel: Prediction and postdiction at finite resolution," *Phys, Rev. E*, vol. 70, Aug. 2004.

[31] K. Binder and D. Heermann, *Monte Carlo Simulation in Statistical Physics*. New York, NY: Springer, fifth ed., 2010.

[32] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. New York, NY: Springer, first ed., 2009.

[33] W. Stallings, *Cryptography and Network Security: Principles and Practice*. New York, NY: Pearson Education, third ed., 2002.

[34] "Security Architecture for Open Systems Interconnection for CCIT Applications," Tech. Rep. X800, International Telecommunication Union, Geneva, CH, 1991.

[35] M. Bellare, *Lecture Notes on Introduction to Modern Cryptography*.

[36] M. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functions for Message Authentication," in *Proc. of the 16th Annu. Int. Cryptology Conf. on Advances in Cryptology*, (London, UK), pp. 1–15, 1996.

[37] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, pp. 1350–1356, Jul 2000.

[38] G. J. Simmons, "A survey of information authentication," *Proc. IEEE*, vol. 76, pp. 603–620, May 1988.

[39] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of secure watermark-based authentication systems," *IEEE Trans. Inf. Forens. Security*, vol. 1, pp. 43–55, Mar 2006.

[40] C. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct 1949.

[41] A. Beirami, H. Nejati, and W. H. Ali, "Zigzag map: a variability-aware discrete-time chaotic-map truly random number generator," *Electron. Lett.*, vol. 48, pp. 1537–1538, Nov 2012.

[42] D. P. B. Chaves, C. E. Souza, and C. Pimentel, "A new map for chaotic communication," in *Int. Telecommunications Symp. (ITS), 2014* , pp. 1–5, Aug 2014.

[43] H. Nejati, A. Beirami, and Y. Massoud, "A realizable modified tent map for true random number generation," in *51st Midwest Symp. on Circuits and Syst.*, (Knoxville, TN), pp. 621–624, Aug 2008.

[44] S. Callegari, G. Setti, and P. J. Langlois, "A CMOS tailed tent map for the generation of uniformly distributed chaotic sequences," in *Proc. of 1997 IEEE Int. Symp. on Circuits and Syst. (ISCAS'97)*, vol. 2, pp. 781–784, Jun 1997.

[45] E. D. M. Hernandez, G. Lee, and N. H. Farhat, "Analog realization of arbitrary one-dimensional maps," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, pp. 1538–1547, Dec 2003.

[46] J. Lopez-Hernandez, A. Diaz-Mendez, R. Vazquez-Medina, and R. Alejos-Palomares, "Analog current-mode implementation of a logistic-map based chaos generator," in *52nd IEEE Int. Midwest Symp. on Circuits and Syst.*, pp. 812–814, Aug 2009.

[47] J. G. Proakis, *Digital Communications*. New York, NY: McGraw-Hill, fifth ed., 2008.

[48] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, first ed., 2005.

[49] T. Rappaport, *Wireless Communications: Principles and Practice*. Englewood Cliffs, NJ: Prentice Hall, second ed., 2001.