國立交通大學

應用數學系

碩 士 論 文

運用連結邏輯斯諦映射在無線保密通訊上

Using Coupled Logistic Maps in Wireless Secure Communcation

研 究 生：王定國

指導教授：張書銘　博士

中 華 民 國 一 百 年 六 月

運用連結邏輯斯諦映射在無線保密通訊上

Using Coupled Logistic Maps in Wireless Secure Communcation

研 究 生：王定國　　Student: Ting-Kuo Wang

指導教授：張書銘　博士　　Advisor: Dr. Shu-Ming Chang

國 立 交 通 大 學

應 用 數 學 系

碩 士 論 文

A Thesis

Submitted to Department of Applied Mathematics

College of Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master

in

Applied Mathematices

June 2011

Hsinchu, Taiwan, Republic of China

中 華 民 國 一 百 年 六 月

運用連結邏輯斯諦映射在無線保密通訊上

學生：王定國　　　　　　　　　　　　　　　指導教授：張書銘　博士

國立交通大學應用數學系（研究所）碩士班

摘　要

本論文運用連結邏輯斯諦映射 (coupled logistic map) 於無線保密通訊上，並提出一些關於在實驗與模擬結果上的分析。在數值模擬過程中，藉由具有混沌性質 (chaotic behavior) 的連結邏輯斯諦映射參數作為加密金鑰 (key)，應用於無線安全通訊中。此安全通訊已被實現於實作的實驗之中，本論文要藉由數值模擬來匹配實驗的結果。最後，找出了關於該項無線安全通訊系統的效率方程，提供在實作上最有效率的傳輸設定。

關鍵詞：連結邏輯斯諦映射、無線安全通訊、漸近同步。

Using Coupled Logistic Maps in Wireless Secure Communcation

Student: Ting-Kuo Wang Advisors: Dr. Shu-Ming Chang

Department (Institute) of Applied Mathematics

National Chiao Tung University

Abstract

In this thesis, we apply coupled logistic maps to cryptography in Wireless Secure Communication, and give some analyses in numerical simulations to compare with the experiments. In numerical simulations, we choose suitable parameters which have chaotic behavior in the coupled logistc map, and then apply it to Wireless Secure Communications. Wireless Secure Communication was realized in the experiment. In this thesis, we simulate numerically to fit the results of the experiments, and propose an efficient function for Wireless Secure Communication.

Keywords: Coupled logistic map, Wireless Secure Communication, asymptotical synchronization.

誌　謝

完成這本論文，首先我要感謝我的指導教授張書銘博士，在過去兩年間的教誨，老師不僅僅教導我解決問題的辦法，還有面對問題跟困難的態度。在碩士生涯中，希望我們不只是在念碩士而已，並要求我們對於日後有所規劃，對人生有所想法。積極面對問題，克服困難。感謝老師的教誨。同時也要感謝莊正教授和莊重教授願意擔任我的口試委員，和指導和指正論文上的缺失和疏漏。

在論文的撰寫中，感謝莊重老師的指導，在老師的混沌與同步課程中，我學習到和書本上不同的看法，老師在課堂上常常啟發我們對於問題不同的觀點，跳脫傳統，並鼓勵我們勇於嘗試這些問題。在我的論文碰到困難時，老師也不吝指教。

在此要特別感謝莊正老師的幫忙，莊正老師不僅提供我們實驗的數據，也提出一些寫作的觀點和看法，和在不同領域的老師合作，我所學習到的是不同於在數學系中的內容，更豐富了我的論文。

感謝在我背後一直支持我的家人，媽媽和姐姐，媽媽獨力扶養我，雖然家境不是很好，但是媽媽和姐姐還是很努力的提供我跟別人相同的環境與資源，讓我能夠無後顧之憂的不斷向前，在為了完成我的學業的同時也犧牲了許多你們想要的夢想。謝謝你們的無私，這份榮耀我希望與你們一同分享。

最後要感謝我生命中一個很重要的人婉如，謝謝你在我求學時期時的陪伴，常常做我的心靈導師，給我一些建議，分擔我的煩惱。這一路上幸好有你的相伴，讓我走的如此順利，希望能和你一起分享這份喜悅。

王定國

謹誌于交通大學

2011 年 6 月

Contents

List of Tables

List of Figures

1 Introduction

Information security is a very important topic today. Personal information or company's documents or national security, we protect our secret hard. Mathematicians propose the cryptography to secure those information. However, past cryptographic algorithm was constructed by algebra or number theory. But recently, some scientists construct a new type cryptographic algorithm. It is different with past algorithm. The new type cryptographic algorithm is built by dynamical system. There is a very special behavior in dynamical systems, chaos. What is chaos? Chaos is in everywhere. Shape of smoke, shape of cream in a coffee cup, erratic weather patterns, population of fish etc. Exactly, chaos is not only in the life, but also in the mathematics. Mathematicians try to describe it and define it exactly[8, 20], and study its behavior and find the characteristic movement. We apply its special behavior to secure the communication system. Chaotic behavior exists in some orbits of dynamical systems, we call it chaotic orbit. A chaotic orbit is generated by a non-linear system is irregular, aperiodic, unpredictable, and sensitive dependence on initial conditions. These characteristics coincide with properties of the cryptography [2]. In recent years, chaos was been applied widely to secure systems. In particular, 1-dimensional chaos has been thoroughly researched. For example, logistic map, is used to generate a chaotic masking sequence, which is applied to the secure system [7, 15, 25, 26, 27, 31, 38]. The logistic map L is defined by

$$x^{(i)} = L(\gamma, x^{(i-1)}) = \gamma x^{(i-1)}(1 - x^{(i-1)}),$$

$i = 1, 2, \ldots$, where the initial value $x^{(0)} \in [0, 1]$ and the parameter $\gamma \in (0, 4]$. In recent years, so many scientists construct a new crpto-system by dynamical system. Generally, we can divide it into three kinds. First, scientists construct a crpto-system by electric circuit[15, 38]. Second, some scientists construct a suitable crpto-system algorithm for dynamical systems[9, 10, 25]. Last, other scientists construct a crypto-system model by dynamical systems, and take a simulation to analyse it[3, 23]. However, there are still some problems in the crypto-system which is constructed by dynamical system. For example, the chaos is defined in the infinite uncountable set, but the operation of cryptography is in the finite set. Chaotic behavior maybe be weak with the finite precision. The problem will be discussed on the later section.

2 Stream Cipher

2.1 Stream Cipher

Vernam cipher (One-Time-Pad), is the predecessor of stream cipher. In 1917, Gilbert Vernam constructed the system to communicate for applying in automatic encryption and decryption of the telegraph messages. The One-Time-Pad was thought for many years to be an "unbreakable" crypto-system, but there was no proof until Shannon appeared. In 1949, Claude Shannon presented the "Communication Theory of Secrecy Theorems". The paper greatly has affected the development of the secure communication. Shannon applyed probability to build the concept of the secure system. And according to the One-Time-Pad, Shannon propose a more general algorithm, stream cipher.

In our work, we propose a crypto-system by stream cipher. Stream cipher converts plaintext to ciphertext 1 bit at a time. In stream cipher algorithm, there is a keystream which is generated by keystream generator. The keystream generator generates a series of keystream through the key. We can regard the keystream as the encrypting sequence. We mix keystream and plaintexts to produce ciphertexts by XOR operator(exclusive or). Hence, this crypto-system is suitable in hardware. Here is the definition of stream cipher.

Definition 2.1. *(Stream Cipher)*[34] *A* ***stream cipher*** *is a tuple* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F}, \mathcal{E}, \mathcal{D})$, *where the following conditions are satisfied:*

1. *$\mathcal{P}$ is a finite set of the possible plaintexts.*
2. *$\mathcal{C}$ is a finite set of the possible ciphertexts.*
3. *$\mathcal{K}$, the key space, is finite set of possible keys.*
4. *$\mathcal{L}$ is a finite set called the keysteam alphabet.*
5. *$\mathcal{F}$=$(f_1, f_2, \ldots)$ is the keystream generator. For $i \geq 1$,*

$$f_i : \mathcal{K} \times \mathcal{P}_{i-1} \to \mathcal{L}.$$

6. *For each $z \in \mathcal{L}$, there is an encryption rule $e_z \in \mathcal{E}$ and a corresponding decryption rule $d_z \in \mathcal{D}$. $e_z : \mathcal{P} \to \mathcal{C}$ and $d_z : \mathcal{C} \to \mathcal{P}$ are functions such that $d_z(e_z(x)) = x$ for every plaintext $x \in \mathcal{P}$.*

Remark 2.2.

1. *Following previous definition, we can figure out that the cryptography is operated on a finite set.*

2. *In cryptography, a stream cipher is synchronous if the key stream is independent of the plaintext string, that is, the key stream is generator as a function only of the key.*

Example 2.3. *Suppose $m = 4$ and the key stream is generated using the rule,*

$$z_{i+m} = z_i + z_{i+1} \mod 2 \tag{1}$$

If start with $(1, 0, 0, 0)$, the keystream is

$$L = 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, \ldots$$

and we mix it with plaintexts to produce ciphertexts. In this example, the key is m, keystream is L, keystream generator is (1).

2.2 Chaotic Stream Cipher

If a keystream of a stream cipher system is generated by chaotic system, we call the cryptosystem is chaotic stream cipher system. Mathematicians take an innovation in chaotic stream cipher system by the dynamical system. In 1989, Robert Matthews first applied the nonlinear function logistic map to cryptography[8], he proposed a generalised logistic map and replaced the keystream generator by the chaotic map to generator keystream, and given a simple digital cryptographic example. In the 1990s, Chua etc.[15] study the chaotic system by the experiment, and they created the Chua' circuit. They replaced the keystream with a chaotic analog string which was generated by Chua' circuit. However, if we desire to perform the chaotic string in the hardware widely, we have to modify the chaotic system to digitize. In 1993, Douglas R. Frey popularized Matthews's idea, he digitized the chaotic system and built a more general crypto-algorithm "approach to secure communication"[10]. They construct algorithms of chaotic stream cipher by the familiar chaotic systems or modified familiar chaotic systems. All of them are very difference with the past stream cipher in cryptography. No matter what, the purpose of keystream is that ciphertext looks like random string. But sometimes, chaotic system can not reveal chaotic behavior on computers. Because the precision of the computer alphabet is finite, some chaotic system will be led into a short output cycle length. To solve this problem, we will discuss some methods to solve that in Section 3.

