UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Security and Robustness of a Modified Parameter Modulation Communication Scheme

by

Xiyin Liang

Submitted in partial fulfilment of the requirements for the degree

Philosophae Doctor (Electronic Engineering)

in the

Faculty of Engineering, Built Environment and Information Technology

University of Pretoria

October 2008

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Security and Robustness of a Modified Parameter Modulation Communication Scheme

by

Xiyin Liang

Promotor: **Prof. Xiaohua Xia**

Co-promotor: **Dr. Jiangfeng Zhang**

Department: **Electrical, Electronic and Computer Engineering**

Degree: **PhD (Electronic Engineering)**

Summary

Chaotic synchronization has attracted much attention because of its potential application in secure communication. Different chaos-based communication schemes are proposed in literature: chaotic parameter modulation, chaotic additive masking, chaotic switching, etc. System parameters play an important role in security problems, since system parameters and initial conditions are often treated as secret keys in chaos-based communication schemes. Although the parameter modulation scheme is a popular chaos-based communication scheme, the modulated parameter in the classic parameter modulation scheme can easily be broken. A definition of *secure synchronization* evaluates the security of synchronization using control theoretic terms. This definition requires the parameters ("password" candidate) satisfying *antiadaptive* and *antirobust* properties. Based on this definition, the generalized Lorenz system with an unknown parameter is thought to be a good candidate to implement secure synchronization.

The objective of the thesis is to give some criteria in the design of chaos-based communication schemes, and to provide such a scheme with high security and robustness as well.

Firstly, an adaptive observer is constructed in this thesis, and proved to be an exponential observer for the generalized Lorenz system. That is, it can estimate the state and the unknown parameter of the generalized Lorenz system simultaneously. To complete the proof, some dynamical properties of the generalized Lorenz system are developed to show that a certain persistently exciting condition holds.

Secondly, it is shown that the unidentifiable parameter is a good choice for a secret key, and a simple parameter identifiability technique based on differential 1-forms is applied to check unidentifiability. In fact, if the system parameter is not identifiable, it is obvious that there is no adaptive observer that can estimate the real parameter value. Hence this kind of system satisfies the antiadaptive property to a certain extent.

Thirdly, a modified parameter modulation scheme is provided in this thesis. It improves security in three aspects. One aspect is choosing an unidentifiable parameter as the modulated parameter such that it is secure against parameter identification techniques. The other two aspects are that the modulated parameter has more choices in key space, and is generated by means of a cryptosystem, which is constructed by a one-dimensional discrete system controlled by a Δ-modulated feedback. Numerical simulations illustrate that the power analysis attack and return map attack are ineffective in this scheme. In addition, the robustness of this scheme against uncertain disturbance is also investigated both analytically and experimentally. The results show that this scheme works properly if the uncertainty satisfies some given bounds.

Finally, this modified parameter modulation scheme is applied to a code division multiple access system with direct sequences approach. Numerical simulations show that the scheme achieves lower bit error rate (BER) values even if there is noise in the transmission channel.

Keywords: Chaotic synchronization, parameter modulation scheme, generalized Lorenz system, persistently exciting, adaptive observer, identifiability, cryptography, Δ-modulated feedback, code division multiple access.

Acknowledgement

While working on my research on the way to my Doctoral degree, I had the great fortune to meet many great people. First and foremost, I would like to acknowledge and thank my supervisor, Prof. Xiaohua Xia, for his invaluable advice, guidance, and patience throughout the past three years. His ideas and points of view have been a constant source of inspiration. This thesis would not have been possible without his insight and expertise. I would also like to thank Dr. Jiangfeng Zhang, for the amount of time he took to discuss my work with me and guide my study. His help improved the quality of my thesis and he gave me much insightful advice. Prof Xia and Dr Zhang have made a great contribution to sharpening my ability to solve scientific problems.

I have benefited enormously from the help of Dr Samuel Bowong, who gave me valuable advice at the beginning of my study. I would like to thank the Department of Electrical, Electronical and Computer Engineering (EECE) at the University of Pretoria for the financial support for my PhD study. I would like to thank all the staff at the department of EECE who helped me all these years. The department's assistance, financial and computing resources gave me peace of mind to focus on my study.

Thanks to all the friends I met here in Pretoria: Y. Li, Dr. Xiangtao Zhuan, Mingzhou Chen, Donghui Wei, Dongdong Jiang and many others gave me the opportunity to enjoy life here during these years. In particular, I want to mention Dr Zhuan from our control group, who gave me a lot of help in my study. From them I learned a great deal.

I am in debt to my parents and my sister. They of course provided the biggest support for my hard work during my graduate study.

Publications

Xiyin Liang, Jiangfeng Zhang, and Xiaohua Xia, “Adaptive synchronization for a class of chaotic systems”, The 8-th IEEE Africon, Windhoek, Namibia, 26–28 September, 2007.

Xiyin Liang, Jiangfeng Zhang, and Xiaohua Xia, “Adaptive synchronization for generalized Lorenz systems”, *IEEE Transactions on Automatic Control*, vol. 53, no. 7, pp. 1740–1746, 2008.

Xiyin Liang, Jiangfeng Zhang, and Xiaohua Xia, “Improving the security of chaotic synchronization with a Δ-modulated cryptographic technique”, *IEEE Transactions on Circuits and Systems II*, vol. 55, no. 7, pp. 680–685, 2008.

Xiyin Liang, Jiangfeng Zhang and Xiaohua Xia, “On the application of parameter identifiability to the security of chaotic synchronization”, The 7-th World Congress on Intelligent Control and Automation, Chongqing, China, 25–27 June, 2008.

Contents

Chapter 1

Introduction

1.1 Background

There has been tremendous interest in the chaotic system over the past decades. The chaotic system is characterized by sensitivity on the initial condition, random behaviour, a continuous broadband spectrum and decaying correlation function. These properties coincide with the requirements of secure communication and cryptography. Therefore chaos has potential application in several functional blocks of a digital communication system: compression, encryption, modulation.

Most communication schemes are based on synchronization of two chaotic systems. Synchronization means concurrent change of the states of two or more systems. According to [25]: "synchronize" means to concur or agree in time, to proceed or to operate at exactly the same rate, to happen at the same time [1]. Trajectories of chaotic systems diverge from each other exponentially even with a tiny difference in initial values. Chaotic systems intrinsically defy synchronization, because even two identical systems starting at nearly the same initial conditions would develop an unsynchronized manner. Nevertheless, [2] showed that it is possible to achieve synchronization in chaotic systems in 1990. Their scheme was viewed as a master-slave (driver-response) system [3]. The master system drives a part of the slave system, which has different initial conditions from the master system. To reach synchronization, the two (or more) chaotic systems adjust their motions to common behaviour [4]. The pioneer work in [2] attracted tremendous interest in the secure communication field, and synchronization of chaotic system has grown to be one of the richest areas during the past decades.

The pioneer work in [2] and several popular chaos-based communication schemes are reviewed in the following.

The authors in [2] considered an n-dimensional chaotic system ruled by the following equation $\dot{u} = f(u)$ where $u = \{u_1, \dots u_n\}$ is the state variable and f is an n-dimensional function.

Divide the system into two subsystems

$$\begin{cases} \dot{v} = g(v, w), \\ \dot{w} = h(v, w), \end{cases} \tag{1.1}$$

where $u = [\{v, w\},\ v = \{u_1, \dots u_m\},\ w = \{u_{m+1}, \dots, u_n\},\ g = \{f_1, \dots f_m\},$ and $h = \{f_{m+1}, \dots, f_n\}$. This equation defines the driver system. Now define a new subsystem

$$w' = h(v, w'), \quad w'(t_0) \neq w(t_0),$$

where t_0 is the initial time. This equation represents the response system whose trajectory is guided by the driver system by means of the driving signal v. In this framework, synchronization is defined as the identity between the trajectories of $w(t)$ and $w'(t)$, i.e., $\lim\limits_{t\to\infty} \|w' - w\| \to 0$, which is assured if all the Lyapunov exponents [5, 6] of the response system are negative [4, 2]. Reference [2] further shows its method by a Lorenz system

$$\begin{array}{ll} \text{driver} & \begin{cases} \dot{x} = \sigma(y - x), \\ \dot{y} = -xz + rx - y, \\ \dot{z} = xy - bz, \end{cases} \\ & \\ \text{response} & \begin{cases} \dot{y}' & = -xz' + rx - y', \\ \dot{z}' & = xy' - bz'. \end{cases} \end{array} \tag{1.2}$$

The Lyapunov exponents of the response system are $(-1.81, -1.86)$ by numerical calculation with parameters $\sigma = 10,\ b = 8/3,\ r = 60$ [2].

Some popular chaos-based communications schemes are additive masking, chaotic shift keying, chaotic parameter modulation, chaos shift keying, chaotic frequency modulation and chaotic cryptosystem. The following text focuses on three schemes: additive masking, parameter modulation and chaotic cryptosystem. Most of the schemes consist of two parts: a transmitter (driver system), which generates the chaotic signal and transmits it with the information signal, and a receiver (response system), which synchronizes with the driver system and decodes the information from the transmitted signal.

One of three schemes is chaotic signal masking [7, 8, 9]. The sender can add a given message to a chaotic signal directly and send it to the receiver as a driving signal. The receiver can extract the message by using the synchronization error between the driving and the regenerated signals. However, the message is required to be weaker than the chaotic mask signal. This method is sensitive to channel noises and parameter mismatches [10]. An observer-based approach for chaotic synchronization is provided to reduce the effect of channel noises in [9]. The transmitter and the receiver are constructed as the following, respectively:

$$
\begin{aligned}
&\text{transmitter} \quad \begin{cases} \dot{x} = Ax + f(x, y') + Bd + Ls, \\ y' = C^T x + s = y + s, \end{cases} \\
&\text{receiver} \quad \begin{cases} \dot{\hat{x}} = A\hat{x} + f(\hat{x}, y') + Bd + L(y' - \hat{y}), \\ \hat{y} = C^T \hat{x}, \end{cases}
\end{aligned}
\tag{1.3}
$$

where $s \in \mathbb{R}$ is the information signal and $y' \in \mathbb{R}$ is the transmitted chaotic signal and drives the receiver. The recovered signal is achieved by $s_R(t) = y'(t) - \hat{y}(t)$ and can be asymptotically recovered at the receiving end of the communication.

The second scheme of chaos-based communication is known as chaotic modulation [7, 11, 12]. In this idea, the information signal modifies the system states or parameters through an invertible procedure. References [7] and [8] are the first publications using chaotic modulation. In [7] and [8], the transmitter and the receiver are constructed as Lorenz systems

$$
\begin{aligned}
&\text{transmitter} \quad \begin{cases} \dot{u} &= \sigma(v - u), \\ \dot{v} &= ru - v - 20uw, \\ \dot{u} &= 5uv - bw, \end{cases} \\
&\text{receiver} \quad \begin{cases} \dot{u}_s &= \sigma(v_s - u_s), \\ \dot{v}_s &= ru - v_s - 20uw_s, \\ \dot{u}_s &= 5uv_s - bw_s. \end{cases}
\end{aligned}
\tag{1.4}
$$

The coefficient b of the transmitter equals 4.4 if the binary bit is “1”, and equals 4.0 if the binary bit is “0”. At the receiver, the modulation is detected by forming the difference between the transmitted signal and the reconstructed driving signal. Observer-based adaptive synchronization for communication is provided in [13, 14, 15]. At the receiving end, an adaptive observer is designed as the receiver, and the message is extracted through estimating the unknown parameter. For example, in [13], the author considered the following system:

$$\text{transmitter}\begin{cases} \dot{x}_d &= Ax_d + \phi_0(y_d) + B\sum_{i=1}^{m}\theta_i\phi_i(y_d), \\ y_d &= Cx_d, \end{cases} \tag{1.5}$$

where $x_d \in \mathbb{R}^n$, $y_d \in \mathbb{R}^l$ are the state and output vector, respectively, and $\theta = [\theta_1, \ldots, \theta_m]^T$ is the parameter vector (possibly representing the message). It is assumed that A, B, C and ϕ_i are known. An adaptive observer is designed at the receiver:

$$\begin{cases} \dot{x} &= Ax + \phi_0(y_d) + B\big[\sum_{i=1}^{m}\hat{\theta}_i\phi_i(y_d) + \hat{\theta}_0 G(y_d - y)\big], \\ y &= Cx, \\ \hat{\theta}_i &= \psi_i(y_d, y), \quad i = 0, 1, \ldots, m, \end{cases} \tag{1.6}$$

where $x \in \mathbb{R}^n$, $y \in \mathbb{R}^l$, $\theta_0 \in \mathbb{R}$ and $G \in \mathbb{R}^l$ is the vector of weights and $\psi_i's$ are suitably defined functions. The persistent excitation (PE) property of $\phi_i(y_d)$ ensures the convergence of parameter estimation.

In [16, 17], chaotic cryptography is provided for improving the degree of security. In this method, chaotic synchronization, combined with the classical cryptography technique, is used to enhance security. The chaos-based scheme for secure communication includes three steps: 1) encryption; 2) synchronization; 3) decryption. Two communications channels are used to send an encrypting signal and driving signal respectively in [16] instead of one channel in [17]. For example, in [17] the authors used Chua’s circuit and an $n-$shift cipher to implement their method, and the encrypter and decrypter are

$$\begin{aligned} &\text{Encrypter}\begin{cases} \dot{v}_1 &= \frac{1}{C_1}[G(v_2 - v_1) - f(v_R)], \\ \dot{v}_2 &= \frac{1}{C_2}[G(v_1 - v_2) + i_3], \\ \dot{i}_3 &= \frac{1}{L}[-v_2], \end{cases} \\ &\text{Decrypter}\begin{cases} \dot{\hat{v}}_1 &= \frac{1}{C_1}[G(\hat{v}_2 - \hat{v}_1) - f(v_R)], \\ \dot{\hat{v}}_2 &= \frac{1}{C_2}[G(\hat{v}_1 - \hat{v}_2) + \hat{i}_3], \\ \dot{\hat{i}}_3 &= \frac{1}{L}[-\hat{v}_2], \end{cases} \end{aligned} \tag{1.7}$$

where $v_R(t)$ is the transmitted signal, $v_2(t)$ is the key signal, $p(t)$ denotes the message signal, $f(v_R) = G_b v_R + \frac{1}{2}(G_a - G_b)(|v_R + E| - |v_R - E|)$, C_1, C_2, L, G_a, G_b, G and E are system parameters. The transmitted signal v_R is $v_1 - e(p(t))$, where $e(p(t))$ is the encrypted signal defined below:

$$e(p(t)) = \underbrace{f_1 \cdots f_1(f_1(}_{n} p(t), \underbrace{v_2(t)), v_2(t) \cdots v_2(t))}_{n},$$

f_1 is a nonlinear function,

$$f_1(x,k) = \begin{cases} (x+k) + 2h, & -2h \le (x+k) \le 2h, \\ (x+k), & h < (x+k) < h, \\ (x+k) - 2h, & h \le (x+k) \le 2h, \end{cases}$$

h is chosen such that $p(t)$ and $v_2(t)$ lie within $(-h, h)$. The recovered encrypted signal $\hat{e}(p(t))$ is defined as $\hat{e}(p(t)) = \hat{v}_1 - v_R$. One has $\hat{e}(p(t)) \to e(p(t))$ when the synchronization is achieved.

In contrast to a synchronization-based technique, chaos has also been used to design a cryptosystem based on direct applications of chaotic transformations to plaintexts. A cryptosystem is an algorithm that converts an original message, referred to as plaintext, into a random message, referred to as ciphertext, and recovers the message in its original form [18]. Chaos and cryptography have many common features, such as sensitivity and ergodicity. Matthews [19] was the first to design a cryptosystem based on a discrete chaotic system. Then Habutsu *et al.* [20] constructed a chaotic block cipher using a skew tend map. Baptista [21] developed a cryptosystem in which initial condition and system parameter were chosen as keys. Kocarev used a systematic procedure to create a chaos-based cipher by means of a logistic map in [22]. Based on discretization of the skew tent map, a new secure cryptosystem was constructed by Masuda in [23]. Pareek *et al.* [18] proposed a symmetric block cipher that does not explicitly use the system parameter as secret key. However, these parameters are generated by an external secret key. This algorithm will be adopted with proposed scheme in this thesis. In this proposed scheme, this algorithm is used to construct a cryptosystem based on a one-dimensional discrete system controlled by a Δ-modulated feedback, and the cryptosystem is one component of a modified parameter modulation scheme.

1.2 Motivations

Security is an important aspect of synchronization. Research on synchronization has been boosted mainly by its possible use in secure communication and encryption. The chaos-based communication schemes are expected to be secure because of two reasons: 1) it is difficult to extract the hidden message by any spectrum method owing to the broadband spectrum; 2) when a set of system parameters are treated as encryption key, it is impossible to recover the message without precise knowledge about them [24, 25].

However, some research shows that most chaos-based schemes have a low level of security. The nonlinear dynamical forecasting method is the first attack method in literature, which is proposed by Short *et al.* in [26, 27]. It can extract the chaotic carrier signal in chaotic additive masking and some chaotic modulation schemes. Then the message can be obtained by removing the carrier signals from transmitted ciphertext signal. Power spectral analysis and return map are the other two powerful attack methods, and even they do not require the structure of the chaotic systems. Pérez and Cerdeira [28] designed the return map method to extract the message masked by a chaotic signal. For a discrete time series $\{x_i\}_{i=1}^{n}$, one plots each x_i against its successor value x_{i+1}. This is called a return map [6]. The attractor of the return map changes when one of the system parameters changes. Low-pass filter and quantization are used in power spectral analysis and the generalized synchronization method [29]. The plaintext can be recovered after quantizing the low-pass filtered signal, which is a modified ciphertext (transmitted signal). For example, when the parameter b changes in (5.2) with the message signal in the parameter modulation method, the amplitude of the transmitted signal's low-frequency spectrum will change. So the message signal can be recognized through investigating the variation of the amplitude. The parameter estimation or parameter identification technique is also a powerful attack method. From the viewpoint of control theory, some adaptive and robust control methods can estimate the system parameters, hence they can be considered as possible attack methods [24, 25].

Besides the security problem, robustness against uncertain perturbation is another important problem. For example, there is unavoidable error when the chaotic map is executed by a computer, because the real number is represented by a binary bits sequence of finite length in a digital computer. Errors may result in some serious problems, such as short cycle length or nonideal distribution and correlation function

[30, 31]. However, most research focuses on the influence of uncertainty on security. Little work has been done on robustness against uncertainty. Uncertainty will make the chaotic orbits stray from the real ones (without error). After a number of iterations, the chaotic orbits may be completely different from theoretical ones [32]). Therefore the chaotic cipher cannot work properly.

There is an interesting paradox between security and robustness, which has been pointed out in [33, 34, 25]. Generally high security implies high sensitivity. Many chaos-based communication schemes may be decrypted by using approximate parameter values, because they are not sufficiently sensitive to parameter mismatch [35]. Nevertheless, there are unavoidable parameter perturbation and parameter mismatch in the practical environment. Robust synchronization means that synchronization is achieved even if there are parameter perturbation and parameter mismatch. Obviously, a balance has to be reached between these two aspects. A trade-off between security and robustness can be achieved at the cost of some other factors. For example, using high-dimension chaotic systems and more parameters will achieve a good balance between the two aspects at the expense of memory cost and encryption time in software and hardware implementation.

1.3 Objectives

The objectives of this thesis are to give some criteria in the design of chaos-based communication schemes, and to provide such a scheme with high security and robustness as well.

The chaotic synchronization has been formulated into an observer design problem by control theory [24, 36, 37]. Hence, one of the objectives is to give some criteria in control theoretic terms, such that the chaos-based communication schemes are secure against some popular attacks. The other objective is to provide a practical scheme based on the criteria. Moreover, the scheme also works properly when there are perturbations in the parameters or transmission channel.

1.4 Contributions

In this study, the above problems on security and robustness will be considered. Reference [24] suggested a definition of *secure synchronization* and the generalized Lorenz system with an unknown parameter, which are the original motivation of this thesis. Chapter 3 gives a proof of an exponential observer for the generalized Lorenz system, which shows that the unknown parameter can be estimated. Hence the unidentifiable parameters are recommended as the secret key. Chapter 3 also provides a modified Lorenz system with unidentifiable parameters such that this system satisfies the requirements of *secure synchronization* to a certain extent. A new parameter modulation scheme is provided in Chapter 4 to improve security in three aspects: unidentifiable parameter, large key space and complex parameter generating process. Numerical simulations show that this scheme is secure against power analysis attack and return map attack. The analysis of the robustness of this scheme gives some sharp upper bounds of uncertainty. The modified parameter modulation scheme is applied in Chapter 5 to the CDMA system. In the application and analysis of the robust problem, the trade-off between security and robustness is also considered. Satisfactory robustness is obtained by degrading security.

The main contributions are listed below:

1. An exponential observer is constructed to achieve synchronization for a generalized Lorenz system with an unknown parameter;

2. To improve security, unidentifiable parameters are chosen as the secret key. The parameter identifiability technique based on differential 1-forms is also applied to test the security of the system parameters in chaos-based communication schemes;

3. A modified parameter modulation communication scheme, which is based on a 1-D discrete system controlled by a Δ-modulated feedback, is proposed to improve security. A cryptosystem is constructed by this 1-D discrete system in order to generate the modulated parameter. This generating process enlarges the key space and increases the difficulty of decryption. Hence security is improved in this scheme.

4. The proposed modified parameter modulation scheme is robust under errors or uncertainties within a certain range. Simulations show that selecting appropriate

parameters can improve the robust property at the expense of security.

5. The modified parameter modulation scheme is applied to a direct sequences code-division-multiple-access (DS-CDMA) scheme. Some encryption steps are simplified to ensure that the CDMA system is robust, when there is noise in the transmission channel.

1.5 Outline of thesis

The thesis is organized as follows. Chapter 2 introduces some preliminary knowledge, which will be used in the following chapters. It consists of the basis of the cryptosystem and two powerful breaking methods, power analysis attack and return map attack.

At the beginning of Chapter 3, the definition of secure synchronization and the generalized Lorenz system are introduced. The authors of [24] formulated the synchronization problem as an observer design problem. Then a conjecture is proposed
Conjecture: The generalized Lorenz system allows secure synchronization.
In this chapter, a kind of adaptive observer proposed in [38] is constructed to achieve synchronization for the generalized Lorenz system with one unknown parameter, and is proved to be an exponential observer. This result shows that the unknown parameter of the generalized Lorenz system can be estimated. To complete the proof, some dynamical properties of the generalized Lorenz system are found by analytic techniques.

To protect the parameter against different kind of parameter identification methods, the identifiability of system parameters should be checked during the design of a chaos-based communication scheme. Identifiability can be treated as the criterion to measure the security of the parameter. The linear algebraic method based on differential 1-forms [39, 40] is used to test the identifiability of the chaotic system. This method is illustrated through studying the identifiability of a modified Lorenz system.

To improve the security of chaotic synchronization, a modified parameter modulation scheme is proposed in Chapter 4, which uses an encryption function to modulate the parameter. The encryption function is implemented by a one-dimensional discrete system controlled by a Δ-modulated feedback. This discrete system is proved to be a chaotic self-map when parameter a belongs to $(\sqrt{2}, 2)$. Hence it is suitable to implement an algorithm as proposed in [18]. Numerical simulations show that the scheme is secure against power spectral analysis and return map attack. The robustness of a cryptosystem, the important component of the proposed modified parameter modulation scheme, is investigated analytically and experimentally in the last part of Chapter 4. In order to prevent the uncertainty from destroying the cryptosystem, this chapter also gives the upper bounds of the uncertainties, which appear in initial conditions and system parameter.

The last chapter considers a chaos-based code-division-multiple-access (CDMA) system with direct sequence (DS) approach, to which some results in the previous chapters are applied. Numerical simulations show that CDMA system has good performance when both the transmission channel and synchronization channel carry noises.

Chapter 2

Preliminary knowledge

2.1 Chapter outline

This chapter introduces some preliminary knowledge, which will be used in the following chapters. Section 2.2 introduces power analysis attack and return map attack, which are two popular attacks for chaos-based communication schemes. Section 2.3 gives the basic structure, general assumption and attacks of the general cryptosystems, which helps the reader to understand this thesis well.

2.2 Power spectral and return map attack methods

Different methods have been proposed to attack chaos-based communication schemes. In chaotic masking schemes, the transmitted message can be extracted using different methods: power spectral analysis, return map analysis, autocorrelation and cross-correlation analysis, etc [28, 29, 41]. Return map, correlation analysis and generalized synchronization technique are used to extract the transmitted message for chaotic switching or modulation schemes [28, 29, 42]. For the scheme with encryption technique proposed in [17], the authors in [43] used the nonlinear dynamic forecasting techniques to extract the encrypted message.

This thesis focuses on improving security of the parameter modulation scheme. The modulated parameter in many schemes has two values corresponding to transmitted bit ‘1’ or ‘0’ [8, 44]. That is why many attacks, such as return map, power analysis and generalized synchronization attacks, can extract the transmitted message. In order to illustrate the pathology of the schemes proposed in [8, 44], only power analysis and return map attacks are considered as they are enough to distinguish the values of the modulated parameter, and the other attacks are not considered.

Although several chaos-based communication schemes are reviewed in Chapter 1, the exact definition of synchronization is not given there. Hence in this section a widely used definition is introduced. Then two attack methods, power analysis and return map, are presented to break a typical parameter modulation scheme [44].

Different notions of synchronization are proposed for chaotic systems in literature [45, 46, 47], such as identical synchronization, generalized synchronization and phase synchronization. Identical synchronization is the strongest and most frequently used definition, and this thesis focuses on this definition.
Identical Synchronization [45]: Two continuous-time dynamical systems $\dot{x} = f(x)$ and $\dot{x}' = f'(x')$ are said to synchronize identically if

$$\lim_{t\to\infty} \| x(t) - x'(t) \| = 0$$

for any combination of initial states $x(0)$ and $x'(0)$.

From a communications perspective, one may think of the two systems as the transmitter and the receiver. This definition means that the state of the receiver system converges asymptotically to that of the transmitter, which is similar to the definitions proposed in [1, 48].

In Chapter 1, it was mentioned that security is an important problem in chaos-based communication schemes, and power analysis and return map are two powerful attack methods, which do not require prior knowledge of the chaotic system. In the following these two methods are illustrated to attack a parameter modulation scheme based on the Lorenz system.

The author in [44] designed an observer-based receiver to synchronize with a given transmitter with unknown parameters. Then the approach is applied to chaos-based secure communication. The efficiency of the scheme is represented through a Lorenz system described by

$$\begin{cases} \dot{x}_1 &= -\sigma_1 x_1 + \sigma_2 x_2, \\ \dot{x}_2 &= r\sigma_1 - x_2 - x_1 x_3, \\ \dot{x}_3 &= x_1 x_2 - b x_3. \end{cases} \tag{2.1}$$

It is well known that system (2.1) exhibits chaotic behaviour with the standard parameters $(\sigma_1, \sigma_2, r, b) = (10, 10, 28, 8/3)$. The transmitted signal is for synchronization x_1. The parameter σ_1 is modulated by the binary encoded plaintext, so that it is $\sigma_1 + 2.5$ if the plaintext bit is '1' and $\sigma_1 - 2.5$ if the plaintext bit is '0'. So system (2.1) can be described as an uncertain system

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -8/3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} y\theta, \tag{2.2}$$

$$y = Cx = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix} x = x_1$$

where the uncertainty $\theta = \Delta\sigma_1 = \pm 2.5$. An observer-based receiver is constructed as

$$\begin{bmatrix} \dot{\hat{x}}_1 \\ \dot{\hat{x}}_2 \\ \dot{\hat{x}}_3 \end{bmatrix} = \begin{bmatrix} -10 & 10 & 0 \\ 28 & -1 & 0 \\ 0 & 0 & -8/3 \end{bmatrix} \begin{bmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{x}_3 \end{bmatrix} + \begin{bmatrix} 0 \\ -\hat{x}_1 \hat{x}_3 \\ \hat{x}_1 \hat{x}_2 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} y\hat{\theta} + L(x_1 - \hat{x}_1), \tag{2.3}$$

$$\dot{\hat{\theta}} = -5y(x_1 - \hat{x}_1),$$

where $L = \begin{bmatrix} 0 & 38 & 0 \end{bmatrix}^T$.

It is important that the bit duration is much larger than the convergence time of the adaptation law. In comparing Figure 2.2a) with Figure 2.2b), it is found that the uncertainty θ is estimated exactly, and the transmitted signal can be recovered from the estimated parameter values.

But this method has a low degree of security. Making use of power analysis attack or return map attack, the transmitted signal can be decoded without the prior information of the Lorenz model [29, 28]. Assume the transmitted signal is $y(t)$, the power analysis attack method is a procedure consisting of three steps [29]:

1. the transmitted signal $y(t)$ is squared;

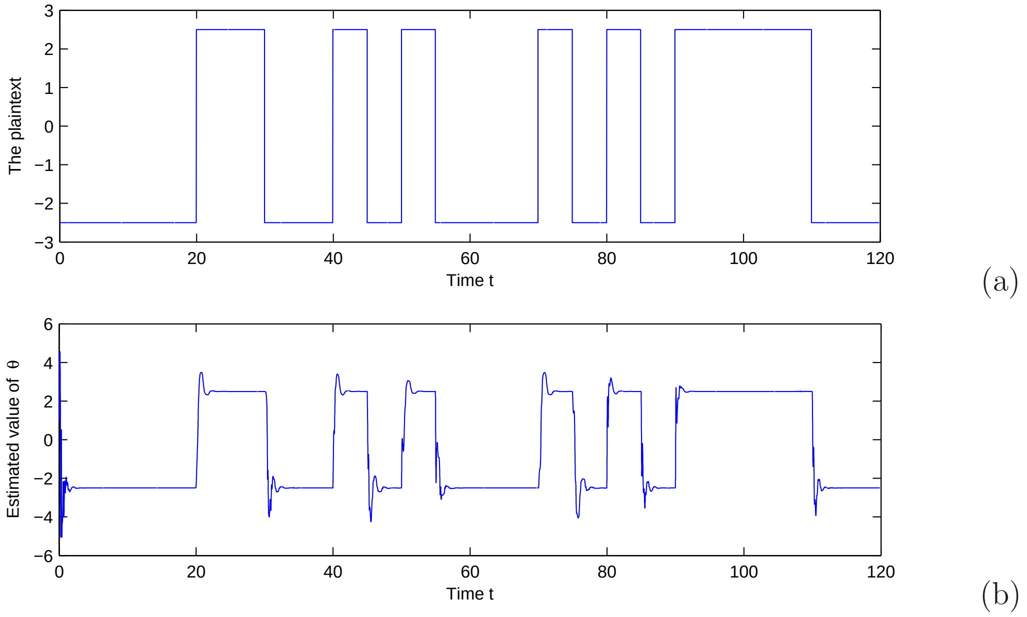


Figure 2.1: Illustration of observer (2.3): (a) the plaintext; (b) the estimated parameter $\hat{\theta}$.

2. a low-pass filter to $y^2(t)$ is employed;

3. the low-pass filtered $y^2(t)$ is binary quantized.

Figure 2.2 and Figure 2.3 illustrate the procedure. Figure 2.2a) is the plaintext. Figure 2.2b) is the transmitted signal containing messages, that is, the transmitted signal x_1. Figure 2.3a) shows the low-pass filtered squared ciphertext signal, that is, x_1^2 is low-pass filtered. Then this signal is binary quantized to obtain the recovered plaintext, which is shown in Figure 2.3b). In comparing Figure 2.2a) with Figure 2.3b), it is obvious that power analysis exhibits good performance in recovering the plaintext.

Now consider the return map attack method. For a discrete time series $\{x_i\}_{i=1}^{n}$, one plots each x_i against its successor value x_{i+1}. This is called a return map in [6]. Assume that the transmitted signal is x_1. Starting from the initial point, X_n denotes the n-th local maximum of x_1, and Y_n denote the n-th local minimum. As described by Perez and Cerdeira [28], the return maps X_{n+1} vs X_n and Y_{n+1} vs Y_n are not used directly, the linear combinations

$$A_n = \frac{X_n + Y_n}{2}, \quad \text{and} \quad B_n = X_n - Y_n,$$

are used instead to get better results. The return map A_n *vs* B_n has a simple attractor, which is shown in Figure 2.4. A small change in the parameters of the transmitter

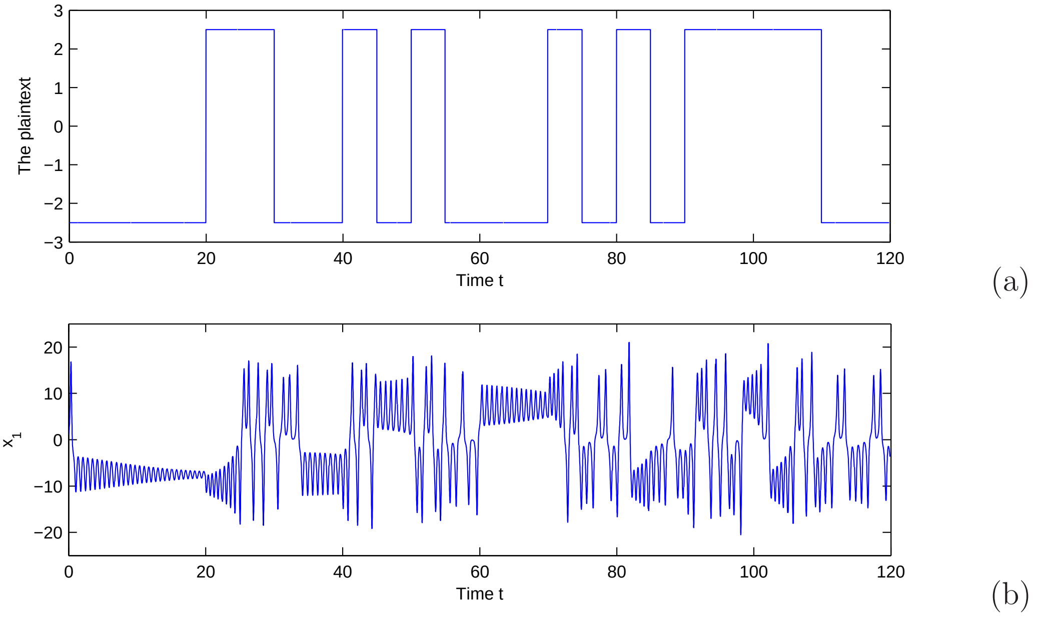


Figure 2.2: Power analysis attack: (a) the plaintext; (b)the ciphertext x_1.

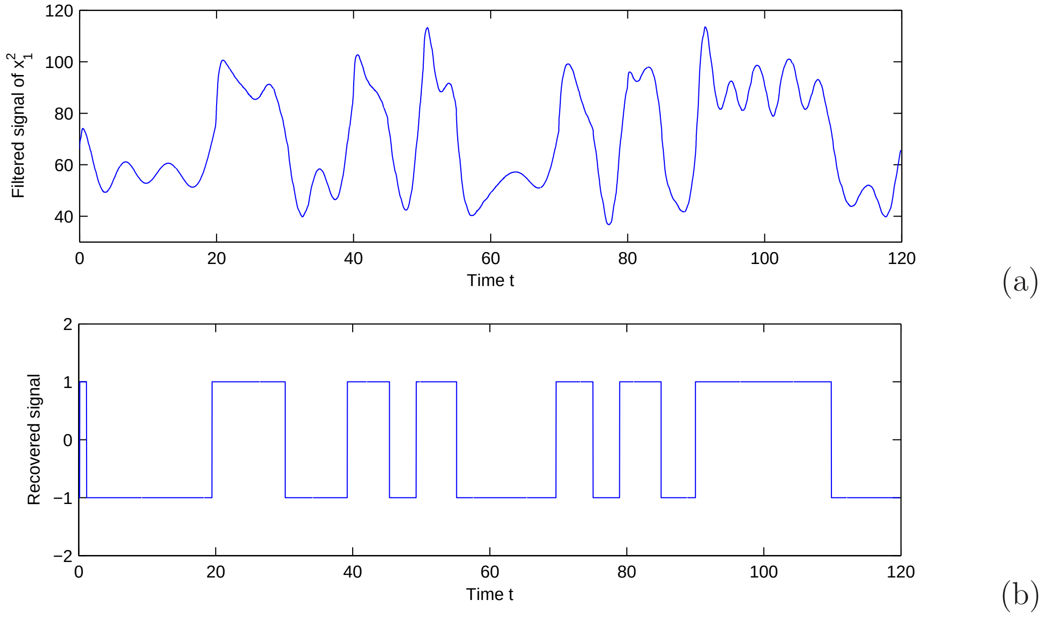


Figure 2.3: Power analysis attack: (a) low pass filtered squared ciphertext signal; (b) the recovered plaintext.

affects the attractor of the chaotic system. It is obvious that each segment is split into two strips in the return map. The reason is that the switching between two parameter values results in the switching between two parallel strips of each segment. According to the line in which the point (A_n, B_n) falls, one can easily unmask the current value of the plaintext.

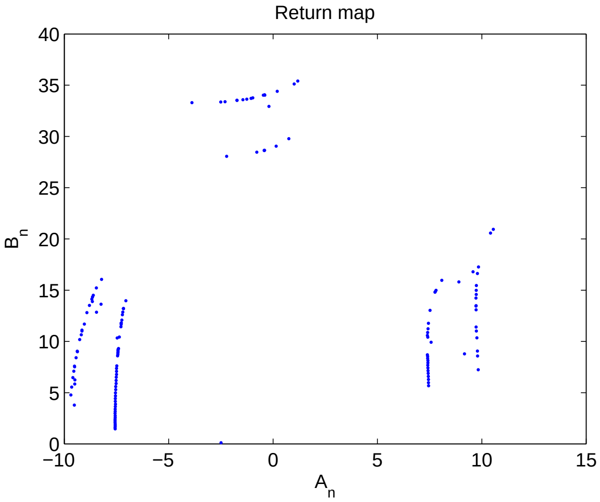


Figure 2.4: Return map: A_n vs B_n.

2.3 Chaos-based cryptography

When performing cryptanalysis on an cryptosystem, the general assumptions are those listed below [49]:

- Public channel: An opponent has access to the transmission channel such that he knows an arbitrary segment of the ciphertext.
- Public structure: An opponent knows the structure of the encryption system and a priori probability of the key that is used. Under these conditions, only the key is kept secret to the intruder. This requirement is referred to as Kerckhoff's principle.