Example 2.4. *(Robert Matthews 1989) A general logistic map is defined by*

$$g(x) = \lambda x(\alpha - x)^\beta,$$

let $\lambda = 8.198790355$*,* $\alpha = 1$*,* $\beta = 2.53$*, and the initial value* $x_0 = 0.45$*, we have* $x_1 = 0.81298077$*,* $x_2 = 0.095875139$*,* $x_3 = 0.609135158$*,* $x_4 = 0.463757308$*. We take the last of representation of value, and module it by 25. We get a keystream 2,14,8,8,23. CHAOS will be EVIWQ.*

3 Chaotic transmission

3.1 Chaos

Chaos is a complex behavior of dynamical systems. It appears to be random, yet it is deterministic. It is predictable over a short time, but it is not over a long time. Mathematicians identify chaos behavior though the mathematic definition exactly. In 1963, Lorenz tried to model the unpredictable behavior of the weather[22], Lorenz attractor. In Lorenz attractor, we can see a embryo of the chaotic behavior in the dynamical system. In 1979, Guckenheimer and Williams proposed a geometric model to describe the Lorenz attractor[12]. But mathematicians proved that the Lorenz attractor exists until 1999 by Tucker[36]. However, the exactly mathematical definition of chaos appeared from 1975. In 1975, chaos, the word appeared in the paper of Li and Yorke[20](Definition 3.1). They describe the chaotic behavior through the mathematic analysis. In 1989, Devaney propose another definition of the chaos[8](Definition3.2). In 1994, Robinson modifies the Devaney definition, and giving a reason in his book[29]. In our work, we theorize about the chaotic behavior of dynamical systems through computing Lyapunov exponents. Based on a coupled map lattice [4, 5, 6, 14, 17, 19, 21, 23], a coupled logistic map will be constructed in our model. This coupled logistic map possesses hyperchaos under choosing suitable parameters. We apply the coupled logistic map in a masking sequence to secure communications.

Definition 3.1. *(Li and Yorke sense 1975)*[1] *A system is chaotic if it contains infintely many periodic orbits whose periods are arbitrarily large.*

Definition 3.2. *(Devaney 1989)*[1] *A map* f *on an invariant set* J *is chaotic if*

1. $f|J$ *is topologically transitive.*

2. f *has sensitive dependence of initial conditions on* J*.*

3. periodic points are dense in J.

Remark 3.3. *Robinson* [1, 29] *identified the definition (1) (2) which is defined by Devaney, but he deleted (3). He given some suggestions about his argument in his book*[29].

3.2 Lyapunov exponent

The definition of Lyapunov exponents (2) can be traced back to the dissertation of Lyaponov in 1892 [24]. Lyapunov exponents measure the exponential rate at which nearby orbits are moving apart [29]. According to Birkhof Ergodic Theorem (Theorem 3.12), it shows that Lyapunov exponents is constant almost everywhere. And by the Multiplicative Ergodic Theorem (Theorem 3.13), there are at most n-different Lyapunov exponents for an n-dimensional dynamical system. A dynamical system is chaotic, if it has at least one positive Lyapunov exponent and invariant on a bounded region [32]. Moreover, if there are equal to or more than two positive Lyapunov exponents, the system is called hyperchaos [30].

Definition 3.4. *(Lyapunov exponent one-dimension)* [29] *Let $f : \mathbb{R} \to \mathbb{R}$ be a C^1 function. For each point x_0, define the Lyapunov exponent of x_0, $\lambda(x_0)$, as follows:*

$$\begin{aligned} \lambda(x_0) &= \limsup_{n\to\infty} \frac{1}{n} \log(|(f^n)'(x_0)|) \qquad (2) \\ &= \limsup_{n\to\infty} \frac{1}{n} \sum_{j=0}^{n-1} \log(|f'(x_j)|), \end{aligned}$$

where $x_j = f^j(x_0)$.

From the previous definition, we can infer it simply. $\log|(f^n)'(x_0)| \approx n\lambda(x_0)$ or $|(f^n)'(x_0)| \approx e^{n\lambda(x_0)} = L(x_0)^n$, where $L(x_0) = e^{\lambda(x_0)}$. By the fundamental calculus theorem,

$$|f^n(x_0 + \delta) - f^n(x_0)| \approx |(f^n)'(x_0)| \approx |\delta| L(x_0)^n. \qquad (3)$$

If $\lambda(x_0) < 0$, the equation (3) will converge to 0. Similarly, if $\lambda(x_0) > 0$, the equation (3) will diverge. We can image that the orbit will diverge in a bounded region. The orbit is restricted in the bounded region, but the orbit still grow up. The orbit will be very sensitive dependence on initial conditions. Hence, when Lyapunov exponent is negative, nearby orbits converge; and when it is positive, nearby orbit diverge. And it conform to the Devaney's (Definition 3.2).

Example 3.5. *(tent map) Let*

$$T(x) = \begin{cases} 2x & for \quad 0 \le x \le 0.5, \\ 2(1-x) & for \quad 0.5 \le x \le 1. \end{cases}$$

If x_0 is such that $x_j = T(x_0) = 0$ for some j, then the $\lambda(x_0)$ does not exist. Since the tent map is not smooth at $x = 0.5$. For other $x_0 \in [0,1]$, $|f'(x_j)| = 2$ for all j, so by (Definition 3.4), the Lyapunov exponent is $\log(2)$.

Definition 3.6. *(Lyapunov exponent high-dimension)* [29] *Let Let $f : \mathbb{M} \to \mathbb{M}$ be a diffeomorphism on a manifold of dimension m. Let$\|\cdot\|$ be the norm on the tangent vectors induced by a Riemannian metric (inner product on tangent vectors) on $\mathbb{M}$. For each $x \in \mathbb{M}$ and $v \in T_x\mathbb{M}$, let*

$$\lambda(x,v) = \lim_{k\to\infty} \frac{1}{k} \log(\|Df_x^k v\|) \tag{4}$$

whenever this limit exists.

We consider that $\|Df_x^k v\|$ in (4).

$$\begin{aligned} \|Df_x^k v\|^2 &= (Df_x^k v)^T Df_x^k v \\ &= v^T[(Df_x^k)^T]Df_x^k v. \end{aligned}$$

The matrix $[(Df_x^k)^T Df_x^k]$ is symmetric and positive definite. Therefore, $[(Df_x^k)^T Df_x^k]^{1/2}$ measures how much lengths are changed by Df_x^k, and $[(Df_x^k)^T Df_x^k]^{1/2k}$ measure the average amount vectors are stretched, the limit

$$\lim_{k\to\infty} [(Df_x^k)^T Df_x^k]^{1/2k} = \Lambda_x$$

exits[29]. The logarithm of the eigenvalues of Λ_x are the Lyapunov exponents. The eigenvalues of Λ_x is the singular values of Df_x^k. Hence, we also can compute the Lyapunov exponents in high dimension by singular value decomposition.

Definition 3.7. [33] *Let A be an $m \times n$ matrix of rank r with positive singular values $\sigma_1 \ge \sigma_2 \ge \cdots \ge \sigma_r$. A factorization $A = U\Sigma V^*$ where U and V are unitary matrices and Σ is the $m \times n$ matrix defined by*

$$\Sigma_{ij} = \begin{cases} \sigma_i & if \ i = j \le r, \\ 0 & ortherwise. \end{cases}$$

is called a singular value decomposition of A.

Definition 3.8. *(Lyapunov exponent high-dimension (Ruelle))*[29] *Let* $J_{n,x_0} = Df^n(x_0) = Df^n(x)|_{x=x_0}$. $\mathbb{N}$ *is an unit ball.* r_i^n = *the length of the* i*-th orthogonal axes of the ellipsoid* $J_n\mathbb{N}$ *for an orbit with initial point* x_0*. The* i*-th Lyapunov exponent of* f *with initial point* x_0 *is*

$$\limsup_{n\to\infty} \frac{\ln r_i^n}{n},$$

where r_i^n : *the singular value of* J_n.

Example 3.9. *(Lyapunov exponents of Coupled logistic map)*

$$(x_1^{(i+1)}, x_2^{(i+1)}) = \begin{bmatrix} 1-c_1 & c_1 \\ c_2 & 1-c_2 \end{bmatrix} \begin{bmatrix} \gamma_1 x_1^{(i)}(1-x_1^{(i)}) \\ \gamma_2 x_2^{(i)}(1-x_2^{(i)}) \end{bmatrix}, \tag{5}$$

and

$$DF(x_1, x_2) = \begin{bmatrix} (1-c_1)r_1(1-2x_1) & c_1 r_2(1-2x_2) \\ c_2 r_1(1-2x_1) & (1-c_2)r_2(1-2x_2) \end{bmatrix}, \tag{6}$$

given a vector $u^0 \in [0,1]\times[0,1]$*. and we have that*

$$DF^k_{\boldsymbol{x}_0} = DF_{\boldsymbol{x}_{k-1}} \cdots DF_{\boldsymbol{x}_0}, \tag{7}$$

where $\boldsymbol{x}_j = F^j(\boldsymbol{x})$

Set

$$\delta x^{(i+1)} = DF_{x_i} u^{(i)},$$
$$u^{(i+1)} = \delta x^{(i+1)} / \|\delta x^{i+1}\|,$$

by the equation (7)*, we have*

$$\begin{aligned} DF^k_{\boldsymbol{x}_0} u^{(0)} &= DF_{\boldsymbol{x}_{k-1}} \cdots DF_{\boldsymbol{x}_0} u^{(0)} \\ &= DF_{\boldsymbol{x}_{k-1}} \cdots DF_{\boldsymbol{x}_1} \delta x^{(1)} \\ &= DF_{\boldsymbol{x}_{k-1}} \cdots DF_{\boldsymbol{x}_1} (u^{(1)} \|\delta x^{(1)}\|) \\ &= \|\delta x^{(k)}\| \cdots \|\delta x^{(1)}\| u^{(k)}, \end{aligned}$$

and by the definition of Lyapunov exponent (Definition 3.6)*, we have*

$$
\begin{aligned}
\lambda(x,u) &= \lim_{k\to\infty} \frac{1}{k} \log(\|Df_x^k u\|) \\
&= \lim_{k\to\infty} \frac{1}{k} \log \|\delta x^{(k)}\| \cdots \|\delta x^{(1)}\| u^{(k)} \\
&= \lim_{k\to\infty} \frac{1}{k} \log \|u^{(k)}\| \prod_{i=1:k} \|\delta x^{(i)}\| \\
&= \lim_{k\to\infty} \frac{1}{k} \|u^{(k)}\| \sum_{i=1:k} \log \|\delta x^{(i)}\|,
\end{aligned}
$$

and the result in the figure (1)*. The algorithm is from* reference [28].

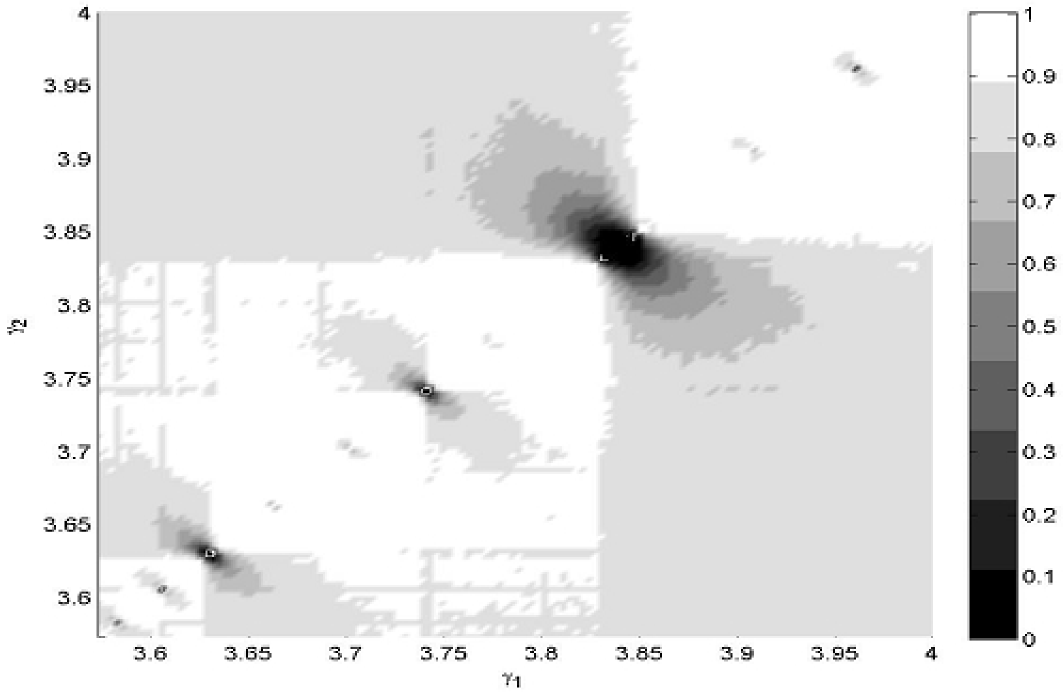

Figure 1: Lyapunov exponent. The horizontal axis represents the parameter γ_1 in the coupled logistic map. The vertical axis represents the parameter γ_2 in the coupled logistic map. Each site represents the rate of chaotic behavior in the coupled logistic map, i.e. the figure represents the key space of the crypto-system.