The analysis of discrete-value cryptosystems is based on a model that characterizes a cryptosystem by five sets [33, 49, 50]:

- the plaintext space $\mathcal{P}$ is the set of possible plaintexts;
- the ciphertext space $\mathcal{C}$ is the set of possible ciphertexts;
- the key space $\mathcal{K}$ is the set of possible keys;
- two function spaces $\mathcal{E}$ and $\mathcal{D}$ are the sets of possible encryption and decryption transformations, respectively. For each key $k \in \mathcal{K}$, there exists an encryption function $e_k \in \mathcal{E}$ and a corresponding decryption function $d_k \in \mathcal{D}$ such that $d_k(e_k(p)) = p$ for every plaintext $p \in \mathcal{P}$.

For example, Block cipher mentioned in [22], one of the encryption systems, is a static transformation $F_k : \mathcal{P} \to \mathcal{C}$, which transforms a relatively short string in plaintext space to a string in ciphertext space under control of a secret key, where $\mathcal{P}$,$\mathcal{C}$ and k denote the plaintext space, ciphertext space and secret key, respectively. Let the plaintext $p = \{p_0, p_1, \ldots\}$, then each plaintext block $p_i \in \mathcal{P}$ is encrypted such that

$$F_k : \{p_0, p_1, \ldots\} \to \{F_k(p_0), F_k(p_1), \ldots\}.$$

The crucial measure for the quality of a public channel cryptosystem is security, which is its capability to withstand the attempts of an intruder to gain the information of the plaintexts. The security of a cryptosystem is evaluated by means of attacks, which try to break the system. Attacks on a cryptosystem can be distinguished according to the opponent's access to additional information. They are enumerated as follows, ordered from the hardest type of attack to the easiest [33, 49]:

- Ciphertext-only: The opponent possesses a string of ciphertext y.
- Known-plaintext: The opponent possesses a string of plaintext x, and the corresponding ciphertext y.
- Chosen plaintext: The opponent has obtained temporary access to the encryption machinery. Hence he can choose a plaintext string x and construct the corresponding ciphertext string y.
- Chosen ciphertext: The opponent has obtained temporary access to the decryption machinery. Hence he can choose a ciphertext string y and construct the corresponding plaintext string x.

In each of these four attacks, the main intention is to determine the secret key, or one of its equivalent forms, which allows the opponent to decrypt arbitrary ciphertexts. Exhaustive key search is another kind of attack, which defines the highest upper bound of computational effort for breaking a given cipher. In this way, any cipher can be attacked with an effort that is proportional to the size of the key space.

To resist common attacks, two general design principles of practical ciphers are confusion and diffusion. As mentioned in [22], the first property means “spreading out of the influence of a single plaintext digit over many ciphertext digits so as to hide the statistical structure of the plaintext. An extension of this idea is to spread the influence of a single key digit over many digits of ciphertext”. Thus the statistical structure of the plaintext is difficult to obtain through studying the ciphertext. The second property means “use of transformations which complicate dependence of the statistics of ciphertext on the statistics of plaintext” [22].

2.4 Summary and conclusion

This chapter introduces some preliminary knowledge, which will be used in the following chapters. The basic structure and general assumption of the general cryptosystems will help the reader to understand why only system parameters are considered when discussing the security problem. Power analysis attack and return map attack will be used in Chapter 3. The chosen ciphertext attack will also be considered in Chapter 3.

Chapter 3

Adaptive synchronization of generalized Lorenz system

3.1 Chapter outline

This chapter gives some criteria in the design of chaos-based communication schemes. Section 3.2 is an overview of this chapter. Section 3.3 and Section 3.4 introduce some preliminary knowledge. Section 3.3 consists of the basis of a kind of adaptive observer and the state affine form [51, 38]. Section 3.4 introduces the definition of *secure synchronization* and the generalized Lorenz system. In Section 3.5, the adaptive observer introduced in Section 3.3 is constructed and proved to be an exponential observer for the generalized Lorenz system. Section 3.6 is the application of parameter identifiability to chaotic synchronization. The conclusion is given in Section 3.7.

3.2 Introduction

According to a fundamental assumption in cryptography, Kerckhoff's principle, the intruder knows the details of the cryptosystems, including the design and the implementation, except the secret key. In many proposed chaotic synchronization schemes, some initial conditions and parameters are treated as the key. It is usually difficult to recover the hidden message without knowing the exact value of the key. Hence the security of the parameter is an important problem for chaotic synchronization.

However, a number of references point out that many adaptive and robust control techniques can estimate the true parameter value. Moreover, a few works focus on how to evaluate the security and performance of chaos-based communication schemes. For this problem, [24] gives a definition of secure synchronization using control theoretic terms. Secure synchronization includes two properties: antiadaptive and antirobust secure. Antiadaptive secure means that there is no adaptive law to estimate the parameter ("password" candidate). Antirobust property is similar to distinguishability; different system parameter values result in different system states. Based on this definition, [54] presents a new class of chaotic synchronization with an unknown parameter, the generalized Lorenz system. This system is thought to be a good candidate to implement secure synchronization. The reason is that the unknown parameter may not be estimated by a class of adaptive observer. Details can be found in Section 3.4. The next section introduces a kind of adaptive observer proposed in [38].

In Section 3.5, it will find more properties of the generalized Lorenz system with an unknown parameter, and thus show that its state and unknown parameter can actually be estimated by the adaptive observer introduced in Section 3.3. To complete the work, the output of this system is proved to satisfy PE property through investigating some dynamical properties of the generalized Lorenz system. It is noted that this proof of PE property is new in literature although [24] mentioned that it may hold owing to the transitivity property. Moreover, the adaptive observer is successfully constructed to estimate the state and parameter of the generalized Lorenz system, and it is also proved to be an exponential observer. This implies that this system is not a good candidate to implement secure synchronization, according to the definition of secure synchronization proposed in [24]. Both theoretic proof and numerical simulations are provided.

Regarding the method to choose a parameter as secret key, [52] claims that an identifiable parameter may be a good choice, because the parameter is difficult to be found through a brute force attack (exhaustive search of the key space). However, identifiability implies that it is possible to determine an estimated parameter (secret key) by parameter identification techniques. Therefore Section 3.6 shows that the unidentifiable parameter based on differential 1-forms [39, 40] is a good choice for the secret key. The linear algebraic method is used to test the identifiability of the chaotic system. A modified Lorenz system is utilized to illustrate this method and to design a chaos-based communication scheme.

3.3 An exponential adaptive observer

Synchronization of the chaotic system is a popular research topic because of its possible use in secure communication. Synchronization has been formulated as an observer design problem from a control viewpoint [36, 37]. In a real system, there are always measurement errors of parameter values. Hence the adaptive observer is designed to estimate the parameters and state variables simultaneously. Convergence of estimated parameters to their true values and the rate of convergence are closely related to the PE property of certain signals. Thus the definition of PE is given before introducing the adaptive observer proposed in [38]:

Definition 1 [53]: A vector function $w : \mathbb{R} \to \mathbb{R}^n$ is *persistently exciting (PE)* if there exist $\alpha_1,\ \alpha_2,\ T > 0$ such that

$$\alpha_1 I \leq \int_t^{t+T} w(s)w^T(s)\,ds \leq \alpha_2 I, \qquad \forall t \geq 0. \tag{3.1}$$

The PE condition requires that $w(s)$ oscillates sufficiently in space so that the integral of the matrix $w(s)w^T(s)$ is uniformly positive definite over any interval of length T, although the matrix $w(s)w^T(s)$ is singular for all s. The condition has another interpretation in scalar form [53]

$$\alpha_1 \leq \int_t^{t+T} (w^T(s)x)^2\,ds \leq \alpha_2, \qquad \forall t \geq 0,\ |x| = 1,$$

where $x \in \mathbb{R}^n$, which appears as a condition on the energy of w in all directions.

The authors in [38] considered a linear time varying multiple input multiple output system of the form

$$\begin{cases} \dot{x}(t) &= A(t)x(t) + B(t)u(t) + \Psi(t)\theta, \\ y(t) &= C(t)x(t), \end{cases} \tag{3.2}$$

where $x(t) \in \mathbb{R}^n,\ y(t) \in \mathbb{R}^m$ and $u(t) \in \mathbb{R}^l$ are the state, output and input vectors, respectively; $A(t),\ B(t),\ C(t)$ and $\Psi(t)$ are known matrices of appropriate dimensions which are piecewise continuous and uniformly bounded in time; and $\theta \in \mathbb{R}^p$ is an unknown constant vector. The following summarizes the main results of [38]:

Condition 1. There exists a bounded time-varying matrix $K(t) \in \mathbb{R}^{n\times m}$ such that the system $\dot{\tau}(t) = [A(t) - K(t)C(t)]\tau(t)$ is exponentially stable.
Condition 2. There exist positive constants $\alpha_1,\ \beta_1,\ T_1$ such that

$$\alpha_1 I \leq \int_t^{t+T_1} \Upsilon^T(s)C^T(s)\Sigma(s)C(s)\Upsilon(s)\, ds \leq \beta_1 I, \quad \forall t \geq t_0,$$

for some $t_0 \geq 0$ and some bounded positive definite matrix $\Sigma(t) \in \mathbb{R}^{m\times m}$, where $\Upsilon(t) \in \mathbb{R}^{n\times p}$ is the solution of $\dot{\Upsilon}(t) = [A(t) - K(t)C(t)]\Upsilon(t) + \Psi(t)$.

Condition 2 is a PE condition typically required for parameter identification. Under Condition 1 and 2, the following theorem provides a global exponential adaptive observer for system (3.2):
Theorem 3.1: Suppose Condition 1 and 2 hold. Let $\Gamma \in \mathbb{R}^{p\times p}$ be any symmetric positive definite matrix. Then the following system

$$\begin{cases} \dot{\hat{x}} = [A(t) - K(t)C(t)]\hat{x}(t) + B(t)u(t) + K(t)y(t) + \Psi(t)\hat{\theta} + \Upsilon(t)\dot{\hat{\theta}}(t), \\ \dot{\hat{\theta}}(t) = \Gamma\Upsilon^T(t)C^T(t)\Sigma(t)[y(t) - C(t)\hat{x}(t)], \\ \dot{\Upsilon}(t) = [A(t) - K(t)C(t)]\Upsilon(t) + \Psi(t), \end{cases} \tag{3.3}$$

is a global exponential adaptive observer for system (3.2) in the sense that for any initial conditions $x(t_0),\ \hat{x}(t_0),\ \hat{\theta}(t_0)$ and any $\theta \in \mathbb{R}^p$, the errors $x(t) - \hat{x}(t)$ and $\theta - \hat{\theta}(t)$ exponentially decay to zero when $t \to \infty$.

Remark 1: If the PE does not hold, the simulation shows that the identification of parameter may fail. The synchronization can be achieved if all the states of the generalized Lorenz system tend to zero. Note that the generalized Lorenz system is not chaotic if the PE does not happen for some parameters.

The above result also can be applied to a class of nonlinear system, which can be described by a state affine representation [51, 38].

$$\begin{cases} \dot{x}(t) = A(u(t), y(t))x(t) + \varphi(u(t), y(t)) + \Phi(u(t), y(t))\theta, \\ y(t) = Cx(t), \end{cases} \tag{3.4}$$

where θ is an unknown constant or slow time varying vectors, and the components of $A(u(t), y(t)), \varphi(u(t), y(t))$ and $\Phi(u(t), y(t))$ are continuous functions depending on u and y, and uniformly bounded.

In the following, the Lorenz system and generalized Lorenz system are written in a state affine form. First consider following famous Lorenz chaotic systems,

$$\begin{cases} \dot{x}_1 &= -\sigma_1 x_1 + \sigma_2 x_2, \\ \dot{x}_2 &= \rho x_1 - x_2 - x_1 x_3, \\ \dot{x}_3 &= x_1 x_2 - \beta x_3, \\ y &= x_1, \end{cases} \tag{3.5}$$

where y is the output, $\sigma_1,\ \sigma_2,\ \rho$ and β are positive parameters. Assume that parameter ρ is unknown, then system (3.5) can be represented as

$$\begin{aligned} \dot{x} &= \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -\sigma_1 & \sigma_2 & 0 \\ 0 & -1 & -y \\ 0 & y & \beta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 \\ y \\ 0 \end{bmatrix} \theta \\ &= A(y)x + \Phi(y)\theta, \end{aligned} \tag{3.6}$$

where

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},\ A(y) = \begin{bmatrix} -\sigma_1 & \sigma_2 & 0 \\ 0 & -1 & -y \\ 0 & y & \beta \end{bmatrix},\ \Phi(y) = \begin{bmatrix} 0 \\ y \\ 0 \end{bmatrix} \text{ and } \theta = \rho.$$

In [24] the authors defined the generalized Lorenz system,

$$\begin{aligned} \frac{d\eta}{dt} &= \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 + \eta_2 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - \frac{1}{2}(\tau + 1)\eta_1^3 \\ \lambda_3\eta_3 + K_1(\tau)\eta_1^2 \end{bmatrix}, \\ y &= \eta_1, \end{aligned} \tag{3.7}$$

where $\eta = \begin{bmatrix} \eta_1 & \eta_2 & \eta_3 \end{bmatrix}^T$ and $K_1(\tau) = \dfrac{\lambda_3(\tau+1) - 2\tau\lambda_1 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}$. It also can be rewritten as state affine form,

$$\begin{aligned} \frac{d\eta}{dt} &= \begin{bmatrix} (\lambda_1 + \lambda_2) & 1 & 0 \\ -\lambda_1\lambda_2 & 0 & -(\lambda_1 - \lambda_2)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix} + \begin{bmatrix} 0 \\ -\frac{1}{2}\eta_1^3 \\ \frac{\lambda_3 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}\eta_1^2 \end{bmatrix} + \begin{bmatrix} 0 \\ -\frac{1}{2}\eta_1^3 \\ \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\eta_1^2 \end{bmatrix} \theta \\ &= A(y)\eta + \varphi(y) + \Phi(y)\theta, \end{aligned} \tag{3.8}$$

where

$$A(y) = \begin{bmatrix} (\lambda_1 + \lambda_2) & 1 & 0 \\ -\lambda_1\lambda_2 & 0 & -(\lambda_1 - \lambda_2)y \\ 0 & 0 & \lambda_3 \end{bmatrix}, \quad \varphi(y) = \begin{bmatrix} 0 \\ -\frac{1}{2}y_1^3 \\ \frac{\lambda_3 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}y_1^2 \end{bmatrix},$$

$$\Phi(y) = \begin{bmatrix} 0 \\ -\frac{1}{2}y_1^3 \\ \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}y_1^2 \end{bmatrix} \quad \text{and} \quad \theta = \tau.$$

3.4 Secure synchronization and generalized Lorenz system

As mentioned in Chapter 1, many robust and adaptive control methods can be treated as possible attacks against synchronization-based communication schemes. The authors in [24] gave a definition of *secure synchronization* using control theoretic terms, and provided a new design of a class of chaotic system to overcome the aforementioned drawbacks of those communication schemes. This section recalls the main results of [24], which will be used in the following sections. The following nonlinear system with parameter vector μ is considered,

$$\dot{x} = f(x, t, \mu), \quad x \in \mathbb{R}^n, \quad \mu \in \mathbb{R}^m, \tag{3.9}$$

where μ is a "password" candidate and possible unknown.

Definition 2 [24]**:** If there exists an auxiliary output, $y = h(x) \in \mathbb{R}^p,\ p < n$, such that the following system is a smooth asymptotic observer for the solution $x(t),\ t \geq t_0$,

$$\dot{\hat{x}} = f(\hat{x}, t, \mu) + \varphi(h(x), h(\hat{x}, \hat{x}, \mu),\ x, \hat{x} \in R^n, \mu \in R^m, \tag{3.10}$$

then system (3.9) is said to achieve a *static synchronization* of a solution $x(t),\ t \geq t_0$.

If there does not exist any adaptive observer of the form

$$\begin{cases} \dot{\hat{x}} & = f(\hat{x}, t, \hat{\mu}) + \varphi(h(x), h(\hat{x}), \hat{x}, \hat{\mu}), \\ \dot{\hat{\mu}} & = \psi(\hat{\mu}, h(x), h(\hat{x}), \hat{x}, t), \end{cases} \tag{3.11}$$

where $x, \hat{x} \in \mathbb{R}^n, \mu \in \mathbb{R}^m$, then the synchronization is said to be *antiadaptive secure* with respect to the parameter μ.

If there exists a positive constant K such that

$$\underline{\lim}_{t\to\infty}\|x(t) - \tilde{x}(t)\| \geq K(\bar{\mu} - \tilde{\mu}),$$

where $\bar{\mu}$ and $\tilde{\mu}$ are chosen from a compact set and substituted into system (3.9) and (3.10), respectively, then the synchronization is said to be *antirobust secure* with respect to the parameter μ.

If the synchronization is both antiadaptive and antirobust secure, then the synchronization is said to be *secure synchronization*.

To motivate the definition, some cases are listed where the synchronization is not secure.

Proposition 3.2 [24]**:** Suppose system (3.9) with output has the form

$$\begin{cases} \dot{x} & = A(y,t)x + \varphi(y,t) + B\Phi(y,t)[\alpha_1(\mu), \dots, \alpha_k(\mu)]^T, \\ y & = h(x) = Cx, \end{cases} \tag{3.12}$$

where $x \in \mathbb{R}^n, y \in \mathbb{R}^p, \mu \in \mathbb{R}^s, A(y,t), B, C$ and $\Psi(x)$ are known matrices with appropriate dimensions. In addition, A and Φ are matrices with uniformly Lipschitz entries. If there exist matrices L and R, a positive definite symmetric matrix S, and a real number T such that the following condition holds,

$$S(A(y,t) + LC) + (A(y,t) + LC)^T S = Q < 0, \quad SB = C^T R, \tag{3.13}$$

then system (3.12) has the following adaptive observer,

$$\begin{cases} \dot{\hat{x}} & = A(y,t)\hat{x} + LC(\hat{x} - x) + \varphi(y,t) + B\Phi(y,t)\hat{p}, \\ \hat{p} & = \Phi^T(y,t)R^T C(x - \hat{x}). \end{cases} \tag{3.14}$$

Proposition 3.2 implies that the synchronization between (3.12) and (3.14) is not antiadaptive secure. Rank$B \leq$ Rank$C$ is a necessary condition for (3.13).

Corollary 3.3 [24]: *Antisecure synchronization with password decryption.* If the conditions of Proposition 3.2 and the following condition holds,

$$\int_t^{t+T} \Phi^T(y,\tau)B^T B\Phi(y,\tau)d\tau \geq KI_{k\times k} > 0, \quad \text{for all } t \geq t_0,$$

where T and K are two positive real constants, then $\hat{p} \to p := [\alpha_1(\mu), \ldots, \alpha_k(\mu)]^T$ when $t \to \infty$.

The above results shows that some known chaotic systems, such as Chua's circuit and Lur's system, may not be good candidates for secure synchronization. For example, it has been shown in [10] that the well-known Chua's circuit can be adaptively synchronized based on the idea described in Proposition 3.2. Reference [24] claims that a good candidate should have some components that are detectable but not observable. Hence the generalized Lorenz system is suggested for secure synchronization in [24].

The following generalized Lorenz system is defined in [54]:

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + \begin{bmatrix} 0 \\ -x_1x_3 \\ x_1x_2 \end{bmatrix}, \quad A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \tag{3.15}$$

where $x = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix}^T$, $\lambda_3 \in \mathbb{R}$, and A has eigenvalues $\lambda_1,\ \lambda_2 \in R$ such that

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{3.16}$$

Moreover, the generalized Lorenz system is said to be *nontrivial* if it has at least one bounded solution that goes neither to zero nor to a limit cycle.