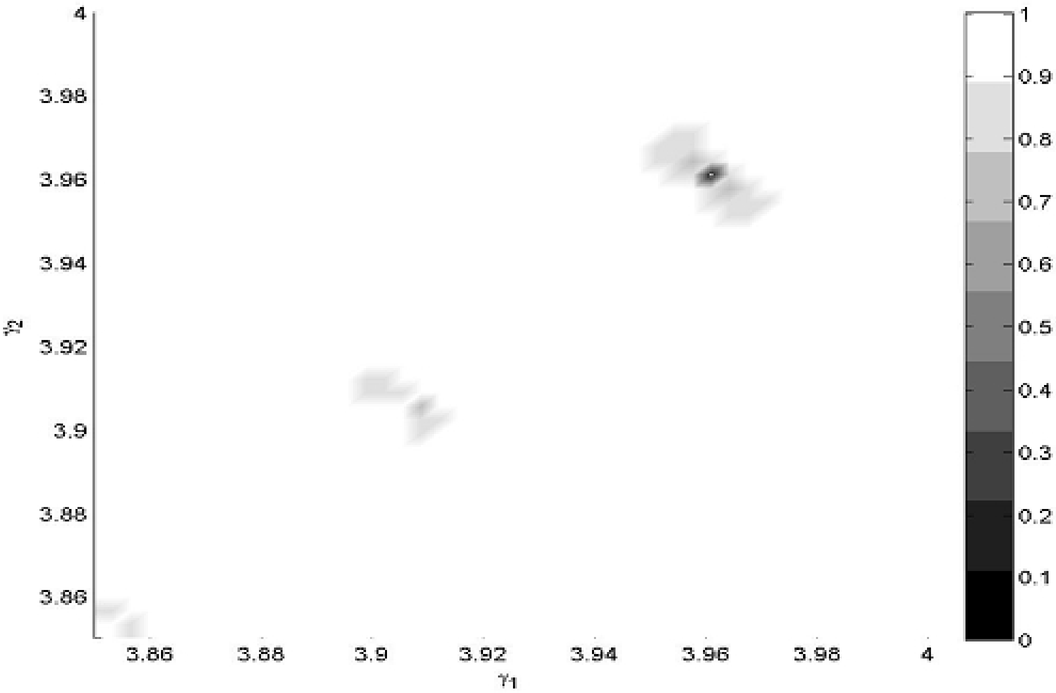

Figure 2: Lyapunov exponent. It is the part of Figure 1. We observe that there is a high density region of the chaotic behavior.

Definition 3.10. *(Measure preserving transformation)* [29] *A measure μ is a invariant for a map $f : X \to X$ provided $\mu(f^{-1}(A)) = \mu(A)$ for all measurable sets A. If μ is an invariant measure for f, f is also said to be a* measure preserving transformation for μ.

Definition 3.11. *(Ergordic with respect to an invariant measure)* [29] *A map $f : X \rightharpoonup X$ is called ergordic with respect to invariant measure μ provided $\mu(X \backslash A) = 0$ for any measurable invariant set A for f with $\mu(A) > 0$.*

Theorem 3.12. *(Birkhof Ergodic Theorem)* [29] *Assume $f : X \to X$ is measure preserving transformation for the measure μ. Assume $g : X \to \mathbb{R}$ is a μ-integrable function. Then,*

1. *$\lim_{n\to\infty}(\frac{1}{n})\sum_{j=0}^{n-1} g \circ f^j(x)$ converges $\mu -$ almost everywhere to an intergrable function g^*.*

2. *g^* is f invariant wherever it is defined, i.e., $g^* \circ f(x) = g^*(x)$ for μ-almost all x.*

3. *if $\mu(X) < \infty$, then $\int_X g^*(x)d\mu(x) = \int_X g(X)d\mu(x)$,and if μ is an ergodic measure for f, then g^* is a constant μ-almost everywhere.*

In addition, if f is ergodic, then g^* is constant a.e., and so $g^* = \frac{\int f dm}{m(x)}$. It means that time average equal space average.

To correspond to (Definition 2), Let f be f in (Theorem 3.12), $g(x) = \log(x)$. If we find the measure μ such that f be a measure preserving transformation for μ, $g(x)$ is μ-integrable function. Then we can apply Theorem 3.12 to realize that Lyapunov exponent is constant a.e..

Theorem 3.13. *(Multiplicative Ergodic Theorem)*[29] *Let M be a compact manifold of dimension m, β be the σ-algebra generates by the Borel subsets of M, and $f : M \to M$ be C^2 diffeomorphism. Then, there is an invariant set $B_f \in \beta$ of the full measure for every $\mu \in \mathcal{M}(f)$ such that the Lyapunov exponents exist for all points $x \in B_f$. Where $\mathcal{M}(f)$ is the set of all invariant Borel probability measures for f. More precisely, the following properties are true.*

1. *The set B_f is invariant, $f(B_f) = B_f$, and of full measure, $\mu(B_f) = 1$ for all $\mu \in \mathcal{M}(f)$.*

2. *For each $x \in B_f$, the tangent space at x can be written as an increasing set of subspaces*

$$\{0\} = V_x^0 \subset V_x^1 \subset \cdots \subset V_x^{s(x)} = T_x M$$

such that for $v \in V_x^j \backslash V_x^{j-1}$ the limit defining $\lambda(x, v)$ exists and $\lambda_j(x) = \lambda(x, v)$ is the same value for all such v, and the bundle of subspaces

$$\{V_x^j : x \in B_f \text{ and } s(x) \geq l\}$$

are invariant in the sense that $Df_x V_x^j = V_{f(x)}^j$ for all $1 \leq j \leq s(x)$.

3. *The function $s : B_f \to \{1, \ldots, m\}$ is a measurable function and invariant, $s \circ f = s$.*

4. *If $x \in B_f$, the exponents satisfy*

$$-\infty \leq \lambda_1(x) < \lambda_2(x) < \cdots < \lambda_{s(x)}(x).$$

(Note that we allow $\lambda_1(x) = -\infty$.) For $1 \leq j \leq m$, the function $\lambda_j(\cdot)$ is defined and measurable on the set

$$\{x \in B_f : s(x) \geq j\},$$

and is invariant, $\lambda_j \circ f = \lambda_j$.

From previous (Theorem 3.13), it states that there are at most n different Lyapunov exponents in n-dimensional space. And the limit (4) exists for almost all points x in (Definition 3.6)

3.3 Quasi Chaos

There is a problem about the application of chaos in cryptography. Chaos is defined in the uncountable infinite set, but the operation of cryptography is in the finite set. The behavior of chaos maybe be lost on the computer, even the system has a positive Lyapunov exponents. For example, in (Example 3.5), the tent map is Devaney's sense chaos, and it has a positive Lyapunov exponents $\log 2$. However, the representation of tent map converges to 0 at every points on computers. Because the computer alphabet is finite precision and binary. When we operate the tent map on computers, the tent map will be carried reluctantly at every iteration. Finally, it will converge to 0. Obviously, there is a difference between theory and reality on operation of chaos in hardware. For solving this problem, scientists propose several methods to maintain the chaotic behavior. Directly, we can add precisions, but the operation will be complicated and the cost will be raised. In [37], author suggested that digital chaotic system implented with more digits can solve the problem of short output cycle length. Another, let the dynamical system be perturbed. For example, the spatiotemporal chaotic system [17, 18, 19, 23], authors add a independent perturbed sequence to perturb the chaotic system, it can avoid that the system be short cycle length. In [6], authors add the dimension of the chaotic system, they coupled several maps to construct multi-dimensional system to increase the complexity of the chaotic dynamics and add the output cycle length. In our work, we add the precisions and couple two logistic maps to add the dimension to maintain the chaotic behavior.

Example 3.14. *(Logistic map) Let $f = \gamma x(1-x)$ be a logistic. In* figure (3)*, we observe that period three occurs where γ between 3.8 and 3.9. By Li and Yorke theorem, it implies that chaos will happen over there, but there are only a simply periodic orbit. The chaotic behavior disappear over γ between 3.8 and 3.9. When we operate the chaotic dynamical system on computer, all numbers are finite. However, the chaos is defined on infinite set. Every system is not chaos, when we operate it on computer. But the display is still complex on computer. So we call it quasi chaos.*

3.4 Synchronization

Synchronization is timekeeping which requires the coordination of events to operate a system in unison. For example, the plants flower, the light of fireflies, and migratory birds' flying array etc. This phenomenon was discovered by Christiaan Huygens in the seventeenth century. He observed that a coupled of pendulum clocks hanging from a common support had same period.

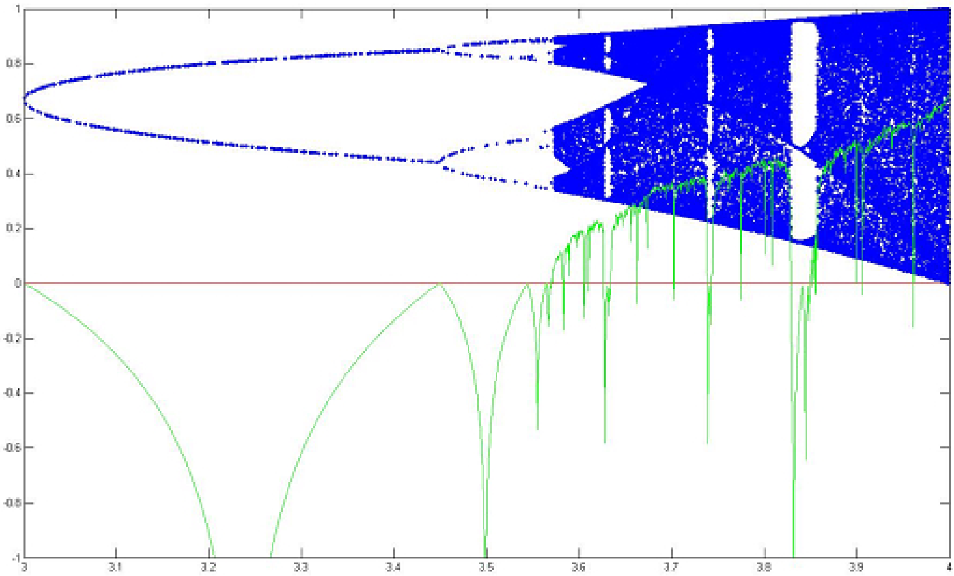

Figure 3: Logistic Map:Birfurcation diagram of a logistic map, and Lyapunov exponents of a logistic map from 3 to 4. The horizontal axis represents the parameters of logistic map. The vertical axis represents the values of logistic map and the values of Lyapunov exponents.

And he purposely destroy period of one of them, but they synchronized in few minutes. In dynamical systems, we give a definition as follows:

Definition 3.15. *(Synchronization) Let* $F(x) = (f_1, f_2) : X \times X \to X \times X$ *be a 2-dimensional dynamical system. We call* F *is synchronization, if for any* $\epsilon > 0$*, there exist* $N_0 \in \mathbb{N}$ *such that* $|f_1^n(x) - f_2^n(x)| < \epsilon$*, for* $n > N_0$*.*

However, there does not exist synchronization in any system. it must have a bridge in the system, if the system is synchronization. In a word, synchronization is a relation between a function and other function(or a system and other system), and they are connected by some operations or some methods. After several iterations, they have same behavior. We use the behavior to connect with encryption and decryption, and add the complication of the system to raise the security by algorithm construction. In our work, we use construct the crypto-system by asymptotical synchronization. Asymptotical synchronization is like synchronization, but they are still a little different. The system $\mathcal{F}$ is asymptotical synchronization with system $\mathcal{G}$. After serval iterations, then $0 \leq \|\mathcal{F}(x) - \mathcal{G}(x)\| < k$ for some small k. It is weaker than synchronization. But it will be helpful to reduce cost of computation.

3.5 Asymptotical Synchronization

In this subsection, we will present that how to operate asymptotical synchronization[3]. The

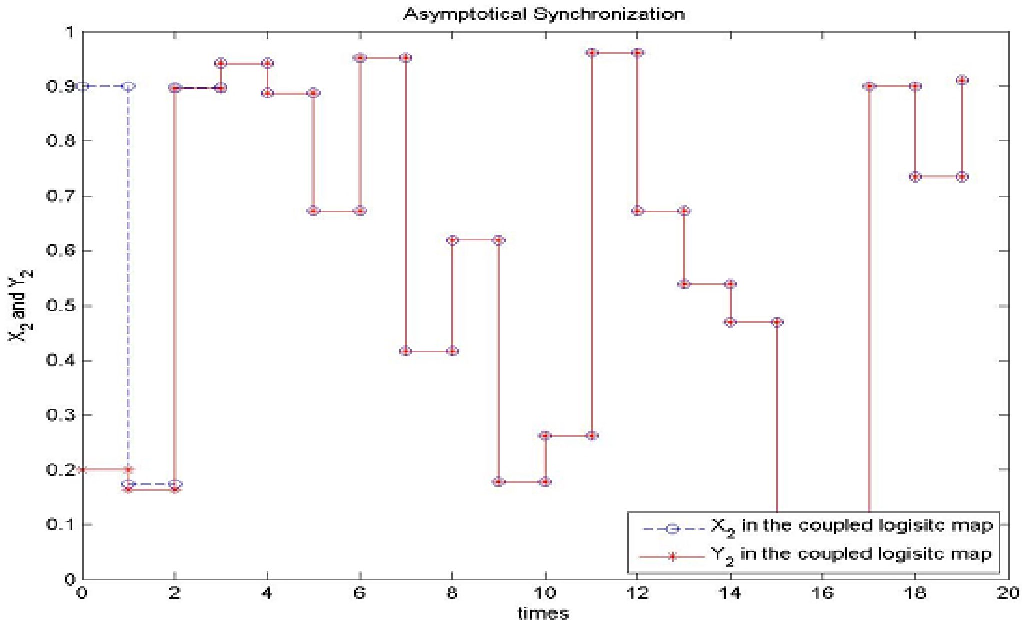

Figure 4: Simulation of the asymptotical synchronization. In numerical simulation, we obtain the average of the asymptotical synchronization. It is 4.7 in 5000 simulations.

coupled logistic map, defined by

$$\mathcal{F}(\mathbf{r},\mathbf{x},C) = C \begin{bmatrix} f_{\gamma_1}(x_1^{(i)}) \\ f_{\gamma_2}(x_2^{(i)}) \end{bmatrix}, C = \begin{bmatrix} 1-c_1 & c_1 \\ c_2 & 1-c_2 \end{bmatrix},$$

where $\mathbf{x} = [x_1, x_2]^\top, \mathbf{r} = [\gamma_1, \gamma_2]^\top$ and C is a coupling matrix with coupling strengths $c_1, c_2 \in [0,1]$.

Let $\mathcal{G}$ be another coupled logistic map defined by

$$\mathcal{G}(\mathbf{r},\mathbf{y},C) = C \begin{bmatrix} f_{\gamma_1}(y_1^{(i)}) \\ f_{\gamma_2}(y_2^{(i)}) \end{bmatrix},$$

where $\mathbf{y} = [y_1, y_2]^\top$ and the parameters $\mathbf{r}$ and C are the same as in $\mathcal{F}$. Now we want to build up a system of communication between $\mathcal{F}$ and $\mathcal{G}$, called the Transmitter and Receiver, respectively. We utilize simplex partial coupling to reach synchronization between the Transmitter and Receiver. More precisely, for given initial datum $x_1^{(0)}, x_2^{(0)}, y_1^{(0)}, y_2^{(0)} \in (0,1)$, we define the communication system and :

$$\mathbf{x}^{(i)} = \mathcal{F}(\mathbf{r}, \mathbf{x}^{(i-1)}, C), \tag{8}$$

$$\begin{cases} \bar{\mathbf{y}}^{(i)} & = \mathcal{G}(r, y^{i-1}, C), \\ \mathbf{y}^{(i)} & = [x_1^{(i)}, \bar{y_2}^i]^\top, \end{cases} \tag{9}$$

where $\mathbf{x}^{(i)} = [x_1^{(i)}, x_2^{(i)}]^\top$ and $\bar{\mathbf{y}}^{(i)}$ for $i = 1, 2, \ldots$. The vector $\mathbf{x}^{(i)}$ and $\mathbf{y}^{(i)}$ of the Transmitter and Receiver can be synchronized by the partial portion $x_1^{(i)}$ with a suitable coupling strength C, as i is sufficiently large. Under the usual metric on $\mathbb{R}/\mathbb{Z}$,we obtain a sufficient condition for synchronization below.

Let $|\cdot|_1$ be the usual metric on $\mathbb{R}/\mathbb{Z}$ defined by

$$|x - y|_1 = min\{|x - y|, 1 - |x - y|\} \ for \ x, y \in [0, 1).$$

For convenience, we define a function $\delta(\gamma)$,

$$\delta(\gamma) = max_{x \in [0,1]} |f'_\gamma(x)|$$

Theorem 3.16. [3] *If* $1 - \frac{1}{\delta(\gamma_2)} < c_2 < 1$, *then* $|x_2^{(i)} - y_2^{(i)}|_1 \to 0$ *as* $i \to \infty$.

4 Chaotic transmission model

4.1 Coupled logistic map

A coupled logistic map is defined by

$$f_{\gamma_j}(x_1) = \gamma_j x_1 (1 - x_1),$$

$$C = \begin{bmatrix} 1 - c_1 & c_1 \\ c_2 & 1 - c_2 \end{bmatrix},$$

$$(x_1^{(i+1)}, x_2^{(i+1)}) = \mathcal{F}(c_1, c_2, \gamma_1, \gamma_2, x_1, x_2) = C \begin{bmatrix} f_{\gamma_1}(x_1^{(i)}) \\ f_{\gamma_2}(x_2^{(i)}) \end{bmatrix}.$$

where $c_j \in (0, 1], j = 1, 2$. $\gamma_j \in [3.573, 4], j = 1, 2$. $x_j \in (0, 1), j = 1, 2$ It is constructed by coupling two logistic maps. In figure 3,the bifurcation diagram and Lyapunov exponent of a logistic map. The chaotic behavior happen from $\gamma > 3.573$. We use the coupled logistic map to build the crypto-system.

4.2 Crypto-System

A wireless communication scheme is sketched in Figure 6. Information is transmitted by a transmitter through a wireless channel after encryption. A receiver recovers the information

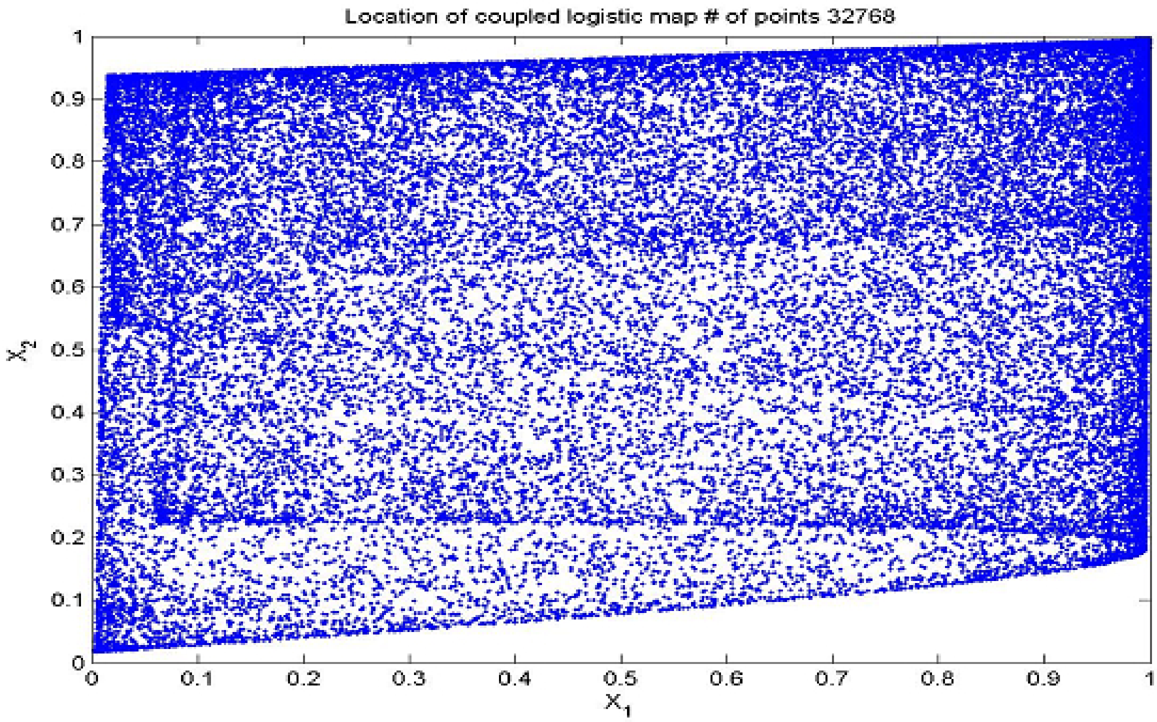

Figure 5: Coupled Logistic Map. It is the image of the digital coupled logistic map.