Reference [54] shows that there exists a nonlinear change of coordinates, $z = Tx$, which transforms (3.15) into the generalized Lorenz canonical form:

$$\dot{z} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} z + cz \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \tau & 0 \end{bmatrix} z, \tag{3.17}$$

where $z = \begin{bmatrix} z_1 & z_2 & z_3 \end{bmatrix}^T$, $c = \begin{bmatrix} 1 & -1 & 0 \end{bmatrix}$ and the parameter $\tau \in (-1, \infty)$. System (3.17) is state equivalent to the following form (see [24]

$$\frac{d\eta}{dt} = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 + \eta_2 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - \frac{1}{2}(\tau + 1)\eta_1^3 \\ \lambda_3\eta_3 + K_1(\tau)\eta_1^2 \end{bmatrix}, \tag{3.18}$$

where $\eta = \begin{bmatrix} \eta_1 & \eta_2 & \eta_3 \end{bmatrix}^T$ and $K_1(\tau) = \dfrac{\lambda_3(\tau+1) - 2\tau\lambda_1 - 2\lambda_2}{2(\lambda_1 - \lambda_2)}$. The corresponding coordinate change and its inverse are [24]

$$\eta^T = \begin{bmatrix} z_1 - z_2 & \lambda_1 z_2 - \lambda_2 z_1 & z_3 - \dfrac{(\tau+1)(z_1-z_2)^2}{2(\lambda_1-\lambda_2)} \end{bmatrix}, \tag{3.19}$$

$$z^T = \begin{bmatrix} \dfrac{\lambda_1\eta_1+\eta_2}{\lambda_1-\lambda_2} & \dfrac{\lambda_2\eta_1+\eta_2}{\lambda_1-\lambda_2} & \eta_3 + \dfrac{(\tau+1)\eta_1^2}{2(\lambda_1-\lambda_2)} \end{bmatrix}. \tag{3.20}$$

Consider system (3.18) with the output $\eta_1(t)$ and its uniformly bounded trajectory $\eta(t)$, $t \geq t_0$, there exists an exponential observer for system (3.18) (Theorem 3.4 in [24],

$$\frac{d\hat{\eta}}{dt} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} \lambda_1+\lambda_2-l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \eta_1 + \begin{bmatrix} 0 \\ -(\lambda_1-\lambda_2)\eta_1\hat{\eta}_3 - \dfrac{1+\tau}{2}\eta_1^3 \\ K_1(\tau)\eta_1^2 \end{bmatrix}, \tag{3.21}$$

where l_1 and l_2 are negative real numbers.

Proposition 3.4 [24]: Consider system (3.18) with $\tau = \tau_{mast}$ and system (3.21) with $\tau = \tau_{sl}$, for sufficiently small $|\tau_{mast} - \tau_{sl}|$, the following inequality holds,

$$\overline{\lim}_{t\to\infty}|\hat{\eta}_i(t) - \eta_i(t)| \leq C_i^{up}(l_1,l_2)|\tau_{mast}-\tau_{sl}|, \quad i = 1,2,3,$$

where $C_i^{up}(l_1,l_2) > 0$, $i = 1,2$, are some parameters converging to zero if $(1/2)(l_1 \pm \sqrt[2]{l_1^2+4l_2}) \to -\infty$, while $C_3^{up}(l_1,l_2) > 0$ does not depend on $l_{1,2}$. For all values of $l_{1,2}$, it holds that

$$\frac{d(\eta_3-\hat{\eta}_3)}{dt} = \lambda_3(\eta_3-\hat{\eta}_3) + K_1(\tau_{mast}-\tau_{sl})\eta_1^2.$$

From Definition 2 and Proposition 3.4, antirobust security is obtained. Moreover, Proposition 3.2 is not applicable to system (3.18) because the second equality in (3.13) does not hold. Hence these properties exclude plenty of possible attacks, although they cannot provide full-scale security. Based on the above analysis, the following conjecture is formulated (Conjecture 3.9 in [24]):

Conjencture 3.5: The generalized Lorenz system allows secure synchronization.

3.5 Adaptive synchronization for generalized Lorenz system

3.5.1 Dynamical properties of generalized Lorenz system

This subsection focuses on investigating some dynamical properties of the following system

$$\frac{d\eta}{dt} = \begin{bmatrix} (\lambda_1+\lambda_2)\eta_1+\eta_2 \\ -\lambda_1\lambda_2\eta_1-(\lambda_1-\lambda_2)\eta_1\eta_3-\frac{1}{2}(\tau+1)\eta_1^3 \\ \lambda_3\eta_3+K_1(\tau)\eta_1^2 \end{bmatrix}, \tag{3.22}$$

where $\eta = \begin{bmatrix}\eta_1 & \eta_2 & \eta_3\end{bmatrix}^T$ and $K_1(\tau) = \dfrac{\lambda_3(\tau+1)-2\tau\lambda_1-2\lambda_2}{2(\lambda_1-\lambda_2)}$. From equation (3.22) and equation (3.17) it is easy to get an equivalent system

$$\begin{cases} \dot{\eta}_1 &= \lambda_1\eta_1+(\lambda_1-\lambda_2)z_2, \\ \dot{z}_2 &= \lambda_2 z_2-\eta_1 z_3, \\ \dot{z}_3 &= \lambda_3 z_3+\eta_1^2+(1+\tau)\eta_1 z_2. \end{cases} \tag{3.23}$$

The following assumption is needed in later text:

Assumption 1: The states of system (3.22) and their time derivatives are continuous and bounded.

Remark 2: The proofs of the boundness of Lorenz type systems are reported in [55] and [56]. As for some specific types of chaotic systems, the corresponding proof is given only for some special parameter region [57]. Therefore the above boundness hypotheses in Assumption 1 are reasonable. It is also helpful to note that, under Assumption 1, $\eta_1(t)$ is uniformly continuous by applying the Mean Value Theorem.

For the parameter τ, [54] shows that the region $\tau < -\frac{\lambda_2}{\lambda_1}$ is need to be considered since (3.16) must be met. Therefore this section consider the region $\tau < -\frac{\lambda_2}{\lambda_1}$ from now on.

System (3.23) has three equilibria $O_0(0,0,0)$ and

$$O_{1,2}(\mp\sqrt{\frac{\lambda_1\lambda_2\lambda_3}{(\lambda_2+\lambda_1\tau)}}, \pm\frac{\lambda_1}{\lambda_1-\lambda_2}\sqrt{\frac{\lambda_1\lambda_2\lambda_3}{(\lambda_2+\lambda_1\tau)}}, \frac{\lambda_1\lambda_2}{\lambda_2-\lambda_1})$$

Obviously, O_0 is unstable. The characteristic polynomial for $O_{1,2}$ is

$$\lambda^3-(\lambda_1+\lambda_2+\lambda_3)\lambda^2+\frac{\lambda_3(\lambda_2^2+\tau\lambda_1^2)}{\lambda_2+\lambda_1\tau}\lambda+2\lambda_1\lambda_2\lambda_3=0.$$

It is possible to make O_1 and O_2 both stable or unstable, for example, they are stable when $\tau<\tau_0$, while unstable when $\tau>\tau_0$, where $\tau_0=-\frac{\lambda_2^2}{\lambda_1^2}\frac{(\lambda_1+\lambda_2+\lambda_3)+2\lambda_1}{(\lambda_1+\lambda_2+\lambda_3)+2\lambda_1}$. Therefore the following assumption is made:
Assumption 2: System (3.22) has three unstable equilibria.

Suppose system (3.22) is chaotic, then it satisfies the following obvious properties which will be used in the proofs of some lemmas:
• at least one solution of the system does not go to zero, or to infinity, or to a limit cycle;
• for any finite $T<\infty$, it is impossible that the derivatives of any state variable of system (3.22) keeps its signs, i.e., neither $\dot{\eta}_i(t)>0$ for $t\geq T$, nor $\dot{\eta}_i(t)<0$ for $t\geq T$, $i=1,2,3$ (see [56] and [57];
• the states $\eta_i(t)$ are not always zero on any interval (α,β), that is, $\eta_i(t)\not\equiv 0$ on any (α,β), $i=1,2,3$ [56] and [57].

Lemma 3.6: For system (3.22), there exists a time t_1 such that $\eta_3(t_1)>0(<0)$ for $t\geq t_1$ if $K_1(\tau)>0(<0)$.
Proof: Conversely, for any $t_1>0$, there exists $t'>t_1$ such that $\eta_3(t')<0(>0)$ and $\dot{\eta}_3(t')=0$ if $K_1(\tau)>0(<0)$. Now $\lambda_3\eta_3(t')>0(<0)$, which contradicts the fact that $\lambda_3\eta_3(t')=-K_1(\tau)\eta_1^2(t')<0(>0)$. This ends the proof. □

The following Lemma 3.7 follows in a similar way as Lemma 4 of [56] or Lemma 1 of [57].

Lemma 3.7: Assume $\dot{\eta}_1(t)\not\equiv 0$ for $t\in(-\infty,+\infty)$. If there exists β such that $\dot{\eta}_1(\beta)=\ddot{\eta}_1(\beta)=0$, then $t=\beta$ is not an extreme value point of $\eta_1(t)$.

Let

$$\dot{F}=-aF+aF^2-be^{-dt}, \tag{3.24}$$

where $a<0,\ b>0,\ d>0$, the initial value $F(0)\in(\frac{1}{2},1)$ and $\dot{F}(0)<0$. Its solution is [58]

$$F(t)=-e^{-\frac{1}{2}dt}\frac{\sqrt{-ab}}{a}\frac{J_{v+1}(x)+C_1Y_{v+1}(x)}{J_v(x)+C_1Y_v(x)},\ \text{where } v=-\frac{a}{d},\ x=2\frac{\sqrt{-ab}e^{-1/2\,dt}}{d}, \tag{3.25}$$

C_1 is determined by $F(0)$, $J_v(x)$ and $Y_v(x)$ are the first and second kind of Bessel function respectively, and are defined by the formulas:

$$J_v(x) = (\frac{x}{2})^v \sum_{k=0}^{\infty} \frac{(-1)^k(\frac{x}{2})^{2k}}{k!\Gamma(v+k+1)}, \qquad Y_v(x) = \frac{J_v(x)\cos\pi v - J_{-v}(x)}{\sin\pi v}, \tag{3.26}$$

with $\Gamma(x)$ the Gamma function. The formula for $Y_v(x)$ is valid for $v \neq 0, \pm1, \pm2, \ldots$. For a nonnegative integer n,

$$\begin{aligned} Y_n(x) = \frac{2}{\pi}J_n(x)\lg\frac{x}{2} - \frac{1}{\pi}\sum_{k=0}^{n-1}\frac{(n-k-1)!}{k!}\left(\frac{2}{x}\right)^{n-2k} \\ -\frac{1}{\pi}\sum_{k=0}^{\infty}(-1)^k\left(\frac{2}{x}\right)^{n+2k}\frac{\psi(k+1)+\psi(n+k+1)}{k!(n+k)!}, \end{aligned} \tag{3.27}$$

where $\psi(1) = -\mathcal{C}$, $\psi(n) = -\mathcal{C} + \sum_{k=1}^{n-1} k^{-1}$, $-\mathcal{C}$ is the Euler constant [59].

Lemma 3.8: Suppose $F(t) > 0$ for $t \geq 0$ and b is bounded in equation (3.24), then there exists $t_1 > 0$ independent of b such that $F(t_1) = F(0)$.

Proof: It is easy to know that $F(t) < 1$ for all $t > 0$. In fact, let $t_1 \in (0\ \ +\infty)$ be the first point such that $F(t_1) = 1$, then $\dot{F}(t_1) < 0$. This is impossible since $F(0) < 1$. Let $x = 2\frac{\sqrt{-ab}e^{-1/2\,dt}}{d}$, then x tends to zero when t is sufficiently large. Now $J_v(x)$ tends to zero and $J_{-v}(x)$ tends to infinite since $v > 0$. If v is not an integer,

$$\begin{aligned} \lim_{t\to\infty} F(t) &= \lim_{t\to\infty} -e^{-\frac{1}{2}dt}\frac{\sqrt{-ab}(\frac{x}{2})^{-(v+1)}}{a\sin(\pi(v+1))\Gamma(-v)}\frac{\sin(\pi v)\Gamma(-v+1)}{(\frac{x}{2})^{-v}} \\ &= \lim_{t\to\infty} -e^{-\frac{1}{2}dt}\frac{\sqrt{-ab}}{a}(-\frac{a}{d})\frac{2d}{2\sqrt{-ab}e^{-1/2\,dt}} = 1. \end{aligned}$$

Now the result follows from the fact that $F(0) \in (\frac{1}{2}, 1)$. The case that v is an integer follows from a similar proof. □

Theorem 3.9: Suppose system (3.22) is chaotic, then there exists a finite time Δt so that $\eta_1(t)$ has at least one extremum in the interval $(t_0,\ t_0 + \Delta t)$ for any $t_0 \geq 0$.

Proof: Conversely, for any increasing sequence $\{\Delta t_i\}_1^\infty$ with $\lim_{i\to\infty}\Delta t_i = +\infty$, there exists a sequence $\{t_i\}_1^\infty$ such that η_1 has no extreme on (t_i, T_i), where $T_i := t_i + \Delta t_i$. Note that $\eta_1(t)$ is monotonic on $[t_i,\ T_i]$, then without loss of generality one can suppose $\{t_i\}_1^\infty$ is increasing, $\lim_{i\to\infty} t_i = +\infty$, $\eta_1(t_i)$ is a minimum, and $\eta_1(T_i)$ a maximum. Since system (3.22) and system (3.23) are state equivalent, system (3.23) is considered for convenience. Now there are the following two cases.

Case I: $\eta_1(t_i) - \eta_1(T_i)$ tends to zero when $i \to \infty$.

Since $\eta_1(t_i)-\eta_1(T_i)$ tends to zero when $i \to \infty$, one can suppose $\eta_1(T_i)-\eta_1(t_i) < \epsilon_i$, where ϵ_i is positive and tends to zero when $i \to \infty$. By Assumption 1 one knows that $\dot{\eta}_1(t) < M_1\epsilon_i$ holds for all $t \in (t_i\ T_i)$, where M_1 is a positive constant. Then $|z_2(T_i)-z_2(t_i)| < M_3\epsilon_i$ by equation (3.23). Similarly it follows that both $\dot{z}_2(t)$ and $\dot{z}_3(t)$ tend to zero for $t \in (t_i\ T_i)$ when i tends to infinity. Thus $(\eta_1(T_i), z_2(T_i), z_3(T_i))$ tends to one of the three equilibria. In the following only the case that $(\eta_1(T_i), z_2(T_i), z_3(T_i))$ tends to O_0 is considered. For the other cases, it can be proved in a similar way after a coordinate change $(\eta_1, z_2, z_3) - O_{1,2}$. There are three subcases:

I.I) If $\eta_1(T_i) = 0$, then $\dot{\eta}_2(T_i) = 0$. Hence $\ddot{\eta}_1(T_i) = 0$, and it contradicts Lemma 3.7 since $\eta_1(T_i)$ is a maximum.

I.II) If $\eta_1(T_i) > 0$, then $\dot{\eta}_1(T_i) = 0$ and $\ddot{\eta}_1(T_i) = (\lambda_1 - \lambda_2)\dot{z}_2(T_i) < 0$. Thus $\dot{z}_2(T_i) < 0$ for $\lambda_1 - \lambda_2 > 0$. However, by equation (3.23) one knows that $z_3(T_i)$ becomes sufficiently small when Δt_i becomes sufficiently large, therefore $z_2(T_i) = -\frac{\lambda_1}{\lambda_1-\lambda_2}\eta_1(T_i)$ and $\dot{z}_2(T_i) = (-\frac{\lambda_1\lambda_2}{\lambda_1-\lambda_2} - z_3)\eta_1(T_i) > 0$. This is a contradiction.

I.III) If $\eta_1(T_i) < 0$ and $K_1(\tau) < 0$, then it follows from Lemma 3.6 that $\eta_3(t_i) < 0$ for sufficiently large i. From equation (3.22) one knows $\dot{\eta}_2(t_i) < \eta_1(-\lambda_1\lambda_2 - (\lambda_1 - \lambda_2)\eta_3 - \frac{1}{2}(\tau+1)\eta_1^2) < 0$. However $\ddot{\eta}_1(t_i) = \dot{\eta}_2(t_i) > 0$ since $\eta_1(t_i)$ is a minimum. It is a contradiction.

I.IV) If $\eta_1(T_i) < 0$ and $K_1(\tau) = 0$, then $\lim_{t\to\infty} \eta_3(t) = 0$, which is impossible since the system is chaotic.

I.V) If $\eta_1(T_i) < 0$ and $K_1(\tau) > 0$, it is obvious that $\eta_1(t_i) < 0$ and $\eta_3(t_i) > 0$. Let $f = \dfrac{z_2}{\eta_1}$, then

$$\dot{f}(t) = af(t) + af^2(t) - z_3(t), \quad f(t_i) = \frac{\lambda_1}{\lambda_2 - \lambda_1}, \tag{3.28}$$

where $a = \lambda_2 - \lambda_1 < 0$. It is easy to obtain $z_2(t_i) > 0$ and $\dot{z}_2(t_i) > 0$ since $\ddot{\eta}_1(t_i) > 0$ and $\dot{\eta}_1(t_i) = 0$. Thus $\dot{f}(t_i) < 0$. If $\dot{\eta}_1(t) = 0$ for some point t, then $f(t) = \frac{\lambda_1}{\lambda_2-\lambda_1}$, that is, $f(t) = f(t_i)$. If it can be proved that there exists an integer N so that the function $y = f(t)$ travels through the line $y = \frac{\lambda_1}{\lambda_2-\lambda_1}$ in the t-y plane for every $i > N$ when $t \in (t_i\ T_i)$, then $\eta_1(t)$ reaches the maximum before $t = T_i$. Now this is proved in the following.

Let $f = -1 + F$, then

$$\dot{F}(t) = -aF(t) + aF^2(t) - z_3(t),\ F(t_i) = \frac{\lambda_2}{\lambda_2 - \lambda_1}. \tag{3.29}$$

From equation (3.22) and transformation (3.20), one knows that for $t \in (t_i\ T_i)$,

$$z_3(t) = \eta_3(t_i)e^{\lambda_3(t-t_i)} + \epsilon(t),$$

where

$$\epsilon(t) = \frac{(\tau+1)}{2(\lambda_1 - \lambda_2)}\eta_1^2(t) + K_1(\tau)e^{\lambda_3(t-t_i)}\int_{t_i}^{t} e^{-\lambda_3(s-t_i)}\eta_1^2(s)ds > 0.$$

It is obtained that the following equations for $F(t)$ and another function $F_1(t)$,

$$\begin{aligned}\dot{F} &= -aF(t) + aF^2(t) - \eta_3(t_i)e^{\lambda_3(t-t_i)} - \epsilon(t),\\ \dot{F}_1 &= -aF_1(t) + aF_1^2(t) - \eta_3(t_i)e^{\lambda_3(t-t_i)}.\end{aligned} \tag{3.30}$$

Let the two equations have the same initial values, that is, $F_1(t_i) = F(t_i) = \frac{\lambda_2}{\lambda_2-\lambda_1}$, then it follows from $\dot{F}(t) < \dot{F}_1(t)$ that $0 < F(t) < F_1(t)$. It follows from (3.30) that

$$\begin{aligned}\dot{F} - \dot{F}_1 &= -a(F(t) - F_1(t)) + a(F^2(t) - F_1^2(t)) - \epsilon(t)\\ &\geq -a(F(t) - F_1(t)) - \epsilon(t).\end{aligned} \tag{3.31}$$

Thus

$$0 > F(t) - F_1(t) > -e^{-a(t-t_i)}\int_{t_i}^{t} e^{as}\epsilon(s)ds,\ \text{for } t \in (t_i\ T_i).$$

Then it follows from Lemma 3.8 that there exists a time $t_{i1} \in (t_i\ T_i)$ independent of $\eta_3(t_i)$ such that $F_1(t_{i1}) = F_1(t_i)$. In a similar way, one can prove that there exists a time $t_{i3} \in (t_{i1}, T_i)$ independent of $\eta_3(t_i)$ such that $F(t_{i3}) = 1/2 + F(t_i)/2 \in (F(t_i), 1)$. Since $\epsilon(t)$ is sufficiently small, there exists a time $t_{i2} \in (t_{i1}, t_{i3})$ such that $F(t_{i2}) = F(t_i)$, that is, there exists a time $t_{i2} < T_i$ for every $i > N$ such that $\eta_1(t_{i2})$ reaches its maximum, where N is a sufficiently large number. This contradicts the hypothesis that $\eta_1(t)$ is monotonic for $t \in (t_i, T_i)$.