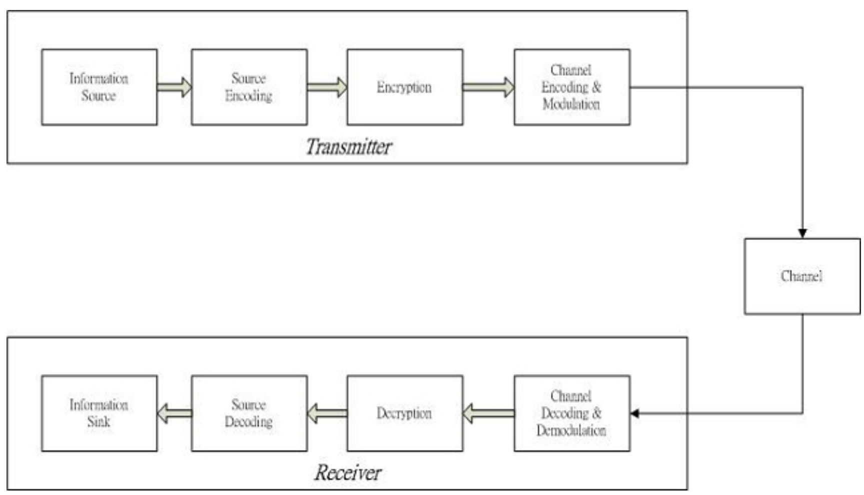

Figure 6: Wireless Communication Scheme. The channel is wireless in the scheme. The coupled logistic maps are in the Encryption and Decryption, respectively.

by decryption. In this section, we will present a crypto-system, which consists of the transmitter and the receiver by two coupled logistic maps, respectively. A coupled logistic map $\mathcal{F}$ is defined by

$$x^{(i)} = \mathcal{F}(\mathbf{r}, x^{(i-1)}, C) := C\mathbf{L}(\mathbf{r}, x^{(i-1)}), \tag{10}$$

$i = 1, 2, \dots$, where $x^{(i)} = [x_1^{(i)}, x_2^{(i)}]^T$, $\mathbf{r} = [\gamma_1, \gamma_2]^T$, $\mathbf{L}(\mathbf{r}, x^{(i-1)}) = [L_1(\gamma_1, x_1^{(i-1)}), L_2(\gamma_2, x_2^{(i-1)})]^T$, in which L_j, $j = 1, 2$, are logistic maps in (10) , and

$$C = \begin{bmatrix} 1 - c_1 & c_1 \\ c_2 & 1 - c_2 \end{bmatrix}$$

is a coupling matrix with coupling coefficients $0 < c_j \leq 1$, $j = 1, 2$.
A masking sequence $z^{(i)}$ is defined by

$$z^{(i)} = x_1^{(i)}, i = 1, 2, \dots. \tag{11}$$

At the same time, we need to construct an unmasking sequence. Therefore, let $\mathcal{G}$ be a coupled logistic map defined by

$$y^{(i)} = \mathcal{G}(\mathbf{r}, y^{(i-1)}, C) := C\mathbf{L}(\mathbf{r}, y^{(i-1)}), i = 1, 2, \dots, \tag{12}$$

where $y^{(i)} = [y_1^{(i)}, y_2^{(i)}]^T$. Here, C and $\mathbf{r}$ are the same as $\mathcal{F}$ in (10). Then the unmasking sequence $\tilde{z}^{(i)}$ is defined by

$$\tilde{z}^{(i)} = y_1^{(i)}, i = 1, 2, \dots. \tag{13}$$

In Figure 7, we present a crypto-system from Encryption layer and Decryption layer in the wireless communication scheme by chaotic coupled logistic maps (defined in (10) and (12)), respectively. There are two stages in the crypto-system. First, the transmitter takes simplex direction to the receiver until Encryption layer and Decryption layer reach asymptotical synchronization. Second, the transmitter begins to encrypt a plaintext to a ciphertext, and preserves asymptotically synchronous between $\mathcal{F}$ in Encryption layer and $\mathcal{G}$ in Decryption layer. Therefore in the first stage, we randomly create initial values $x_j^{(0)}$ and $y_j^{(0)}$, $j = 1, 2$, in $\mathcal{F}$ and $\mathcal{G}$, respectively. The transmitter transmits partial $x_1^{(i)}$ to the receiver, and the receiver receives it to update $y_1^{(i)}$. After α iterations ($i = 1, 2, \dots, \alpha$), $\mathcal{F}$ and $\mathcal{G}$ will reach asymptotical synchronization. This stage is called pre-iteration. In the second stage, the transmitter begins to transmit signals, at the same time we have to preserve asymptotically synchronous between

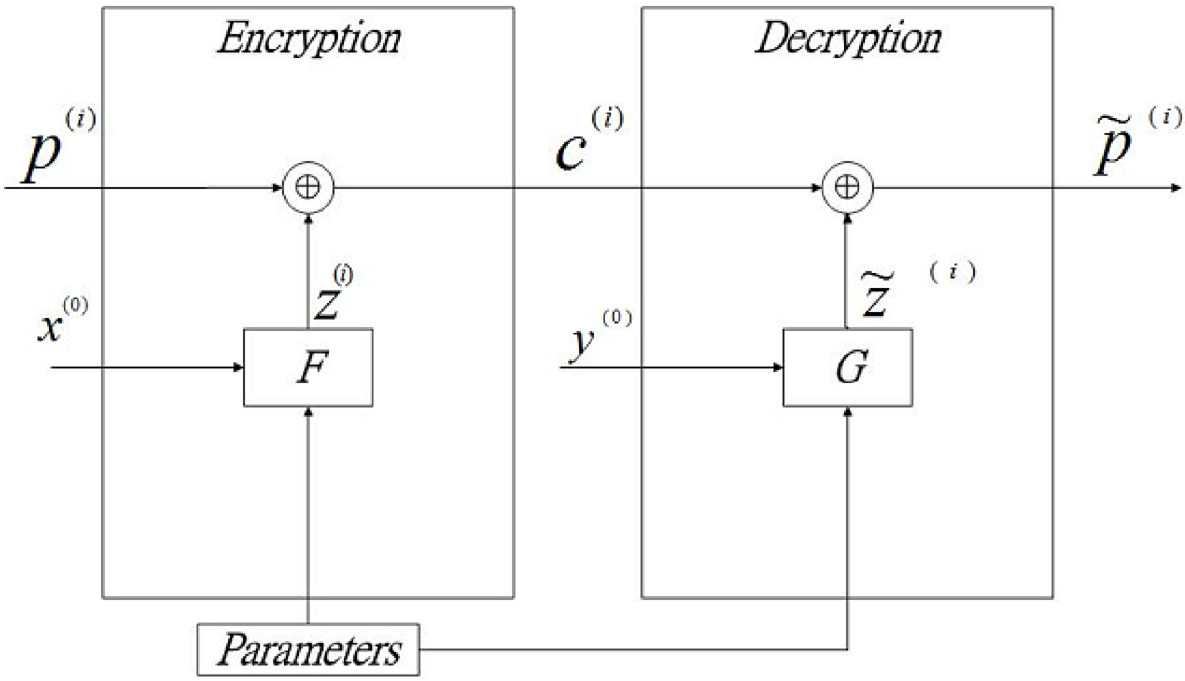

Figure 7: Crypto-system. The part of the Figure 6. p is plaintext, $\widetilde{p}$ is the decipher, c is ciphertext, $z, \widetilde{z}$ are the masking sequence and the unmasking sequence, respectively. x, y are the values of $\mathcal{F}$ and $\mathcal{G}$,respectively.

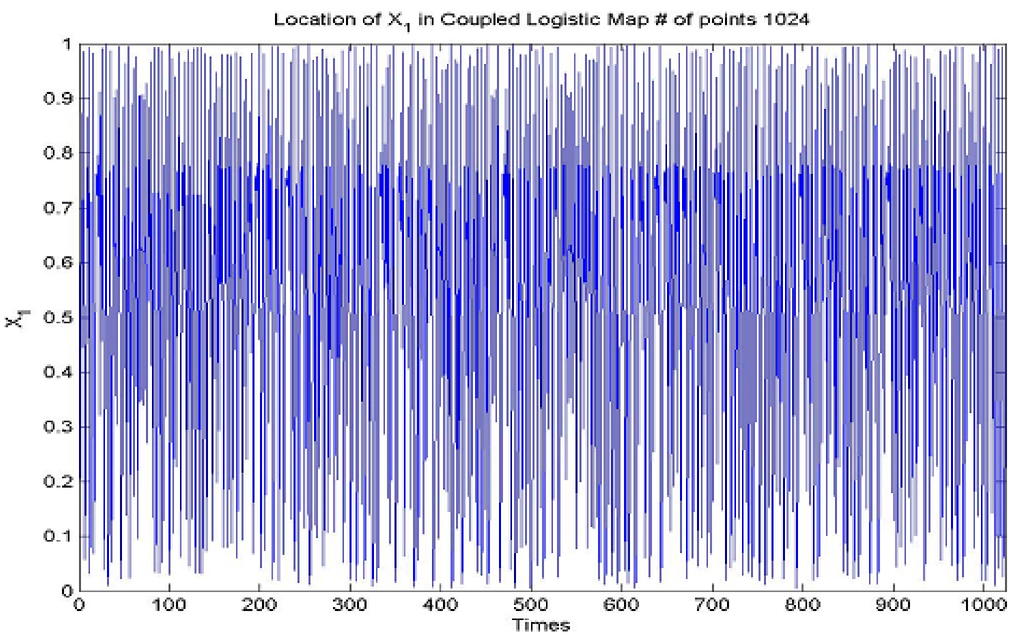

Figure 8: Trajectory. It is the trajectory of x_1 in the coupled logistic map. And it is the masking sequence of the crypto-system.

$\mathcal{F}$ and $\mathcal{G}$. Thus, in Encryption layer to encrypt information sources by the masking sequence $z^{(i)}$ (11). In Decryption layer, to decrypt the ciphertext by the unmasking sequence $\tilde{z}^{(i)}$ (13). In order to decode the ciphertext correctly, the unmasking sequence $\tilde{z}^{(i)}$ must be identical to the masking sequence $z^{(i)}$. For preserving asymptotical synchronization between $\mathcal{F}$ and $\mathcal{G}$, the receiver needs to keep updating $y_1^{(i)}$ by the partial $x_1^{(i)}$. However, in a wireless channel, noise accumulates in signals. In order to prevent that from happening, we need to reset the initial values of $\mathcal{F}$ and $\mathcal{G}$ per β transmissions by the pre-iteration. It is called resynchronization in this strategy.