By the above four subcases, it concludes that Case I does not happen. Therefore the second case is considered.

Case II: $\eta_1(t_i) - \eta_1(T_i)$ does not tend to zero when $i \to \infty$.

Since Δt_i tends to infinity, one chooses $\Delta t_i \geq 2^{2i}$. Let $\eta_1(t_{m1}) = \frac{1}{2}(\eta_1(T_i) - \eta_1(t_i))$, then either $t_{m1} - t_i$ or $T_i - t_{m1}$ is greater than 2^{2i-1}. Without loss of generality, let $T_i - t_{m1} \geq 2^{2i-1}$. Then there exists a time $t_{m2} \in (t_{m1}, T_i)$ such that $\eta_1(t_{m2}) =$

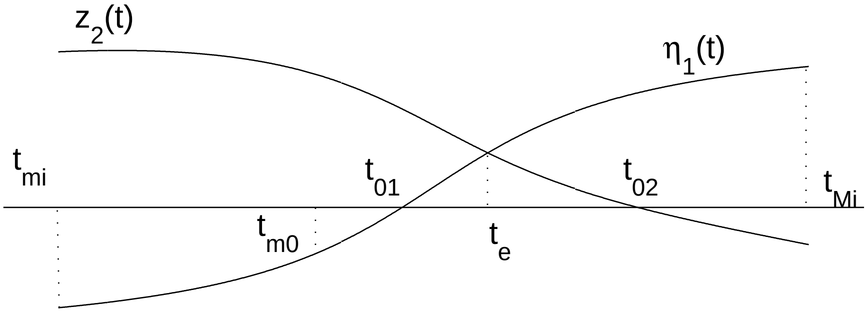


Figure 3.1: Illustration for $\eta_1(t)$ and $z_2(t)$ in Case II.

$(\eta_1(T_i) - \eta_1(t_{m1}))/2$. It is obvious that either $t_{m2} - t_{m1}$ or $T_i - t_{m2}$ is greater than 2^{2i-2}. After repeating the above process for i times, two times t_{mi} and t_{Mi} are obtained such that $\eta_1(t_{Mi}) - \eta_1(t_{mi}) < \frac{1}{2^i}(\eta_1(T_i) - \eta_1(t_i))$ and $t_{Mi} - t_{mi} \geq 2^i$ (see Figure 3.1 for illustration.)

Following the same way in Case I, $\eta_1(t_{Mi})$ and $\eta_1(t_{mi})$ tend to one of the three equilibria. For the same reason as in Case I, only the equilibrium O_0 is considered. From subcase I.I) one knows that $\eta_1(T_i) > 0$. Thus one can suppose that $-\epsilon_i = \eta_1(t_{mi}) < 0 < \eta_1(t_{Mi}) = \epsilon_i$ and $\lim_{i\to\infty}(t_{Mi} - t_{mi}) = +\infty$.

Since $z_2(T_i) < 0$, there exists a time t_{02} such that $z_2(t_{02})$ reaches 0 for the first time. Firstly it is proved that $z_2(t)$ is decreasing on $(t_{mi},\ \min(t_{Mi}, t_{02}))$. Since $\eta_1(t) < \epsilon_i$ for $t \in (t_{mi}, t_{Mi})$, one can assume, without loss of generality, that $|\eta_3(t_{mi})| < \frac{-\lambda_1\lambda_2}{\lambda_1-\lambda_2}$. Let t_{01} be the time at which $\eta_1(t_{01}) = 0$. Then by $\dot{\eta}_1(t_{01}) > 0$ one has $\eta_2(t_{01}) > 0$. It obviously follows from (3.22) that $\dot{\eta}_2(t) < 0$ on (t_{mi}, t_{01}) and $\dot{\eta}_2(t) > 0$ on $(t_{01}\ t_{Mi})$. Now by (3.20) one knows that $\dot{z}_2 = \frac{\lambda_2\dot{\eta}_1+\dot{\eta}_2}{\lambda_1-\lambda_2} < 0$ for $t \in (t_{mi}\ t_{01})$, and $\dot{z}_2 < \frac{\lambda_2}{\lambda_1-\lambda_2}(\lambda_2\eta_1 + \eta_2) < 0$ for $t \in (t_{01},\ \min(t_{Mi}, t_{02}))$ for $z_2(t) = \frac{\lambda_2\eta_1+\eta_2}{\lambda_1-\lambda_2} > 0$.

Since $z_2(T_i) < 0$, there exists a time t_e so that $\eta_1(t_e)$ is positive and reaches $z_2(t_e)$ for the first time. Let $\delta = \eta_1(t_e)$, then t_e must be less than t_{Mi}. In fact, if $z_2(t) > \epsilon_i$ on $(t_{mi}\ t_{Mi})$, then $\dot{\eta}_1(t) = \lambda_1\eta_1 + (\lambda_1 - \lambda_2)z_2 > -\lambda_2\epsilon_i$, thus $\eta_1(t_{Mi}) > \epsilon_i$ which contradicts $\eta_1(t_{Mi}) = \epsilon_i$.

Let $g = \dfrac{\eta_1}{z_2}$, after a simple computation one has the following formula from equation (3.23) for $t \in (t_{mi}, t_{01})$

$$\dot{g} = -a - ag + g^2 z_3, \qquad g(t_{01}) = 0. \tag{3.32}$$

If $t_{01} - t_{mi}$ tends to infinity with i, then $z_3(\frac{t_{01}+t_{mi}}{2})$ and $\eta_3(\frac{t_{01}+t_{mi}}{2})$ are sufficiently small on $(t_{mi}\ t_{01})$. Since $g(t) < 0$ for $t \in (t_{mi}, t_{01})$ and $g(t_{01}) = 0$, there exists a time $t_{m0} \in (\frac{t_{01}+t_{mi}}{2}, t_{01})$ such that $g(t_{m0}) = -\frac{1}{2}$, that is, $\frac{\eta_1}{z_2}(t_{m0}) = -\frac{1}{2}$. Hence, by equation (3.23), $\dot{\eta}_1(t_{m0}) = (2\lambda_2 - \lambda_1)\eta_1$ and $\dot{z}_2(t_{m0}) = (2\lambda_2 - z_3)\eta_1$. By coordinate change (3.20), one knows $\dot{\eta}_2(t_{m0}) = (-4\lambda_2^2 + 3\lambda_1\lambda_2 - z_3(\lambda_1 - \lambda_2))\eta_1 > 0$; however equation (3.22) gives $\dot{\eta}_2(t_{m0}) = (-\lambda_1\lambda_2 - (\lambda_1 - \lambda_2)\eta_3 - \frac{1}{2}(1+\tau)\eta_1^2)\eta_1 < 0$, which is a contradiction. Hence $\{t_{01} - t_{mi} : i = 1, 2, \cdots\}$ is bounded.

Since $t_{01} - t_{mi}$ is a finite time independent of i and $t_{Mi} - t_{mi}$ tends to infinity , $t_{Mi} - t_{01}$ tends to infinity too. It is assumed that $|z_3(t_{mi})| < -\frac{\lambda_1\lambda_2}{2(\lambda_1-\lambda_2)}$ by the same reason of the boundedness of $|\eta_3(t_{mi})|$. It follows from equation (3.28) that $f(t)$ becomes small enough after a long time. Hence $\dot{\eta}_1(t) > \frac{\lambda_1}{2}\eta_1(t)$ for $t \in (\frac{t_{mi}+t_{Mi}}{2}, t_{Mi})$. Then it follows from $\dot{\eta}_1(t_{mi}) > 0$ that $z_2(t_{mi}) > \frac{\lambda_1}{\lambda_1-\lambda_2}\epsilon_i$. Now one obtains $|\eta_1(t)| < \frac{\lambda_1-\lambda_2}{\lambda_1}z_2$ for $t \in (t_{mi}\ t_{01})$ because $\dot{\eta}_1(t) = \lambda_1\eta_1(t) + (\lambda_1 - \lambda_2)z_2(t) > 0$. From equation (3.23) it follows that

$$\dot{z}_2(t) = \lambda_2 z_2(t) - \eta_1(t)z_3(t) > \lambda_2 z_2(t) + \frac{\lambda_2}{2}z_2(t) = \frac{3}{2}\lambda_2 z_2(t).$$

Thus

$$z_2(t_{01}) > e^{\frac{3}{2}\lambda_2(t_{01}-t_{mi})}z_2(t_{mi}).$$

Similarly one has

$$\delta = z_2(t_e) > e^{\frac{3}{2}\lambda_2(t_e-t_{01})}z_2(t_{01}) - \delta M, \text{ where } M \text{ is a positive constant,}$$
$$\Longrightarrow \delta > \frac{1}{1+M}e^{\frac{3}{2}\lambda_2(t_e-t_{01})}z_2(t_{01}) > \frac{1}{1+M}\frac{\lambda_1}{\lambda_1-\lambda_2}e^{\frac{3}{2}\lambda_2(t_e-t_{mi})}z_2(t_{01})\epsilon_i.$$

Since $\dot{\eta}_1 > \frac{\lambda_1}{2}\eta_1$, one has

$$\eta_1(t_{Mi}) > e^{\frac{\lambda_1}{2}\frac{t_{Mi}-t_{mi}}{2}}\eta_1(t_{mi} + \frac{t_{Mi}-t_{mi}}{2}) > e^{\frac{\lambda_1}{2}\frac{t_{Mi}-t_{mi}}{2}}\delta > \epsilon_i,$$

which contradicts $\eta_1(t_{Mi}) = \epsilon_i$. □

3.5.2 Adaptive synchronization with PE condition

Consider system (3.22) with the output $y = \eta_1(t)$; it can be rewritten as a state affine form,

$$\begin{aligned}\frac{d\eta}{dt} &= \begin{bmatrix} (\lambda_1+\lambda_2) & 1 & 0 \\ -\lambda_1\lambda_2 & 0 & -(\lambda_1-\lambda_2)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix} + \begin{bmatrix} 0 \\ -\frac{1}{2}\eta_1^3 \\ \frac{\lambda_3-2\lambda_2}{2(\lambda_1-\lambda_2)}\eta_1^2 \end{bmatrix} + \begin{bmatrix} 0 \\ -\frac{1}{2}\eta_1^3 \\ \frac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}\eta_1^2 \end{bmatrix}\tau \\ &= A(y)\eta + \varphi(y) + \Phi(y)\tau, \\ y &= C\eta(t) = \eta_1(t), \end{aligned}$$

where

$$A(y) = \begin{bmatrix} (\lambda_1+\lambda_2) & 1 & 0 \\ -\lambda_1\lambda_2 & 0 & -(\lambda_1-\lambda_2)y \\ 0 & 0 & \lambda_3 \end{bmatrix}, \quad \varphi(y) = \begin{bmatrix} 0 \\ -\frac{1}{2}y_1^3 \\ \frac{\lambda_3-2\lambda_2}{2(\lambda_1-\lambda_2)}y_1^2 \end{bmatrix},$$

$$\Phi(y) = \begin{bmatrix} 0 \\ -\frac{1}{2}y_1^3 \\ \frac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}y_1^2 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}.$$

Let

$$K(t) = \begin{bmatrix} \lambda_1+\lambda_2-l_1 \\ -\lambda_1\lambda_2-l_2 \\ 0 \end{bmatrix},$$

by (3.3) and (3.4), the following adaptive observer is constructed for system (3.22):

$$\begin{aligned}\frac{d\hat{\eta}}{dt} &= \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2-\lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix}\hat{\eta} + \begin{bmatrix} \lambda_1+\lambda_2-l_1 \\ -\lambda_1\lambda_2-l_2 \\ 0 \end{bmatrix}\eta_1 + \begin{bmatrix} 0 \\ -\frac{1}{2}\eta_1^3 \\ \frac{\lambda_3-2\lambda_2}{2(\lambda_1-\lambda_2)}\eta_1^2 \end{bmatrix} + \begin{bmatrix} 0 \\ -\frac{1}{2}\eta_1^3 \\ \frac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}\eta_1^2 \end{bmatrix}\hat{\tau} + \Upsilon(t)\dot{\hat{\tau}}, \\ \dot{\hat{\tau}}(t) &= \Upsilon^T(t)C^T(t)[\eta_1(t) - C(t)\hat{\eta}(t)], \\ \dot{\Upsilon}(t) &= \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2-\lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix}\Upsilon(t) + \begin{bmatrix} 0 \\ -\frac{1}{2}\eta_1^3 \\ \dfrac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}\eta_1^2 \end{bmatrix}, \end{aligned} \tag{3.33}$$

where $l_i < 0,\ i = 1, 2$. Synchronization between (3.22) and (3.33) is achieved if $\lim_{t\to\infty} |\eta(t) - \hat{\eta}(t)| = 0$, that is, the above observer is an asymptotically stable observer for system (3.22). As mentioned in Section 3.3, the observer is asymptotically stable under Condition 1 and 2. Condition 1 is proved in [24]. The difficulty is to prove that Condition 2 holds, that is $\Upsilon_1(t)$ is PE. In order to prove Condition 2, it needs some properties of $\eta_1(t)$ and PE conditions.

Lemma 3.10: Suppose that system (3.22) is nontrivial and there exists a finite time Δt so that $\eta_1(t)$ has at least one extremum in the interval $(t_0,\ t_0+\Delta t)$ for any $t_0 \geq 0$, then $\eta_1(t)$ is PE.

Proof: For any $t_0 > 0$, if there exist a positive constant $\alpha > 0$, a finite time Δt_0, and a time t' in $[t_0,\ t_0+\Delta t_0]$ such that $|\eta_1(t')| > \alpha$, and α and Δt_0 are independent of time t_0, then there exists $\delta > 0$ independent of time t_0 such that $|\eta_1(t)| \geq \frac{\alpha}{2}$ for all $t \in [t'-\delta,\ t'+\delta] \subset [t_0,\ t_0+\Delta t]$ since the derivation of $\eta_1(t)$ is bounded according to Assumption 1. Hence the PE condition (3.1) is satisfied. If the above α and Δt_0 do not exist, then for any positive integer i and $\frac{M}{2^i}$, and any increasing sequence $\{\Delta t_i\}$ with $\Delta t_1 > 4\Delta t$ and $\lim_{i\to\infty}\Delta t_i = +\infty$, there exists a sequence $\{t_i\}$ such that $|\eta_1(t)| < \frac{M}{2^i}$ on $[t_i, T_i]$ for all i, where $M := \sup_{t\geq 0}|\eta_1(t)|$ and $T_i := t_i + \Delta t_i$. Note that $\frac{\Delta t_i}{2} > 2\Delta t$ and η_1 has at least one extremum in the interval $(t_0,\ t_0+\Delta t)$ for any $t_0 \geq 0$, there exists a $t' \in [t_i + \frac{\Delta t_i}{2},\ T_i]$ such that $\eta_1(t')$ is a maximum, therefore one has $\ddot{\eta}_1(t') = (\lambda_1+\lambda_2)\dot{\eta}_1(t') + \dot{\eta}_2(t') = \dot{\eta}_2(t') < 0$. Note also that $|\eta_1| < \frac{M}{2^i}$ on $[t_i, T_i]$ and $\dot{\eta}_3 = \lambda_3\eta_3 + K_1(\tau)\eta_1^2$, therefore, when Δt_i is sufficiently large, $\eta_3(t)$ will become sufficiently small such that $-\lambda_1\lambda_2 - (\lambda_1-\lambda_2)\eta_3(t) - \frac{1}{2}(1+\tau)\eta_1^2(t) > 0$ for all $t \in [t_i + \frac{\Delta t_i}{2},\ T_i]$. If $\eta_1(t') \geq 0$, then by (3.22) one has $\dot{\eta}_2(t') \geq 0$, which contradicts the previously obtained $\dot{\eta}_2(t') < 0$. In case of $\eta_1(t') < 0$, it follows from $\frac{\Delta t_i}{2} > 2\Delta t$ that there must exist a $t'' \in [t_i + \frac{\Delta t_i}{2},\ t')$ or $(t', T_i]$ such that t'' is the nearest minimum point to t'. A similar proof also leads to a contradiction. □

Lemma 3.11 [60, 53]): Let $a > 0$, and the input $u(t)$ be PE in the one-dimensional system $\dot{x} = -ax + u(t)$, then the solution $x(t)$ is also PE.

Remark 3: Lemma 3.11 is a simplified version compared to the original versions in [61, 60, 53].

Lemma 3.12: Let $x(t)$ be a scalar function of time, and suppose $x(t)$ and $\dot{x}(t)$ are continuous and bounded, then $x^2(t)$ is PE if $x(t)$ is PE.

Proof: Since $x(t)$ is PE, there exist $\alpha_1,\ \alpha_2,\ T > 0$ such that

$$\alpha_1 I \leq \int_{t_1}^{t_1+T} x^2(s)\,ds \leq \alpha_2 I, \quad \forall t_1 \geq 0.$$

Then there exists a time $t_2 \in (t_1,\ t_1+T)$ such that $x^2(t_2) \geq \frac{\alpha_1}{T}$. Since $\dot{x}$ is bounded, one has $|x(t')-x(t'')| = |\dot{x}(\xi)||t'-t''| \leq M|t'-t''|$, where $M>0$ and $\xi \in (t',\ t'')$. Thus there exists $\delta > 0$ independent of time t_1 such that $x^2(t) \geq \frac{\alpha_1}{2T}$ for all $t \in [t_2-\delta,\ t_2+\delta]$. Then it is obvious that

$$\int_{t_1}^{t_1+T} x^4 ds \geq \int_{t_2-\delta}^{t_2+\delta} x^4 ds \geq 2\delta(\frac{\alpha_1}{2T})^2. \ \square$$

Now, $\Upsilon(t)$ is rewritten in the following form

$$\dot{\Upsilon}(t) = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \Upsilon(t) + \begin{bmatrix} 0 \\ (\lambda_2-\lambda_1)y\Upsilon_3 - \frac{1}{2}y^3 \\ \dfrac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}y^2 \end{bmatrix}, \tag{3.34}$$

where $y(t)$ is the output of system (3.22), that is, $\eta_1(t)$. Apply the following transformation to (3.34)

$$\zeta = \begin{bmatrix} 1 & 1 & 0 \\ -a_2 & -a_1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \Upsilon = P\Upsilon, \qquad a_1 + a_2 = l_1,\ -a_1 a_2 = l_2, \tag{3.35}$$

then

$$\dot{\zeta} = \begin{bmatrix} a_1 & 0 & 0 \\ 0 & a_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \zeta + \begin{bmatrix} (\lambda_2-\lambda_1)y\Upsilon_3 - \frac{1}{2}y^3 \\ -a_1[(\lambda_2-\lambda_1)y\Upsilon_3 - \frac{1}{2}y^3] \\ \dfrac{\lambda_3-2\lambda_1}{2(\lambda_1-\lambda_2)}y^2 \end{bmatrix}. \tag{3.36}$$

Remark 4: From Lemma 3.11 it is easy to know that $\Upsilon_3(t)$ or $\zeta_3(t)$ is PE since Lemma 3.10 has already proved that $\eta_1(t)$ is PE.