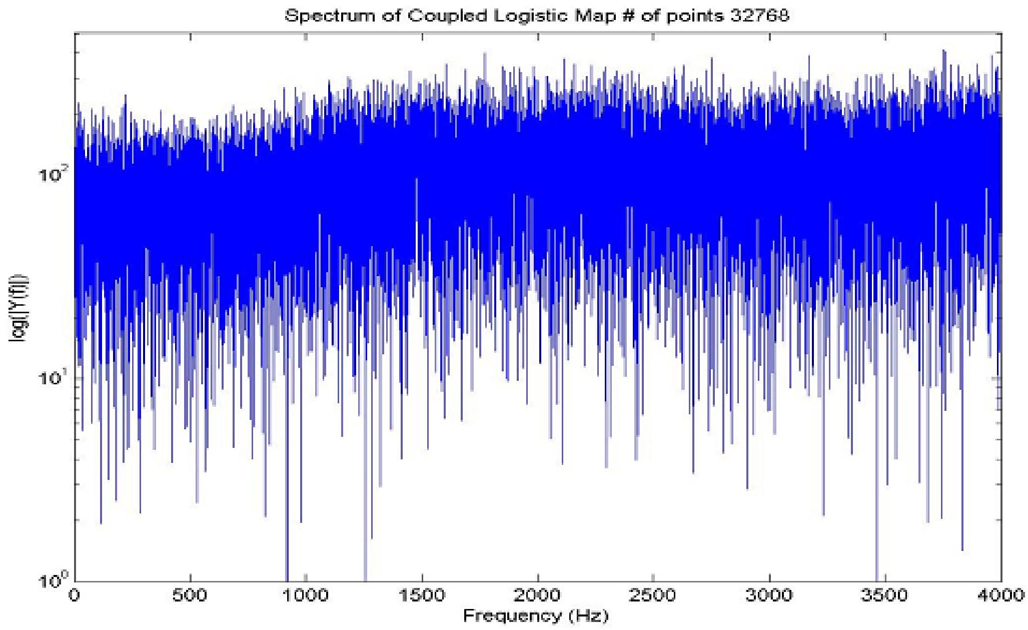

Figure 9: FFT of the Coupled Logistic Map. We compute the fast Fourier transform of the x_1 in the coupled logistic map. The horizontal axis represents the Frequency. The vertical axis represents the values of the FFT.

Theorem 4.1. *[3] Using suitable previous tactics with* $1 - \frac{1}{\delta(\gamma_2)} < c_2 < 1$, *there exists* $i_{syn} \in \mathbb{N}$ *such that*

$$|y_2^{(i)} - x_2^{(i)}| < \left[1 + \frac{c_2\delta(\gamma_1)}{1-(1-c_2)\delta(\gamma_2)}\right] 10^{-n},$$

as $i > i_{syn}$.

Theorem 4.2. *[3] For* $j \geq 1$ *and* $i = i_{syn} + j$, *then*

$$|y_1^{(i)} - x_1^{(i)}| < \left[(1-c_1)\delta(\gamma_1) + c_1\delta(\gamma_2) + \frac{c_1c_2\delta(\gamma_1)\delta(\gamma_2)}{1-(1-c_2)\delta(\gamma_2)}\right] 10^{-n}$$

Following previous theorems(Theorem 4.1, 4.2), the connection which is constructed by asymptotical synchronization can be realized. And we also simulate the asymptotical synchronization numerically. It works, and the average of iterations is 4.7 in 5000 times simulation.

5 Simulation Setups

In the crypto-system, all numbers are represented in finite digits. Assume that $x_1^{(i)}$ and $x_2^{(i)}$ ($y_1^{(i)}$ and $y_2^{(i)}$) in the vector $x^{(i)}$ ($y^{(i)}$) are represented in m digits, the transmitted signal $t_x^{(i)}$ and the received signal $r_y^{(i)}$ are represented in n digits, and length of each plaintext $p^{(i)}$ is represented in l digits, where $m > n > l$. The parameters γ_j and the coupling coefficients c_j, $j = 1, 2$, are represented in r digits and k digits, respectively.
Then the encryption process follows: $i = \alpha + 1, \alpha + 2, \ldots,$

$$\begin{aligned}
z^{(i)} &= x_1^{(i)}(1:n),\\
t_x^{(i)}(1:l) &= z^{(i)}(1:l) \bigoplus p^{(i)},\\
t_x^{(i)}(l+1:n) &= z^{(i)}(l+1:n),
\end{aligned}$$

where $\bigoplus$ is an XOR operation (Exclusive or) and $x_1^{(i)}(1:n)$ denotes dropping the first n digits from $x_1^{(i)}$. At the same time, in Decryption layer a decipher $\tilde{p}$ needs to be defined. Then the decryption process follows: $i = \alpha + 1, \alpha + 2, \ldots$

$$\begin{aligned}
\tilde{z}^{(i)} &= y_1^{(i)}(1:n),\\
\tilde{p}^{(i)} &= \tilde{z}^{(i)}(1:l) \bigoplus r_y^{(i)}(1:l),
\end{aligned}$$

where $\tilde{p}^{(i)}$ is the decipher. Since it will keep asymptotical synchronization between $\mathcal{F}$ in the transmitter and $\mathcal{G}$ in the receiver, and $n > l$, the decipher $\tilde{p}^{(i)}$ can be identical to plaintext $p^{(i)}$.

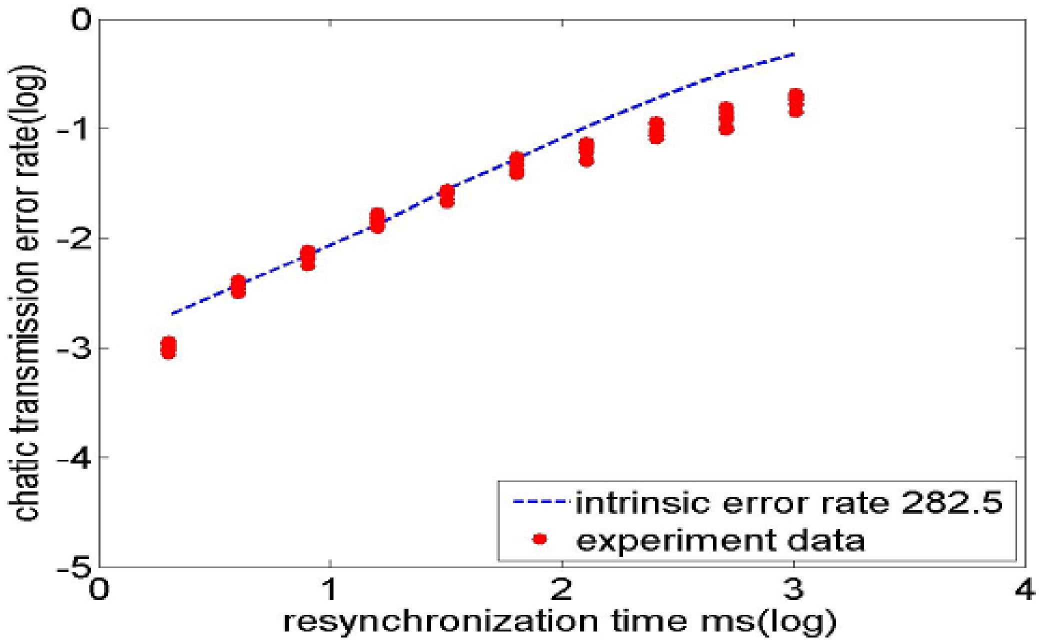

Figure 10: Simulation. The horizontal axis represents the resynchronization timeunder the intrinsic error rate 282.5ppm. The vertical axis represents the chaotic error rate under the intrinsic error rate 282.5ppm. The experiment is represented by •. The numerical simulation is represented by $--$.

6 Hypothesis Test

In our work, we apply the hypothesis test to find the relation between the numerical simulation and the experiment. The hypothesis test is a statistical method. Hypothesis Test is applied to find the relation between data and data or data and a standard. There are two kinds of hypothesis test, one sample and two sample. The hypothesis test is builded on the conditional probability and Central Limit Theorem. In different situation, we will propose different way to solve our problem. That is conditional probability sense. Central Limit Theorem can arrange the random variable to the standard normal distribution. It is helpful to compute the probability about the hypothesis test. Based on those theory, there are five steps about the hypothesis test. It follows that

1. Set the null hypothesis and the alternative hypothesis. ex. $H_0 : p = \frac{1}{6}, H_1 : p < \frac{1}{6}$.

2. Set the significance level of α.

3. Compute the statistics about the sample and compare the statistics with the standard.

4. Compute the probability of type I error and type II error.

5. Determine to reject or accept the null hypothesis.

However, hypothesis test only provides the selection, it can not guarantee the determination absolutely. When we decide to reject the alternative hypothesis, we maybe mistake. There are four situations in the blow table.

Acc╲Real	H_0	H_1
H_0	Right	TypeII
H_1	TypeI	Right

The type I error is that rejecting H_0 and accepting H_1 when H_0 is true. The type II error is that Failing to reject H_0 when H_1 is true, that is H_0 is false. The probability which the type I error happened is p-value. The p-value associated with a test is the probability, under the null hypothesis H_0, that the test statistic is equal to or exceeds observed value of the test statistic in the direction of the alternative hypothesis.

Example 6.1. *(Dice) We will check that dice is fair or not. Let p equal the probability of rolling a 6 with one of these dice. To test $H_0 : p = \frac{1}{6}$ against the alternative $H_1 : p > \frac{1}{6}$, several of these dice will be rolled to yield a total of $n = 8000$ observation. Let Y equal the number of times that six resulted in the 8000 trials. The test statistic is*

$$Z = \frac{Y/n - 1/6}{\sqrt{(1/6)(5/6)/n}} = \frac{Y/8000 - 1/6}{\sqrt{(1/6)(5/6)/8000}}.$$

If we use a significance level of $\alpha = 0.05$, the critical region is

$$z \geq z_{0.005} = 1.645.$$

The results of the experiment yielded $y = 1389$, so that the calculated value of the test statistic is

$$z = \frac{1389/8000 - 1/6}{\sqrt{(1/6)(5/6)/8000}} = 1.670.$$

Since

$$z = 1.670 > 1.645,$$

the null hypothesis is rejected.

6.1 Wilcoxon Test

In our work, we use Wilcoxon test. Wilcoxon test is a kind of the hypothesis tests. In our case, we don't know the population of the data(the experiment and numerical simulation), and do not know the statistic of the population. We do not suppose distribution of the data. So we use the non-parametric(distribution-free) statistic method to analyse our data. Wilcoxon test is suitable in our case. Wilcoxon test does not need to know the population of the data, it only operates the data to determine that the relation between the experiment and numerical simulation exists or does not.

There are four steps for testing a hypothesis by Wilcoxon test[11, 13]:

- State the null hypothesis $H_0 : m_X = m_Y$, and the alternative hypothesis $H_1 : m_X \neq m_Y$.
- Determine the significance level α.
- Compute the testing statistic.
- Reject or do not the null hypothesis.

Proposition 6.2. *(two-sample) There two identical independent distribution samples, $X_1, X_2, \ldots, X_{n_1}$ and $Y_1, Y_2, \ldots, Y_{n_2}$. Assign to the ordered values the ranks $1, 2, \ldots, n_1 + n_2$. In the case of ties, assign the average of the ranks assiociated with the tied values . Let W equal the sum of the ranks $Y_1, Y_2, \ldots, Y_{n_2}$. Let m_X and m_Y are the respective medians, the critical region for testing $H_0 : m_X = m_Y$ against $H_1 : m_X < m_Y (m_X > m_Y)$ would be of the form $w \geq c (w \leq c)$. The mean and variance of W are*

$$\mu_w = \frac{n_1(n_1 + n_2 + 1)}{2}$$

and

$$Var(W) = \frac{n_1 n_2 (n_1 + n_2 + 1)}{12}$$

and the statistic

$$Z = \frac{W - n_1(n_1 + n_2 + 1)/2}{\sqrt{n_1 n_2 (n_1 + n_2 + 1)/12}}$$

is approximately $N(0, 1)$.