Note that it can make $a_1, a_2 < 0$ by choosing properly l_1 and l_2 in (3.35), therefore it is assumed from now on that $a_1 < 0$ and $a_2 < 0$.

Lemma 3.13: There exist $\alpha_1,\ \alpha_2,\ \Delta t > 0$ such that

$$\alpha_1 I \leq \int_t^{t+\Delta t} \Upsilon_3^2(s)\, ds \leq \alpha_2 I, \qquad \forall t \geq 0$$

and there is at least one local maximum of Υ_3 in $[t,\ t+\Delta t]$.

Proof: Since $\Upsilon_3(t)$ is PE, it always finds appropriate $\alpha_1,\ \alpha_2,\ \Delta t > 0$ such that

$$\alpha_1 I \leq \int_t^{t+\Delta t} \Upsilon_3^2(s)\, ds \leq \alpha_2 I, \qquad \forall t \geq 0.$$

The proof of the lemma is by contradiction. If the result does not hold, then by following the same way as in Theorem 3.9, there exist two increasing sequences $\{t_i\}_1^\infty$ and $\{T_i\}_1^\infty$ such that t_i and $\Delta t_i = T_i - t_i > 0$ tend to infinity, and $\Upsilon_3(t)$ is monotonic on $[t_i,\ t_i + T_i]$. For the same reason in case II of Theorem 3.9, one can assume that $|\Upsilon(T_i) - \Upsilon(t_i)| < \epsilon_i$ where ϵ_i is a sufficiently small positive number when i is sufficiently large. It follows from (3.34) and Assumption 1 that $\Upsilon_3(t)$ and $\dot{\Upsilon}_3(t)$ are bounded, therefore $|\dot{\Upsilon}_3(t)| < M\epsilon_i$ on $(t_i,\ T_i)$, where M is a positive constant. However, by Theorem 3.9 there exist $t_i < t', t'' < T_i$ such that $y^2(t'') - y^2(t') = \theta$, where θ is a positive constant. Let $b = \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} < 0$, then $|\dot{\Upsilon}_3(t'')| = |\lambda_3 \Upsilon(t'') + by^2(t'')| = |\dot{\Upsilon}_3(t') + \lambda_3(\Upsilon(t'') - \Upsilon(t')) + b(y^2(t'') - y^2(t'))| > |b\theta| - (M - \lambda_3)\epsilon_i > M\epsilon_i$ when ϵ_i is sufficiently small. This contradiction ends the proof. □

Lemma 3.14: Let $a = (\lambda_2 - \lambda_1) < 0$, then $f(t) = ay\Upsilon_3(t) - \frac{1}{2}y^3(t)$ is PE.
Proof: Let $b = \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)} < 0$, then it follows from $\dot{\Upsilon}_3(t) = \lambda_3 \Upsilon_3(t) + by^2(t)$ that

$$f(t) = \frac{a}{\lambda_3} y \dot{\Upsilon}_3(t) - \frac{2ab + \lambda_3}{2\lambda_3} y^3 = \frac{a}{\lambda_3} y \dot{\Upsilon}_3(t) - \frac{\lambda_1}{\lambda_3} y^3,$$

and $\Upsilon_3(t) < 0$ from Lemma 3.6. From Lemma 3.13, there exists $t_1 \in (t, t + \Delta t)$ such that $\dot{\Upsilon}_3(t_1) = 0$ and

$$y^2(t_1) = \frac{1}{b}(\dot{\Upsilon}_3(t_1) - \lambda_3 \Upsilon_3(t_1)) \geq \frac{\lambda_3}{b}\sqrt{\frac{\alpha_1}{\Delta t}},$$

where Δt and α_1 are defined in Lemma 3.13. Since $y(t)$ and $\dot{\Upsilon}_3(t)$ are uniformly continuous, there exists $\delta > 0$ independent of time t such that $|a\dot{\Upsilon}_3(t)| < \frac{\lambda_1 \lambda_3}{4b}\sqrt{\frac{\alpha_1}{\Delta t}}$ and $\lambda_1 y^2(t) > \frac{\lambda_1 \lambda_3}{2b}\sqrt{\frac{\alpha_1}{\Delta t}}$ for $t \in [t_1 - \delta, t_1 + \delta]$. Therefore $|f(t)| = |\frac{y}{\lambda_3}(a\dot{\Upsilon}_3(t) - \lambda_1 y^2(t))| > \varepsilon$ for all $t \in [t_1 - \delta, t_1 + \delta] \subset [t, t + \Delta t]$, where ε is a positive constant. Hence

$$\int_t^{t+\Delta t} f^2(s)ds > \int_{t_1-\delta}^{t_1+\delta} f^2(s)ds > 2\varepsilon\delta. \qquad \square$$

Theorem 3.15: Under Assumption 1 and Assumption 2, observer (3.33) is an exponential observer for system (3.22) under the output $y = \eta_1(t)$.
Proof: By the transformation (3.35) one has $\Upsilon_1(t) = \dfrac{1}{a_1 - a_2}(a_1\zeta_1 + \zeta_2)$ and $a_i < 0, i = 1, 2$, thus

$$\dot{\Upsilon}_1 = \frac{(a_1(a_1\zeta_1 + f) + (a_2\zeta_2 - a_1 f))}{a_1 - a_2} = \frac{1}{a_1 - a_2}(a_1^2\zeta_1 + a_2\zeta_2) = a_1\Upsilon_1 - \zeta_2. \qquad (3.37)$$

It follows Lemma 3.14 that $f(t) = (\lambda_2 - \lambda_1)y\Upsilon_3 - \frac{1}{2}y^3$ is PE, then from Lemma 3.11 and equation (3.36) one has $\zeta_2(t)$ is PE. Similarly $\Upsilon_1(t)$ is also PE. As mentioned

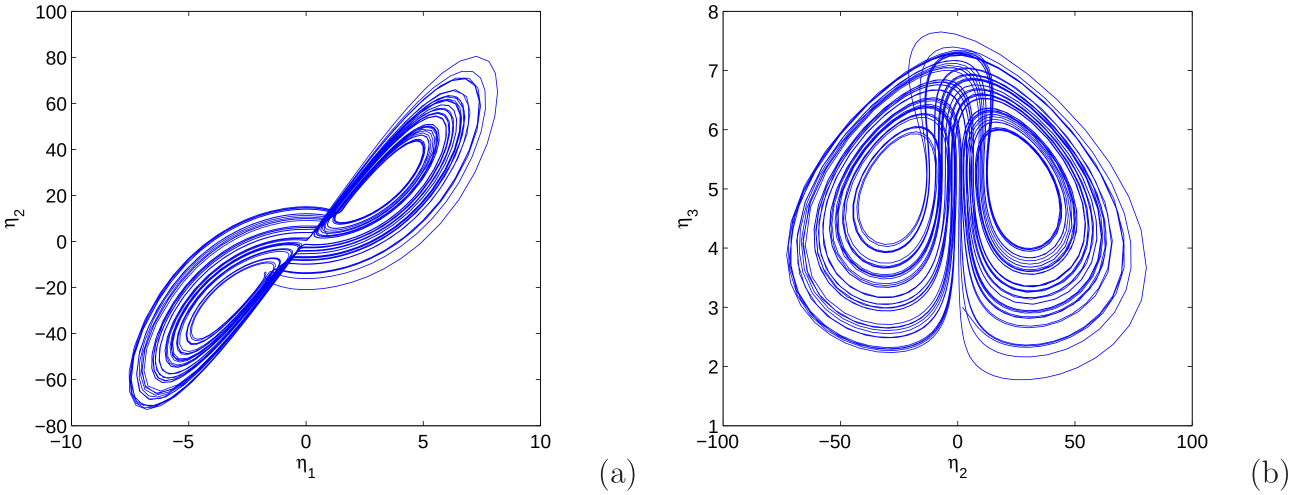


Figure 3.2: Phase plot when $\tau = 0.5$: a)η_1 vs η_2, b) η_2 vs η_3.

above, Condition 1 is proved in [24]. Condition 2 holds from the fact that $\Upsilon_1(t)$ is PE. Theorem 3.1 in [38] shows that observer (3.33) is an exponential observer for system (3.22). □

Remark 5: For system (3.22) with output $\eta_1(t)$, the authors of [24] proved that it cannot achieve synchronization by certain kinds of observer, owing to the unknown parameter τ. Now, without additional conditions, observer (3.33) is proved that it can estimate the states and the unknown parameter at the same time. Hence the conjecture does not hold.

3.5.3 Numerical illustration

In [24], the authors illustrated that system (3.22) cannot be synchronized without knowing the exact τ with the parameters $\lambda_1 = 8, \lambda_2 = -16, \lambda_3 = -1$ and $\tau = 0.5$. Now, selecting $l_1 = -28, l_2 = -180$, numerical simulations show the efficiency of the observer (3.33) with the same parameters. First, one computes the three equilibria and the eigenvalues of the corresponding Jacobian matrices. Obviously, $O_0(0, 0, 0)$ is unstable since $\lambda_1 > 0$. After a simple computation, the other two equilibriums are obtained: $O_1(3.266, 26.128, 5)$ and $O_2(-3.266, 26.128, 5)$. The Jacobian matrices corresponding to O_1 and O_2 have the eigenvalues 15.434 and $-12.217 \pm 10.385i$. Figure 3.2 plots the trajectories of system (3.22), which shows that system (3.22) is chaotic when $\tau = 0.5$.

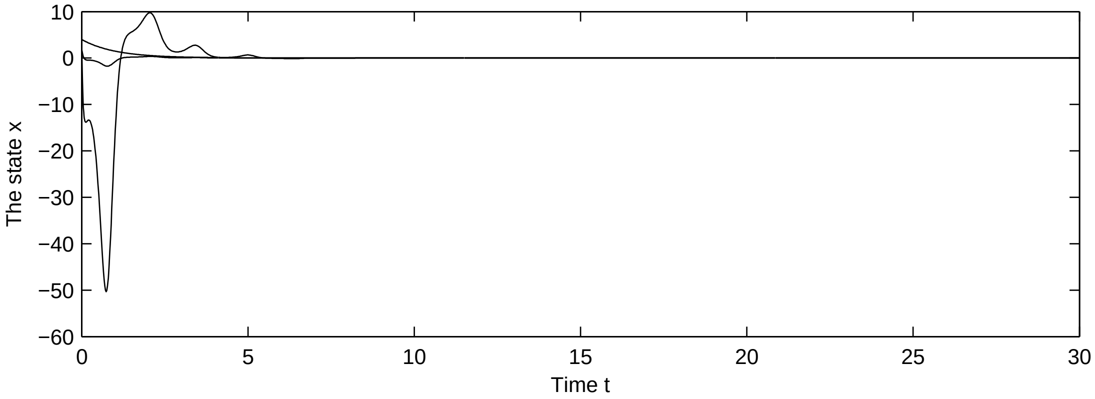


Figure 3.3: The trajectories of system (3.38) when $\tau = 0.5$.

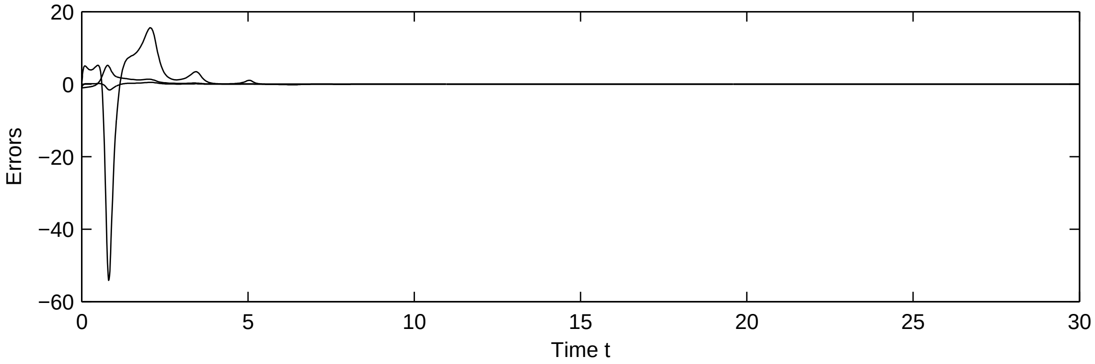


Figure 3.4: The synchronization errors between (3.22) and (3.33) when $\tau = 0.5$.

To test that Condition 1 holds, Figure 3.3 plots the trajectories of the following system:

$$\frac{dx}{dt} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2 - \lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} x, \tag{3.38}$$

where $x = [x_1, x_2, x_3]^T$ and the initial condition is $[2\ 3\ 4]^T$. Obviously, all the trajectories tend to zero quickly, which shows that Condition 1 holds. Figure 3.4 shows the synchronization errors between system (3.22) and (3.33). Figure 3.5 shows that the unknown parameter τ is estimated exactly, which implies that parameter τ cannot be a password. The initial values of system (3.22) and (3.33) are $[1\ 2\ 3]$ and $[2\ 3\ 4\ 3\ 2\ -1\ 2]$, respectively. The two figures show that both the state and the unknown parameter of (3.22) can be estimated.

The other two sets of system parameters are chosen to show the efficiency of the observer (3.33) for system (3.22) with different parameter τ,

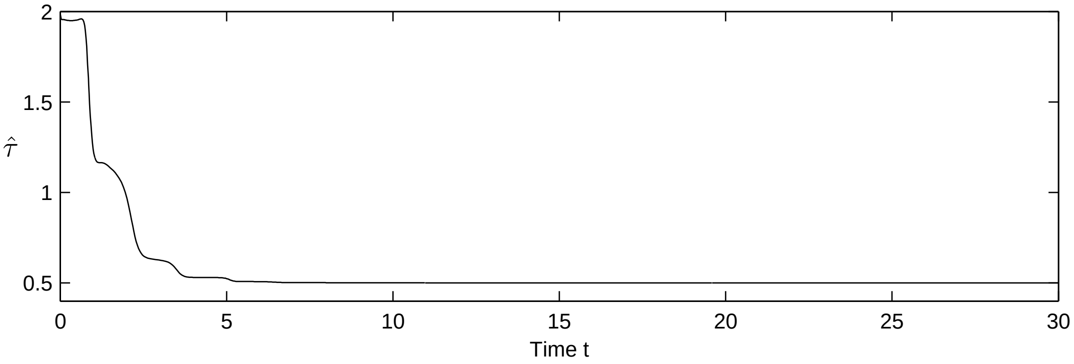


Figure 3.5: The parameter estimation value when $\tau = 0.5$.

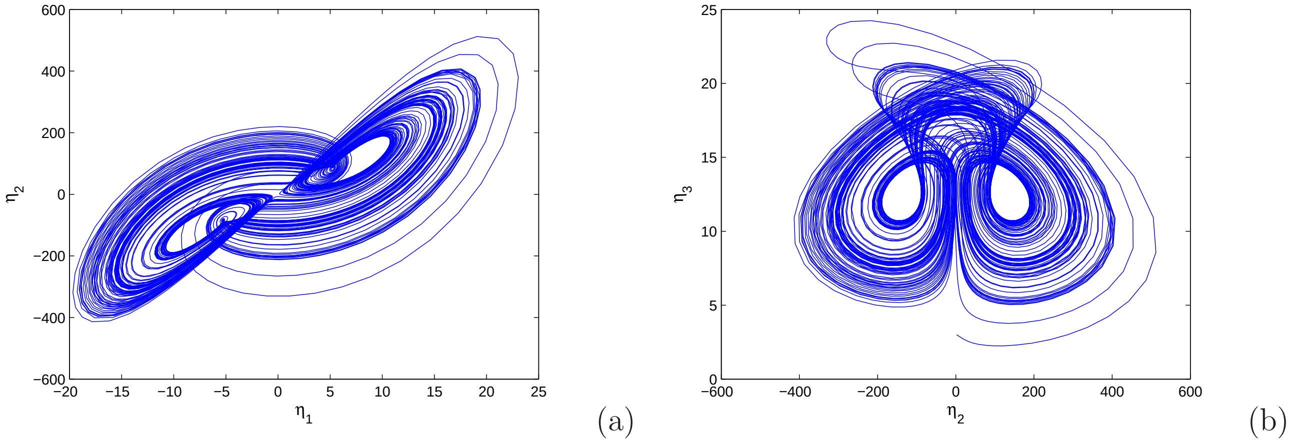


Figure 3.6: Phase plot when $\tau = 0$: a)η_1 vs η_2, b) η_2 vs η_3.

1. $\lambda_1 = 20, \lambda_2 = -36, \lambda_3 = -3$ and $\tau = 0, l_1 = -20, l_2 = -50$;

2. $\lambda_1 = 23.8, \lambda_2 = -30.8, \lambda_3 = -3$ and $\tau = -0.07, l_1 = -20, l_2 = -50$.

The initial conditions are the same as the case $\tau = 0.5$. Figure 3.6 and 3.10 show that system (3.22) is chaotic under these two sets of parameters. As illustrated in Figure 3.7 and 3.11, Condition 1 still holds. The synchronization between system (3.22) and (3.33) is achieved as shown in Figure 3.8 and 3.12. Figure 3.9 and 3.13 show that the unknown parameter τ is estimated exactly. These four figures, Figure 3.8, 3.9, 3.12 and 3.13, show that the adaptive observer (3.33) successfully estimates the state and parameter τ simultaneously.

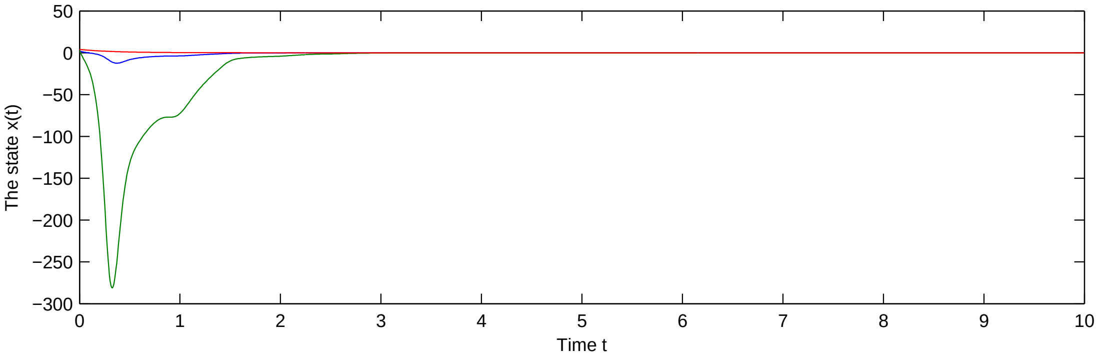


Figure 3.7: The trajectories of system (3.38) when $\tau = 0$.