Alternative	Rejection Region
$m_X - m_Y < 0$	$W_N \geq w_\alpha$
$m_X - m_Y > 0$	$W_N \leq w'_\alpha$
$m_X - m_Y \neq 0$	$W_N \leq w'_{\alpha/2}$ or $W_N \geq w_{\alpha/2}$

where w_α is right tail, w'_α is left tail.

Example 6.3. *X is results of the experiment of the crypto-system. Y is results of the numerical simulation of the crypto-system. In the wireless channel, the noise increase along with the distance. However, in the numerical simulation, it does not have the factor about distance. We have to produce the noise to simulate effect of the distance. So in the numerical, there are two factors, resynchronization, change rate. In the experiment, there are also two factors, resynchronization, distance. The data are*

$$X : 55.95\ 69.79\ 69.00\ 69.79\ 55.04\ 56.41\ 64.70\ 72.20\ 60.75\ 82.70.$$

$$Y : 81.25\ 40.13\ 54.81\ 89.49\ 65.80\ 55.61\ 62.33\ 33.41\ 69.23\ 31.08.$$

The critical region for testing $H_0 : m_X = m_Y$ against $H_1 : m_X \neq m_Y$ at $\alpha = 0.05$. Let$n_1+n_2 = N$ The pooled array with X values underlined is $31.08, 33.41, 40.13, 54.81, \underline{55.04}, 55.61, \underline{55.95}, \underline{56.41}, \underline{60.75}, 62.33, \underline{64.70}, 65.80, \underline{69}, 69.23, \underline{69.79}, \underline{69.79}, \underline{72.20}, 81.25, \underline{82.70}, 89.49$, *and* $W_N = 5+7+8+9+11+13+14+15+16+19 = 117$. *The right tail:*

$$w_{\alpha/2} = n_1(N+1)/2 + 0.5 + z_{\alpha/2}\sqrt{n_1 n_2 (N+1)/12} = 131.4284.$$

The left tail:

$$w'_{\alpha/2} = n_1(N+1)/2 - 0.5 - z_{\alpha/2}\sqrt{n_1 n_2 (N+1)/12} = 78.5716$$

and

$$w'_{\alpha/2} < W_N < w_{\alpha/2}.$$

So, we accept the H_0.

Table 1: We theorize about the error of the distance by hypothesis test in the experiments. Where SQ is from least square method.

resyn\dist	0.4	2	5	7	7.5	7.7	8
2	23	23	26.5	37	86	159	226
4	39	41	43	62	199	288	419.5
8	42	43	44	56	221.5	289	430
16	40	40	42	43	173.5	303	477
32	43	43	44	45.5	210.5	282.5	429
64	34.5	34.5	36	40	159	269	405
128	27.5	28.5	31.5	31.5	74.5	198.5	300.5
256	19	20	20	21.5	96.5	142	215.5
512	11.5	11.5	11.5	11.5	58	96.5	136.5
1024	8.5	9.5	10.5	10.5	51	77.5	99
SQ	43	43	44	45.5	210.5	282.5	429

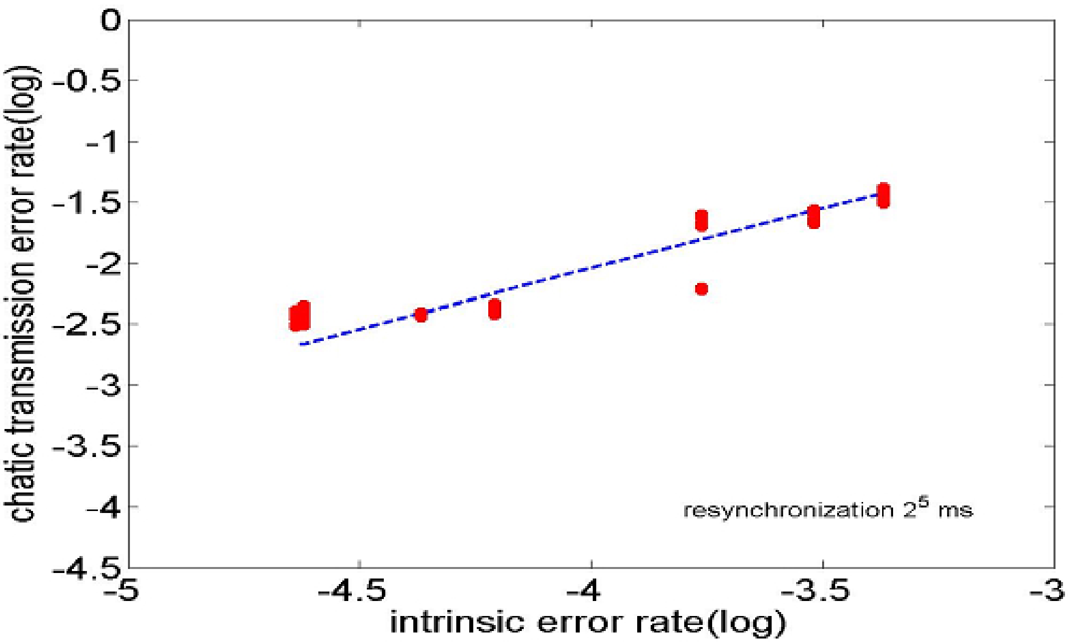

Figure 11: Simulation. The horizontal axis represents the intrinsic error rate. The error is intrinsic in the channel under each distance. The vertical axis represents that the results of the communication was effected by the intrinsic error. The experiment is represented by •. The numerical simulation is represented by $--$.

7 Results and Conclusion

7.1 Parameter Space

In a dynamical system, a chaotic behavior is determined by the parameter. When we draw a bifurcation diagram of the logistic map, we observe the chaotic behavior for $\gamma \geq \gamma_\infty$. However, all parameters are not equally strong. Sometimes, the orbit diagram reveals an unexpected mixture of order and chaos, with periodic windows interspersed between chaotic clouds of dots[35]. Thus, we have to choose a suitable set of parameters such that the coupled logistic maps $\mathcal{F}$ and $\mathcal{G}$ are chaotic. There are many parameters in the coupled logistic map in (2) and (4), γ_1, γ_2, c_1 and c_2. Let $S = (\gamma_1, \gamma_2, c_1, c_2)$ be a parameter space of the coupled logistic map. The values of γ_1 or γ_2 are chosen from 3.573 to 4 and the values of c_1 or c_2 are chosen from 0 to 1. We check that the coupled logistic map is chaotic by Lyapunov exponents. There are 86 percent of the parameters in S which has positive Lyapunov exponents, while the remainders are periodic windows (Figure 1).

7.2 Simulation Result and Experiment

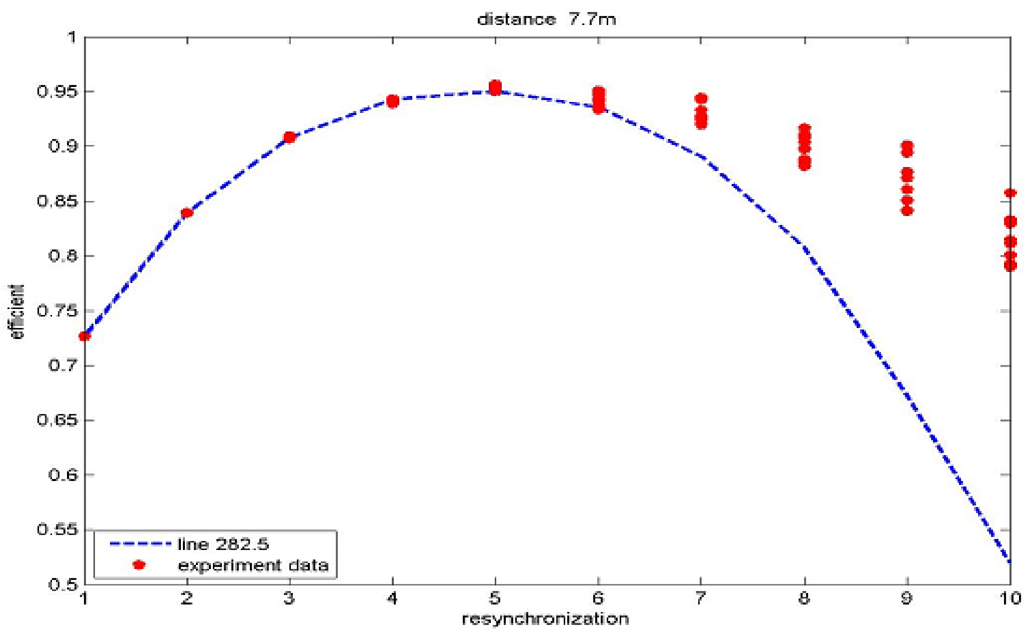

Figure 12: Simulation. The horizontal axis represents the resynchronization time. The vertical axis represents the efficient of the crypto-system. The experiment is represented by $\bullet$. The numerical simulation is represented by $--$.

In this thesis, all results of experiments are offered by [16]. In the numerical simulations, we set digital variable: $m = 24$, $r = 16$, $k = 8$, $n = 16$ and $l = 8$, and the size of a plaintext is 0.24 million bytes. We suppose that the noise is uniformly distributive in the wireless channel and there are the different intrinsic error rates with the different distances on the wireless channel. In order to maintain the asymptotical synchronization between the transmitter and the receiver, we need to operate resynchronization per β ms. In the Professor James Juane's experiments, 16 bytes plaintexts can be transmitted per 1 ms. In Figure 11, it shows the relation between the intrinsic error rate and the chaotic transmission error rate. Those dots denote results of the experiment with 7 different distance. The dashed line comes from numerical simulations with different intrinsic error rates and it tests 100 times per intrinsic error rate. In this figure, we set 2^5ms resynchronization. In Figure 10, it shows the relation between the resynchronization and the chaotic transmission error rate. Those dots denote results of the experiment data and the dashed line comes from numerical simulations. The result reveals that the chaotic transmission error rate will increase with the distance (intrinsic error rate). Next, we will propose an efficiency function of the crypto-system to find out the optimal resynchronization for the crypto-system in Wireless Secure Communication. The efficiency function $E(\kappa)$ is defined as follow:

$$E(\kappa) = \frac{\kappa}{\beta\eta + T},$$

where κ is the number of the ciphertext which we expect to decrypt successfully,

$$T = \frac{\kappa}{1 - \epsilon},$$

T is the cost, when the chaotic transmission error rate is ϵ and we expect to decrypt κ ciphertexts successfully. And η is the times of the resynchronization which is equal to T over β. Here β is resynchronization. In Figure (12), it shows the length of per resynchronization vs. the efficiency as the intrinsic error rate is 282.5 ppm (that is the distance between the transmitter and the receiver with 7.7 m). Those dots denote experiment data and the dashed line comes from numerical simulations. The result reveals that the optimal efficiency occurs on the resynchronization with 32 ms.

Appendix

There are two stages in the algorithm. First, the transmitter takes one-way connection to the receiver until Encryption layer and Decryption layer are synchronized. Second, the transmitter begins transmitting plaintexts to the receiver, and keeps the one-way connection for preserving with the synchronization between Encryption layer and Decryption layer.

Setup

Parameters: c_i , $\gamma_i, i = 1, 2.$
Initial values:$x_i^{(0)}$ and $y_i^{(0)}$ are represented in x digits, $i = 1, 2.$
Carrier (transmitted signal): t_x is represented in car digits.
Discharger (received signal): r_y is represented in car digits.
Plaintext signal: sgn is represented in n digits.
Decipher: decipher is represented in n digits.
Pre-iterations: β times.