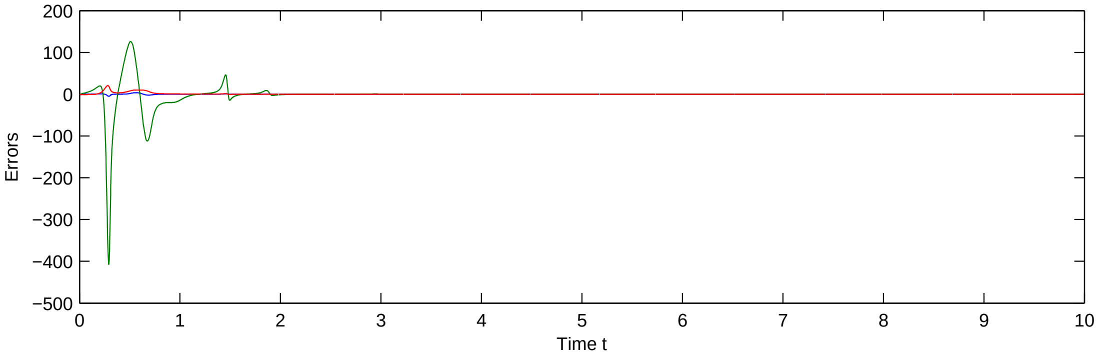


Figure 3.8: The synchronization errors between (3.22) and (3.33) when $\tau = 0$.

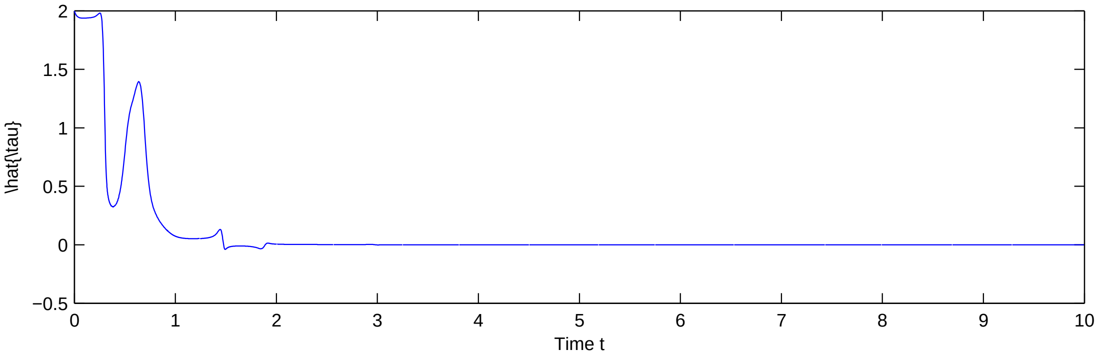


Figure 3.9: The parameter estimation value when $\tau = 0$.

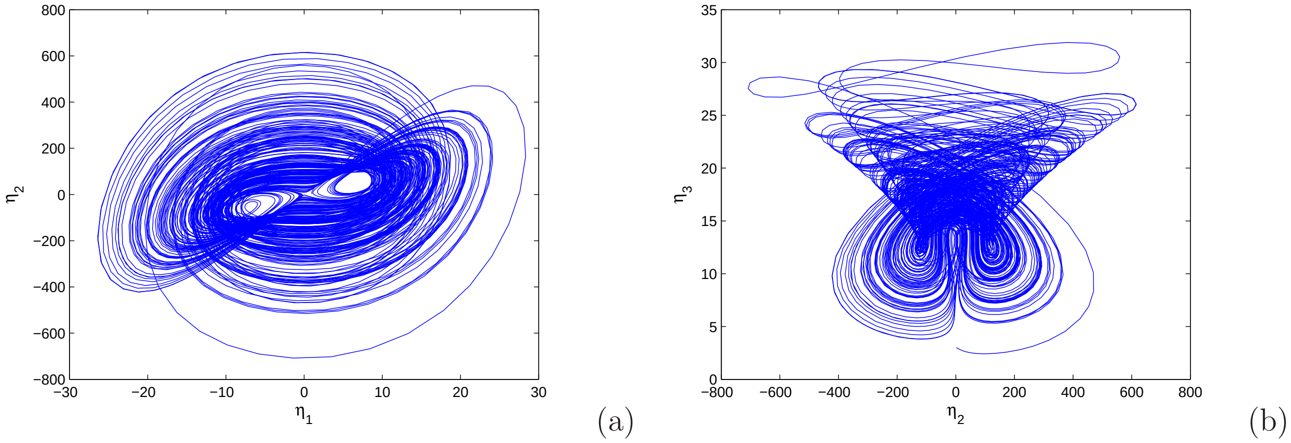


Figure 3.10: Phase plot when $\tau = 0.07$: a)η_1 vs η_2, b) η_2 vs η_3.

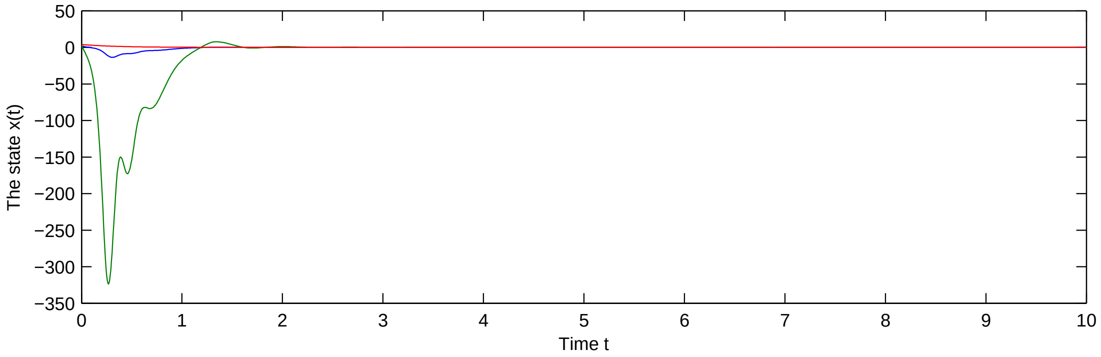


Figure 3.11: The trajectories of system (3.38) when $\tau = 0.07$.

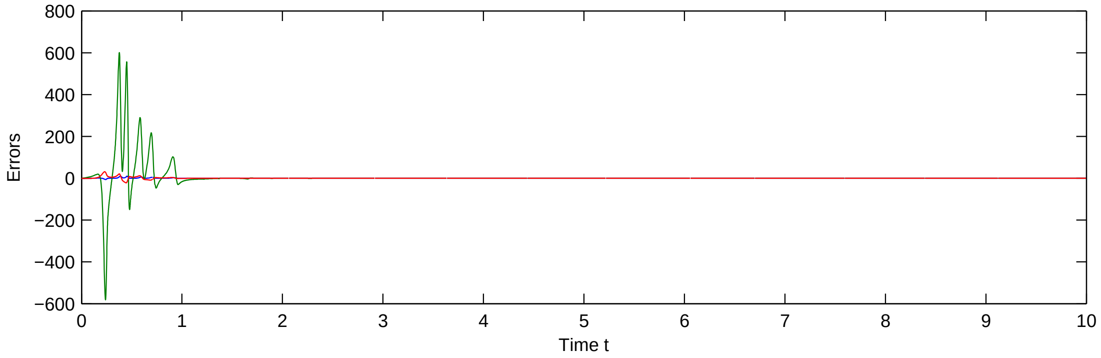


Figure 3.12: The synchronization errors between (3.22) and (3.33) when $\tau = 0.07$.

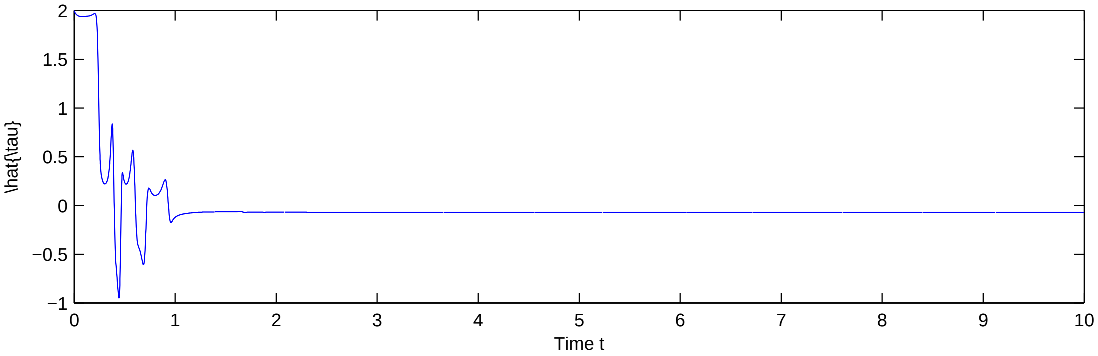


Figure 3.13: The parameter estimation value when $\tau = 0.07$.

3.6 On the application of parameter identifiability to the security of chaotic synchronization

As mentioned in Chapter 2, a fundamental assumption of all kinds of cryptosystems, as first stated by A. Kerckhoff [62], is:

- public structure: an opponent knows the structure of the encryption system and the a priori probability of the key that is used. This requirement is referred to as Kerckhoff's principle.

Kerckhoff's principle means that the intruder knows the details of the cryptosystems, including the design and the implementation, except the secret key. That is, the security of the cryptosystem should depend only on the key. In many proposed chaotic synchronization schemes, some initial conditions and parameters are treated as the key. It is believed that recovering the hidden message is difficult without the exact values of the key. Hence the security of the parameter is an important problem for chaotic synchronization.

The authors in [52] claimed that it is very difficult to find an identifiable parameter by a brute force attack (exhaustive search of the key space), because the uniqueness of the parameter is directly linked to the parameter identifiability concept. Hence this kind of parameter vector may be a good choice for the secret key. However, this claim is incomplete. Identifiability describes the one-to-one property of the map from the parameter to the measured output. Therefore the identifiable parameter is harmful to the security of the parameter. The authors in [63] made use of the notion of identifiability and parameter identification technique to estimate the parameters by the output. There are other different methods to realize parameter identification [64, 65, 25]. The above results show that that identifiable parameter is not a good choice for the key.

To protect the parameter against all kinds of parameter identification techniques, the identifiability of the parameter should be checked during the design of a chaos-based communication scheme. To test the identifiability, the authors in [52] used the input/output relation approach based on a technique of Gröbner bases and a characteristic set for polynomial systems. However, it is very complex to compute Gröbner bases or characteristic set for general polynomial systems. This section uses definitions of identifiability and the linear algebraic method based different 1-forms introduced in [39, 40]. This method simplifies the computation and deals with systems described by meromorphic functions, which are more general than the polynomial systems discussed in [52].

In order to discuss the security of chaos-based communication schemes, [24] introduces the concept of secure synchronization. This definition requires the synchronization to be antiadaptive secure and antirobust secure. However, it is difficult to verify these two properties. If one system parameter is not identifiable, it is obvious that there is no adaptive observer which can estimate the real parameter value. Hence this kind of system satisfies the antiadaptive property to a certain extent.

3.6.1 Preliminary knowledge about identifiability

Before stating the main results, in this subsection some basis of identifiability is recalled from [40]. Consider the following nonlinear system

$$\begin{cases} \dot{x} = f(x,p,u), \;\; x(0,p) = x_0, \\ y = h(x,p,u), \end{cases} \tag{3.39}$$

where $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$ and $y \in \mathbb{R}^l$ are the system state, input and output, respectively, the constant parameter vector p belongs to a simply connected subset $\Omega \subset \mathbb{R}^q$. It is assumed that x_0 is independent of p and $\text{rank}\partial h(x,p,u)/\partial x = q$. The functions $f(x,p,u)$ and $h(x,p,u)$ are meromorphic functions on a simply connected open subset $M \times \Omega \times U$ of $\mathbb{R}^n \times \mathbb{R}^q \times \mathbb{R}^m$. An input $u(t) : [0,T] \to U$ is said to be an admissible input if equation (3.39) admits a unique (local) solution, where U is a simply connected open subset of $\mathbb{R}^m$. The following definitions are from [66] and [40].

Definition 3 [40]**:** System (3.39) is said to be x_0 identifiable at p through an admissible input $u(t)$ (on $[0,T]$) if there exists an open set $\Omega^0 \subset \Omega$ containing p such that for any two parameters $p_1, p_2 \in \Omega^0, p_1 \neq p_2$, the corresponding solutions of equation (3.39) exist on $[0,\epsilon] \subset [0,T]$, and their corresponding outputs $y(t,p,x_0,u) \neq y(t,p,x_0,u)$ on $[0,\epsilon]$.

In order to study some generic properties of identifiability, a topology for the input function space is introduced. For any $T > 0$ and a positive integer N, $C^N[0,T]$ denotes the space of all functions on $[0,T]$ which have continuous derivatives up to order N. A topology of the space $C^N[0,T]$ is the one associated with a well-defined norm:

$$\|r(t)\| = \sum_{i=0}^{N} \max_{t\in[0,T]} |r^{(i)}(t)|, \quad \text{for } r(t) \in C^N[0,T].$$

Definition 4 [40]**:** System (3.39) is structurally identifiable if there exist a $T > 0$, and a positive constant N, and three open and dense subsets $M^0 \subset M, \Omega_0 \subset \Omega, U^0 \subset C_U^N[0,T]$ such that system (3.39) is x_0-identifiable at p through u, for every $(x_0,p,u) \in M^0 \times \Omega^0 \times U^0$.

Definition 5 [40]**:** System (3.39) is said to be algebraically identifiable if there exist a $T > 0$, a positive constant k, and a meromorphic function $\Phi : \mathbb{R}^q \times \mathbb{R}^{(k+1)m} \times \mathbb{R}^{(k+1)l} \longrightarrow \mathbb{R}^q$ such that

$$\det \frac{\partial \Phi}{\partial p} \neq 0$$

and

$$\Phi(p, u, \dot{u}, \dots, u^{(k)}, y, \dot{y}, \dots, y^{(k)}) = 0$$

hold on $[0,T]$ for all $(p, u, \dot{u}, \dots, u^{(k)}, y, \dot{y}, \dots, y^{(k)})$, where (p, x_0, u) belongs to an open and dense subset of $\Omega \times M \times \times C_U^N[0,T]$; $\dot{u}, \dots, u^{(k)}$ are the corresponding derivatives of u; and $\dot{y}, \dots, y^{(k)}$ are the corresponding derivatives of y.

Definition 6 [40]**:** System (3.39) is said to be identifiable with partially known initial conditions $x_j(0)$, $j = i_1, \dots, i_s, i_s \in \{1, \dots, n\}$ if there exist a positive constant k and a meromorphic function $\Phi : \mathbb{R}^q \times \mathbb{R}^s \times \mathbb{R}^{(k+1)m} \times \mathbb{R}^{(k+1)l} \longrightarrow \mathbb{R}^q$ such that

$$\det \frac{\partial \Phi}{\partial p} \neq 0,$$

and

$$\Phi(p, x_{i_1}(0), \ldots, x_{i_s}(0), u(0^+), \dot{u}(0^+), \ldots, u^{(k)}(0^+), y(0^+), \dot{y}(0^+), \ldots, y^{(k)}(0^+)) = 0$$

hold for all $(p, x_{i_1}(0), \ldots, x_{i_s}(0), u(0^+), \dot{u}(0^+), \ldots, u^{(k)}(0^+), y(0^+), \dot{y}(0^+), \ldots, y^{(k)}(0^+))$, belonging to an open and dense subset of $\mathbb{R}^q \times \mathbb{R}^s \times \mathbb{R}^{(k+1)m} \times \mathbb{R}^{(k+1)l} \rightarrow \mathbb{R}^q$.

The structural identifiability is also called geometric identifiability. It is used to characterize the one-to-one property of the map from the parameter to the system output. The algebraic identifiability enables one to obtain the parameter from solving the algebraic equation based on system input and output.

Denote $\mathcal{Y} = \bigcup_{k=0}^{\infty} \mathrm{span}\{dy, d\dot{y}, \ldots, dy^{(k)}\}$, $\mathcal{X} = \mathrm{span}\{dx\}$, $\mathcal{P} = \mathrm{span}\{dp\}$, $\mathcal{U} = \bigcup_{k=0}^{\infty} \mathrm{span}\{du, d\dot{u}, \ldots, du^{(k)}\}$. Assume the initial conditions are partially known for $x_j(0), j = i_1, \ldots, i_s, i_s \in \{1, \ldots, n\}$, define $\mathcal{X}_p = \mathrm{span}\{dx_j, j = 1, \ldots, i_s\}$.

Theorem 3.16 [40]**:** System (3.39) is algebraically identifiable if and only if $\mathcal{P} \subset (\mathcal{Y} + \mathcal{U})$.

Theorem 3.17 [40]**:** 1) If

$$\mathcal{X} \bigcap (\mathcal{Y} + \mathcal{P} + \mathcal{U}) = \mathcal{X} \bigcap (\mathcal{Y} + \mathcal{U}), \tag{3.40}$$

then system (3.39) is algebraically identifiability if and only if it is structurally identifiable;
2) If system (3.39) is algebraically identifiable, then (3.40) holds.

Theorem 3.18 [40]**:** System (3.39) is identifiable with known $x_j(0)$, $j = i_1, \ldots, i_s$ if and only if $\mathcal{P} \subset (\mathcal{Y} + \mathcal{U}) + \mathcal{X}_p$, or equivalently $\mathcal{P} \bigcap (\mathcal{Y} + \mathcal{U}) + \mathcal{X}_p = \mathcal{P}$.

3.6.2 Identifiability and security of the parameter

Generally, the chaos-based communication scheme includes two parts:

$$\begin{aligned}
&(Transmitter) \quad \begin{cases} \dot{x} &= f(x, p, m), \ x(0) = x_0, \\ y &= h(x, p, m), \end{cases} \\
&(Receiver) \quad \begin{cases} \dot{\hat{x}} &= \hat{f}(\hat{x}, y, p), \ \hat{x}(0) = \hat{x}_0, \\ \hat{y} &= \hat{h}(\hat{x}, y, p,), \end{cases}
\end{aligned} \tag{3.41}$$

where m represents the hidden message, p is the constant parameter vector, f and h describe, respectively, the chaotic dynamic system and the process of hiding the message $m(t)$. When the synchronization is achieved, $\lim_{t\to\infty}|x-\hat{x}|=0$, and the hidden message m is recovered at the receiver end. Generally the initial condition x_0 is assumed to be unknown and the parameter vector p is treated as the secret key. It is also assumed that the intruder cannot recover the message $m(t)$ through the output y without knowledge of the parameter vector p. According to Kerkhoff's assumption [62], the intruder knows the details of the transmitter and receiver, except the key. That is, the intruder knows the functions $f, \hat{f}, h$ and $\hat{h}$, except the parameter vector p. Hence the security of the chaos-based communication scheme depends on the security of the parameter vector p.

The identifiability of p implies that it is possible to determine the parameter p by the output. If the parameter is not identifiable, the only way of finding the parameter is by searching every possible parameter value in the key space, that is, a brute force attack. Then one can measure the possibility of finding the parameter. Hence, to prevent the intruder from determining the parameter, one should choose a parameter that is not identifiable. The identifiability of the parameter should be tested before designing a chaos-based communication scheme. The authors in [40] give the definitions and the necessary and sufficient conditions of identifiability. All the results are obtained in a single framework: the linear algebraic framework. Compared with the Gröbner bases approach and characteristic set approach in [52], this method greatly simplifies the computation and is applicable to more general systems defined by meromorphic functions. To illustrate this method, the identifiability of the Lorenz system is considered,

$$\begin{cases} \dot{x} &= \sigma_1 y - \sigma_2 x, \qquad x(0) = x_0, \\ \dot{y} &= \rho x - y - xz, \qquad y(0) = y_0, \\ \dot{z} &= xy - \beta z, \qquad z(0) = z_0, \end{cases} \tag{3.42}$$

the output is the first state variable x. It is well known that system (3.42) exhibits chaotic behaviour with the standard parameters, $(\sigma_1, \sigma_2, \rho, \beta) = (10, 10, 28, 8/3)$. Assume that the initial values are unknown, all the parameters σ_1, σ_2, ρ and β are unknown. In addition, assume $\sigma_1 \neq \sigma_2$. Under this condition, system (3.42) may also exhibit chaotic behaviour. According to Theorem 3.16 and 3.17 introduced above, for system (3.42), $\mathcal{X}_p \subset \mathcal{Y}$ since the initial value of the output x is known. Hence the algebraic identifiability is equivalent to identifiability with known partially initial conditions.