First step

The transmitter connects the receiver in only one direction, and to take several pre-iterations until Encryption layer and Decryption layer are synchronized asymptotically. We create initial values $x_i^{(0)}$ and $y_i^{(0)}$ randomly in Encryption layer and Decryption, $i = 1, 2.$
In the transmitter: $j = 1, 2, \ldots \beta,$
Generating a hyper-chaotic string, and choosing a carrier,
$x_1^{(j)}(1 : x)$, $t_x^{(j)}(1 : car)$.
The system $\mathcal{F}$:

$$\begin{aligned}
\bar{x}_1 &= \gamma_1 x_1^{(j-1)}(1 - x_1^{(j-1)}),\\
\bar{x}_2 &= \gamma_2 x_2^{(j-1)}(1 - x_2^{(j-1)}),\\
x_1^{(j)} &= \bar{x}_1 + c_1(\bar{x}_2 - \bar{x}_1),\\
x_2^{(j)} &= \bar{x}_2 + c_2(\bar{x}_1 - \bar{x}_2),
\end{aligned}$$

$t_x^{(j)}(1 : car) = x_1^{(j)}(1 : car)$.
Send t_x
In the receiver: $j = 1, 2, \ldots \beta,$
Generating a hyper-chaotic string, producing a discharger,
$y_1^{(j)}(1 : x)$

The system $\mathcal{G}$:

$$\begin{aligned}\bar{y}_1 &= \gamma_1 y_1^{(j-1)}(1-y_1^{(j-1)}),\\ \bar{y}_2 &= \gamma_2 y_2^{(j-1)}(1-y_2^{(j-1)}),\\ y_1^{(j)} &= \bar{y}_1 + c_1(\bar{y}_2 - \bar{y}_1),\\ y_2^{(j)} &= \bar{y}_2 + c_2(\bar{y}_1 - \bar{y}_2),\end{aligned}$$

Receive $r_y^{(j)}(1:car)$ and update the y_1 by $r_y^{(j)}$.
$y_1^{(j)}(1:ca) = r_y^{(j)}(1:car)$.
And repeat the step β times until F and G are synchronized asymptotically.

Second Step

The transmitter begins transmitting signals, and we have to keep the connection between the transmitter and the receiver for preserving synchronization between Encryption layer and Decryption layer. Reset the initial values $x_i^{(0)}$ and $y_i^{(0)}$ in $\mathcal{F}$ and $\mathcal{G}$ by first step $x_i^{(\beta)}$ and $y_i^{(\beta)}$ which is after Encryption layer and Decryption layer synchronization.
In the transmitter: $k = 1, 2, \ldots,$
1. Generating masking sequence $z^{(k)}(1:car)$ and the carrier $t_x^{(k)}(1:car)$ by the system $\mathcal{F}$

$$\begin{aligned}\bar{x}_1 &= \gamma_1 x_1^{(k-1)}(1-x_1^{(k-1)}),\\ \bar{x}_2 &= \gamma_2 x_2^{(k-1)}(1-x_2^{(k-1)}),\\ x_1^{(k)} &= \bar{x}_1 + c_1(\bar{x}_2 - \bar{x}_1),\\ x_2^{(k)} &= \bar{x}_2 + c_2(\bar{x}_1 - \bar{x}_2),\\ z^{(k)}(1:car) &= x_1^{(k)}(1:car),\end{aligned}$$

2. Load signals $sgn(1:n)$.
3. Combine the signals and the masking sequence $z^{(k)}, t_x^{(k)}(1:n) = z^{(k)}(1:n) \bigoplus sgn(1:n)$,
4. Edit the carrier $t_x^{(i)}, t_x^{(k)}(n+1:car) = z^{(k)}(n+1:car)$.
5. Send $t_x^{(i)}$ to the receiver.

In the receiver: $k = 1, 2, \ldots,$

1. Generating unmaking sequence $\tilde{z}^{(k)}(1:car)$ by the system $\mathcal{G}$.

$$\begin{aligned}
\bar{y}_1 &= \gamma_1 y_1^{(k-1)}(1-y_1^{(k-1)}),\\
\bar{y}_2 &= \gamma_2 y_2^{(k-1)}(1-y_2^{(k-1)}),\\
y_1^{(j)} &= \bar{y}_1 + c_1(\bar{y}_2-\bar{y}_1),\\
y_2^{(j)} &= \bar{y}_2 + c_2(\bar{y}_1-\bar{y}_2),\\
z^{(k)}(1:car) &= y_1^{(k)}(1:car).
\end{aligned}$$

2. Receive $\widetilde{r}_y^{(k)}$

3. Decode the cipher by the unmasking sequence $\tilde{z}^{(k)}(1:car)$, get $decipher(1:n)$,
$decipher(1:n) = \widetilde{r}_y^{(k)}(1:n) \bigoplus \tilde{z}^{(k)}(1:n)$,

4. Update the initial value $y_1^{(k)}(1:car)$ in $\mathbf{G}$ by $\widetilde{r}_y^{(k)}$,
$y_1^{(k)}(1:n) = r_y^{(k)}(1:n) \bigoplus decipher(1:n)$.
$y_1^{(k)}(n+1:car) = r_y^{(}(k))(n+1:car)$.

5. Save the decipher.

References

[1] V. Afraimovich and S. B. Hsu. *Lectures on Chaotic Dynamical Systems.* American Mathematical Society, 1 edition, 2002.

[2] G. Alvarez and S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurcation and Chaos*, 16:2129–2151, 2006.

[3] S. M. Chang, M. C. Li, and W. W. Lin. Asymptotic synchronization of modified logistic hyper-chaotic system. *Nonlinear Analysis*, 10:869–880, 2009.

[4] C. H. Chiu, W. W. Lin, and C. C. Peng. Asymptotic sychronization in lattices of coupled three-dimension nonlinear chaotic equations. *J. Mathematical Analysis and Applications*, 250:222–244, 2000.

[5] C. H. Chiu, W. W. Lin, and C. S. Wang. Synchronization in a lattice of coupled van der pol systems. *Int. J. Bifurcation and Chaos*, 8:2353–2373, 1998.

[6] C. H. Chiu, W. W. Lin, and C. S. Wang. Synchronization in lattices of coupled oscillators with various boundary conditions. *Nonlin. Anal. Theory, Methods Appl.*, 46:213–239, 2001.

[7] K. M. Cuomo and A. V. Openheim. Circuit implementation of synchronized chaos with applications to communications. *Physical Review Letters*, 71:65–68, 1993.

[8] R. Devaney. *Chaotic Dynamical systems.* Addison-Wesley, 1 edition, 1989.

[9] U. Feldmann, M. Hasler, and W. Schwarz. Communication by choatic signals: the inverse system approach. *IEEE*, 40:680–683, 1995.

[10] D. R. Frey. Chaotic digital encoding: an approach to secure communication. *IEEE*, 40(10):660–666, 1993.

[11] J. D. Gibbons. *Nonparametric Statistical Inference.* Dekker, 3 edition, 1992.

[12] J. Guckenheimer and R. F. Williams. Structural stability if lorenz attractors. *Publ. Math. IHES*, 50:59, 1979.

[13] R. V. Hogg and E. A. Tains. *Probability and Statistical Inference.* Pearson Prentic Hall, 7 edition, 2006.

[14] S. Hu, Y. Zou, J. Hu, and L. Bao. A synchronous cdma system using discrete coupled-chaotic sequence. *Southeastcon '96. 'Bringing Together Education, Science and Technology'., Proceedings of the IEEE*, pages 484–487, 1996.

[15] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz. Experimental demonstration of secure communications via chaotic synchronization. *Int. J. Bifurcation and Chaos*, 2:709–713, 1992.

[16] X. Q. Kuo. *Voice encryption using HEX scramble algorithm in wireless application*. Minghsin University of Science and Technology, 1 edition, 2009.

[17] P. Li, Z. Li, W. A. Halang, and G. Chen. Analysis of a multiple output pseudorandom-bit generator based on a spatiotemporal chaotic system. *Int. J. Bifurcation Chaos*, 16:2949–2963, 2006.

[18] P. Li, Z. Li, W. A. Halang, and G. Chen. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. *Physics Letters A*, 349:467–473, 2006.

[19] P. Li, Z. Li, W. A. Halang, and G. Chen. A stream cipher based on a spatiotemporal chaotic system. *Chaos, Solitons and Fractals*, 32:1867–1876, 2007.

[20] T. Y. Li and J. A. Yorke. Period three implies chaos. *Amer. Math.*, 82:985–992, 1975.

[21] W. W. Lin, C. C. Peng, and C. S. Wang. Synchronization in coupled map lattices with periodic boundary condition. *Int. J. Bifurcation Chaos*, 9:1635–1652, 1999.

[22] E. Lorenz. Deterministic nonperiodic flow. *J. Atmos. Sci.*, 20:130, 1963.

[23] H. Lu, S. Wang, X. Li, G. Tang, J. Kuang, W. Ye, and G. Hu. A new spatiotemporally chaotic cryptosystem and its security and performance analyses. *Chaos*, 14:617–629, 2004.

[24] A. Lyaunov. Problème général de la stabilité du mouvement. *Ann. Fac. Sci. Univ. Toulouse*, 9:203–475, 1907.

[25] R. Mathews. On the derivaion of a "chaotic" encryption algorithm. *Cryptologia*, 13(1):29–41, 1989.

[26] Q. Memon. Synchronized chaos for network security. *Comp. Comm.*, 26:498–505, 2003.

[27] O. Morgul and M. Feki. A chaotic masking scheme by using synchronized chaotic systems. *Physics Letters A*, 251:169–176, 1999.

[28] T. S. Parker and L. O. Chua. *Partical Numerical Algorithms for Chaotic Systems*. Springer-Verlag, 1 edition, 1989.

[29] C. Robinson. *Dynamical Systems: Stability, Symbolic Dynamics, and Chaos*. CRC, 2 edition, 1998.

[30] O. E. Rossler. An equation for hyperchaos. *Physics Letters A*, 71:155–157, 1979.

[31] S. M. Shahruz, A. K. Pradeep, and R. Gurumoorthy. Design of a novel cryptosystem based on chaotic oscillators and feedback inversion. *J. Sound and Vibration*, 250:762–771, 2002.

[32] J. C. Sprott. *Chaos and times-series analysis*. Oxford University Press, 1 edition, 2003.

[33] H. F. Stephen, J. I. Arnold, and E. S. Lawrence. *Linear Algebra*. Pearson Education, 4 edition, 2003.

[34] Douglas R. Stinson. *Cryptography*. CRC, 1 edition, 1995.

[35] S. H. Strogatz. *Nonlinear Dynamics And Chaos: With Applications To Physics, Biology, Chemistry, And Engineering (Studies in Nonlinearity)*. Springer-Verlag, 1 edition, 1994.

[36] W. Tucker. The lorenz attrocter exists. *C. R. Acad. Paris Sér. I Math.*, 328:1197, 1999.

[37] D.D. Wheeler. Problems with chaotic cryptosystem. *Cryptologia*, 13:243–250, 1989.

[38] C. W. Wu and L. O. Chua. A simple way to synchronize chaotic systems with applications to secure communications systems. *Int. J. Bifurcation and Chaos*, 3:1619–1627, 1993.