Let $\theta = [\sigma_1, \sigma_2, \rho, \beta]^T$, compute

$$d\dot{x} = a_1 d\theta - \sigma_2 dx + \sigma_1 dy, \tag{3.43}$$

$$d\dot{y} = a_2 d\theta + (\rho - z)dx - dy - xdz, \tag{3.44}$$

$$d\dot{z} = a_3 d\theta + ydx - xdy - \beta dz, \tag{3.45}$$

where $a_1 = [y, -x, 0, 0], a_2 = [0, 0, x, 0]$ and $a_3 = [0, 0, 0, -z]$. Then one has

$$d\ddot{x} = (\dot{a}_1 + \sigma_1 a_2)d\theta + \sigma_1(\rho - z)dx - \sigma_2 d\dot{x} - \sigma_1 dy - \sigma_1 xdz. \tag{3.46}$$

From equation (3.43) and (3.46), it is obtained that

$$\begin{aligned} \sigma_1 dy \quad &= -a_1 d\theta + \sigma_2 dx + d\dot{x}, \\ \sigma_1 xdz \quad &= (\dot{a}_1 + \sigma_1 a_2)d\theta + \sigma_1(\rho - z)dx - \sigma_2 d\dot{x} - d\ddot{x} - \sigma_1 dy \end{aligned} \tag{3.47}$$

If $x \neq 0$, substitute equation (3.47) into the following equation,

$$dx^{(3)} = \ddot{a}_1 d\theta - \sigma_2 d\ddot{x} + \sigma_1 d\ddot{y} = c_1 d\theta + c_2 dx + c_3 d\dot{x} + c_4 d\ddot{x}, \tag{3.48}$$

where

$$\begin{aligned} c_1 \quad &= \ddot{a}_1 + \sigma_1[\dot{a}_2 - a_2 - \frac{a_1}{\sigma_1} - \frac{a_1}{\sigma_1}x^2 + (\frac{1}{\sigma_1} - \frac{\dot{x}}{\sigma_1}x + \beta x)(\dot{a}_1 + a_1 + \sigma_1 a_2) \\ &= [g_1, g_2, g_3, g_4], \end{aligned} \tag{3.49}$$

and

$$\begin{aligned} g_1 = \beta\rho x, \quad g_2 = -x^3 - \dot{x} - \ddot{x} + \tfrac{\dot{x}}{x}(x + \dot{x}) - \beta(x + \dot{x}), \\ g_3 = \sigma_1 \beta x, \quad g_4 = \sigma_1 \rho x - (1 + \sigma_2)(x + \dot{x}), \end{aligned} \tag{3.50}$$

c_2, c_3 and c_4 are the functions with respect to $(\theta, x, \dot{x}, \ddot{x})$ such that equality (3.48) holds. For $k \geq 3$, it is easy to compute that

$$dx^{(k)} = c_1^{(k-3)} d\theta + (c_2 dx + c_3 d\dot{x} + c_4 d\ddot{x})^{(k-3)}. \tag{3.51}$$

It follows from equation (3.51) and (3.49) that

$$\frac{\partial(x^{(3)}, x^{(4)}, x^{(5)}, x^{(6)})}{\partial(\sigma_1, \sigma_2, \rho, \beta)} = \begin{bmatrix} g_1 & g_2 & g_3 & g_4 \\ \dot{g}_1 & \dot{g}_2 & \dot{g}_3 & \dot{g}_4 \\ \ddot{g}_1 & \ddot{g}_2 & \ddot{g}_3 & \ddot{g}_4 \\ g_1^{(3)} & g_2^{(3)} & g_3^{(3)} & g_4^{(3)} \end{bmatrix}. \tag{3.52}$$

By equation (3.50), the column vectors $[g_1, \dot{g}_1, \ddot{g}_1, g_1^{(3)}]^T$ and $[g_3, \dot{g}_3, \ddot{g}_3, g_3^{(3)}]^T$ are linearly dependent. Therefore, system (3.42) is not algebraically identifiable.

Define a new parameter vector $\theta' = [\sigma_1\rho\beta, \sigma_2, \beta]^T$. From equation (3.48), the following equation is obtained for $k \geq 3$

$$dx^{(k)} = c{'}_1^{(k-3)} d\theta' + (c_2 dx + c_3 d\dot{x} + c_4 d\ddot{x})^{(k-3)},$$

where

$$c_1' = [f_1, f_2, f_3] = [x, g_2, g_4 - \sigma_1\rho x].$$

If the set of functions $\{f_1, f_2, f_3\}$ is linearly independent, the rank of Jacobian matrix $\frac{\partial(x^{(3)}, x^{(4)}, x^{(5)})}{\partial(\sigma_1\rho\beta, \sigma_2, \beta)}$ is 3.

If the set of functions $\{f_1, f_2, f_3\}$ is linearly dependent on $[0, T]$, that is, there exists three different parameters a_1, a_2, a_3, different from zero, such that

$$a_1 f_1 + a_2 f_2 + a_3 f_3 = 0 \tag{3.53}$$

holds on $[0, T]$. Then equation (3.53) is a second order differential equation. By the Poincaré-Bendixon Theorem [67], a second order differential equation cannot exhibit chaotic behaviour. It is contradictory to the chaotic solution of equation (3.42). Hence the set of functions $\{f_1, f_2, f_3\}$ is linearly independent, and the rank of matrix $\frac{\partial(x^{(3)}, x^{(4)}, x^{(5)})}{\partial(\sigma_1\rho\beta, \sigma_2, \beta)}$ is 3. Therefore the new parameter vector θ' is algebraically identifiable. That is, the parameter vector θ' can be determined uniquely through the output. If the parameter ρ or σ_1 is known, then the other parameters can be determined through the output. The parameters ρ or σ_1 is a good choice for a secret key. It should be noted that system (3.42) is identifiable if $\sigma_1 = \sigma_2$.

3.6.3 Two applications of the theory of identifiability

A modified parameter modulation scheme

System (3.42) is used to construct a modified parameter modulation scheme. Let $(\sigma_1, \sigma_2, \rho, \beta) = (13, 10, 28, 8/3)$. Note that $\sigma_1 \neq \sigma_2$, and the parameter σ_1 is unknown to the intruder. For the classical parameter modulation scheme [8][44], the parameter σ_1 is modulated by binary encoded plaintext, so that it is $\sigma_1 + \delta$ if the plaintext bit is '1', and $\sigma_1 - \delta$ if the plaintext bit is '0', where δ is a constant. The proposed method consists of three steps.

Step 1 (Encryption) Let $B = [B_0, B_1, \dots, B_n]$ be the plaintext bit sequence, where $B_i = B_{i1}B_{i2}\dots B_{ik}$ is a plaintext block of length k bits. Let $b_i = \sum_{j=1}^{k} 2^{j-1}B_{ij} + 1$ and $\rho_i = 28 + b_i/2^k$.

Step 2 (Synchronization) Construct an adaptive observer as introduced in [51] to estimate the state and parameter. When synchronization is achieved, $|\rho_i - \rho_i'| < \epsilon$, where ρ_i' is the estimated parameter and ϵ is a small enough positive constant.

Step 3 (Decryption) Let $\widehat{\rho}_i$ be the nearest integer to ρ_i', then the bit sequence information B_i is recovered from binary representation of $2^k(\widehat{\rho}_i - 28)$.

Remark 6: The selection of k depends on ϵ. The smaller the parameter ϵ is, the larger the k is. Hence one should select an exponential observer before implementing this communication scheme. In the classical parameter modulation method, the parameter has two states corresponding to '1' or '0' of the plaintext. This method only transmits one bit when synchronization is achieved. Compared with the classical parameter modulation scheme, ρ has more choices in the modified parameter scheme. It can choose 2^k different values in the interval $(28, 29]$. The plaintext B_i is a block of k-bits, thus this method can also transmit more information. If the parameter ρ has more choices, the return map and the power analysis attacks cannot recover the plaintext through the output, which is shown in [68]. The intruder cannot obtain the plaintext without the precise value of b_i. From the above analysis it follows that the parameter ρ cannot be determined by the output if the parameter σ_1 is unknown. Hence, the only way of finding the actual parameter value of ρ is brute force attack, since system (3.42) is not identifiable. For this attack, the intruder needs to search 2^k times to find the actual parameter ρ from the interval $(28, 29]$. That is, the intruder has a possibility of $1/2^k$ to find the parameter.

Security against chosen ciphertext attack

This subsection shows that system (3.42) is secure against the chosen ciphertext attack proposed in [50]. The following chaos-based communication scheme was proposed in

[69]

$$(Transmitter)\begin{cases}\dot{x} = \sigma_1 y - \sigma_2 x,\\ \dot{y} = (\rho-\mu)[x+m(t)] + \mu x - y - [x+m(t)]z,\\ \dot{z} = [x+m(t)]y - \beta z,\end{cases} \tag{3.54}$$

$$(Receiver)\begin{cases}\dot{x}_1 = \sigma_1 y_1 - \sigma_2 x_1,\\ \dot{y}_1 = (\rho-\mu)[x+m(t)] + \mu x_1 - y_1 - [x+m(t)]z_1,\\ \dot{z}_1 = [x+m(t)]y_1 - \beta z_1,\end{cases} \tag{3.55}$$

where $m(t)$ is the message signal and $\sigma_1 = \sigma_2$. Once the synchronization is achieved, $x = x_1$ and the message $m(t)$ is recovered by stripping away $x(t)$. In the receiver equation (3.55), the input is $s = x + m(t)$, and the output is x_1. A chosen-ciphertext attack is adopted to analyze the parameters in [50]. When s is constant, system (3.55) has a fixed point,

$$\left(\frac{(-\beta s(\rho-\mu)}{(-s^2+\beta\mu-b)}, \frac{(-\beta s(\rho-\mu)}{(-s^2+\beta\mu-b)}, \frac{(-s^2(\rho-\mu)}{(-s^2+\beta\mu-b))}\right).$$

Selecting different values of s, one obtains a number of equations with respect to the parameters ρ, μ and β, then they can be solved from these equations.

Now, system (3.42) is used to construct system (3.54) and (3.55), that is, let $\sigma_1 \neq \sigma_2$. Then the chosen ciphertext attack cannot determine the parameter vector. The receiver system has a fixed point when s is a constant,

$$\left(\frac{(\beta\sigma_2 s(\rho-\mu)}{(\beta\sigma_2+s^2\sigma_2-\beta\mu\sigma_1)}, \frac{\beta\sigma_1 s(\rho-\mu)}{(\beta\sigma_2+s^2\sigma_2-\beta\mu\sigma_1)}, \frac{\sigma_2 s^2(\rho-\mu)}{(\beta\sigma_2+s^2\sigma_2-\beta\mu\sigma_1))}\right).$$

Let $a_1 = \beta\sigma_2\rho, a_2 = \beta\sigma_2\mu, a_3 = \beta\sigma_2, a_4 = \sigma_2, a_5 = \beta\mu\sigma_1$. Obviously, if $\mu\beta^3\sigma_2^3 \neq 0$, $\sigma_1, \sigma_2, \rho, \beta, \mu$ can be determined if and only if a_1, a_2, a_3, a_4, a_5 can be determined. Let

$$C_1 = \frac{(\beta\sigma_2 s(\rho-\mu)}{(\beta\sigma_2+s^2\sigma_2-\beta\mu\sigma_1)} = (a_1-a_2)s/(a_3+s^2a_4-a_5),$$

then one has

$$(a_1-a_2)s - (a_3+s^2a_4-a_5)C_1 = 0. \tag{3.56}$$

Substitute different values of s into equation (3.56), the following linear equations are obtained,

$$\begin{bmatrix} c_1 & -c_1 & -C_{11} & -c_1^2C_{11} & C_{11}\\ c_2 & -c_2 & -C_{12} & -c_2^2C_{12} & C_{12}\\ c_3 & -c_3 & -C_{13} & -c_3^2C_{13} & C_{13}\\ c_4 & -c_4 & -C_{14} & -c_4^2C_{14} & C_{14}\\ c_5 & -c_5 & -C_{15} & -c_5^2C_{15} & C_{15}\end{bmatrix}\begin{bmatrix}a_1\\a_2\\a_3\\a_4\\a_5\end{bmatrix} = Ap' = 0,$$

where $p' = [a_1, a_2, a_3, a_4, a_5]$, s takes different values c_1, c_2, c_3, c_4, c_5 and the corresponding $C_1 = C_{11}, C_{12}, C_{13}, C_{14}, C_{15}$. Then a_1, a_2, a_3, a_4, a_5 cannot be determined uniquely, since A is singular.

In fact, s can be treated as an input or an known parameter in system (3.55). In the same way in the analysis of system (3.42), one also can obtain equation (3.56), and prove that system (3.55) is not identifiable. That is, the parameters cannot be determined from the output.

3.7 Summary and conclusion

In this chapter synchronization is achieved for the generalized Lorenz system with an unknown parameter. The synchronization implies that this system is not suitable to implement secure synchronization. This result is based on investigating some dynamical properties and the PE condition of this system. Parameter identifiability is used to evaluate whether the parameter of a chaotic system is secure in a chaos based communication scheme. A linear algebraic method based on differential 1-forms is used to test the identifiability of more general system.

Chapter 4

Security and robustness of a modified parameter modulation communication scheme

4.1 Chapter outline

This chapter provides a modified parameter modulation communication scheme to improve security. This scheme and its security analysis are given in Section 4.2. The modified parameter scheme is based on a cryptosystem constructed by a 1-D discretized chaotic map controlled by a Δ-modulated feedback, which is proved to be chaotic when parameter a belongs to $(\sqrt{2}, 2]$. The idea comes from [16] and [17]. The modulated parameter is generated by this cryptosystem and selected according to the criteria in Section 3.6. Hence the parameter has more choices in key space and is difficult to be recovered without the information of this cryptosystem. In Section 4.3, the robustness of this scheme against uncertainty or noise is studied. This study is also important because a large error could make the cryptosystem go astray from real value. The upper bounds are obtained so that the cryptosystem works properly in practical implementation. Numerical simulation shows that the upper bounds are sharp. The last section is the summary and conclusion.

4.2 Improving the security of chaotic synchronization with a Δ-modulated cryptographic technique

Based on conventional cryptographic techniques, various chaos-based schemes have recently been developed [16, 17]. A common feature of these methods is the utilization of state variables of the chaotic systems as keys in the encryption algorithms. For parameter modulation schemes, more secure methods were proposed in [70, 68]. In this section, a modified parameter modulation scheme is proposed to improve security further. The numerical simulation shows that two popular attacks are ineffective when using the modified parameter modulation scheme and the parameter has a high degree of security. In this modified parameter modulation scheme, a continuous chaotic system with a parameter is used to transmit encoded message. The parameter is generated by a cryptosystem which offers it many choices corresponding to transmitted bit '0' or '1', and thus protection against power analysis and return map attack. The cryptosystem is constructed by using a one-dimensional discrete-time system controlled by a Δ-modulated feedback, which is quite different from [18] that uses a logistic map. The first reason why the proposed scheme uses this Δ-modulated system is the simplicity and speciality of Δ-modulation, which makes it an attractive choice for control practitioners. Yet, little attention has been paid to the chaotic property of this kind of system. Another reason is that the result can easily be extended to high-dimensional Δ-modulated control systems, which will make the cryptosystem more secure. The complex behaviour of this simple control system due to Δ-modulated feedback has been investigated in [71], [72]–[73]. When some parameter $a > 2$ in this particular one-dimensional discrete system, the system is chaotic [74, 72] but not a self-map. Note that the construction of a cryptosystem needs a self-map. In this section, the system is proved to be chaotic and also a self-map when $a \in (\sqrt{2}, 2]$.

Subsection 4.2.1 proves that the one-dimensional discrete system controlled by a Δ-modulated feedback is chaotic when the parameter $a \in (\sqrt{2}, 2]$. Then two basic requirements for security and the framework of proposed method are given in subsection 4.2.2. With the help of the Lorenz system and a secure cryptosystem based on a Δ-modulated feedback control system, the modified parameter modulation scheme is also illustrated in detail in subsection 4.2.2. Finally, the security of this scheme is analyzed by numerical simulations.

4.2.1 A one-dimensional discrete system controlled by a Δ-modulated feedback

As mentioned above, a chaotic discrete self-map is used to construct a secure chaotic cryptosystem. Hence the one-dimensional discrete time chaotic system [74, 72] is introduced:

$$x^{+} = ax - \Delta \mathrm{sgn}(ax), \tag{4.1}$$

where

$$\mathrm{sgn}(x) = \begin{cases} 1, & x \geq 0, \\ -1, & x < 0, \end{cases}$$

x^{+} denotes the system state at the next discrete time, a is a real number, and Δ is a positive constant. In [72], the authors proved that (4.1) is chaotic when $|a| > 2$. This section considers $1 < |a| \leq 2$. For simplicity, only consider $a \in (1, 2]$. This map will be proved to be chaotic and maps an interval to itself, when the parameter $a \in (\sqrt{2}, 2]$. Hence, it can be used to implement a similar cryptographic algorithm as proposed in [18]. Based on this algorithm, a modified parameter modulation scheme is illustrated.

By performing a state transformation $y = x/\Delta$, a new map is obtained

$$y^{+} = f(y), \quad \text{where } f(y) = \begin{cases} ay - 1, & y \geq 0, \\ ay + 1, & y < 0. \end{cases} \tag{4.2}$$

When $a = 2$, this map is equivalent to Baker's map, which is chaotic [75]. Hence the following only considers the case $a \in (1, 2)$. When $a \in (1, 2)$, f is surjective on $[-1, 1)$. Before stating the main result, the following well-known and frequently used definitions are recalled from [5]. The symbol $f^{n}(x)$ denotes $\underbrace{f \ldots (f(x))}_{n}$.

Definition 1 [5]**:** Consider a map: $F : I \to I$, where I is an interval, F is *topologically transitive* on I if for any two open sets $U, V \subset I$ there exists an integer $n > 0$ such that $f^{n}(U) \cap V \neq \varnothing$.

Definition 2 [5]**:** Consider a map: $F : I \to I$, where I is an interval, F has *sensitive dependence on initial conditions* if there exists a $\delta > 0$ such that, for any

$x \in I$ and any neighbourhood N of x, there exist a $y \in N$ and an $n > 0$ such that $|F^n(x) - F^n(y)| > \delta$.

Definition 3 [5]: Let X be a metric space. A map $F : X \to X$ is said to be *chaotic* on X if

1. F is transitive;
2. the periodic points of F are dense in X;
3. F has sensitive dependence on initial conditions.

In the above definitions F may not be continuous (c.f. [5]). The following lemma can be found in [76] and [77].

Lemma 4.1: If $a > \sqrt{2}$, then

1. there is an integer n such that $f^n(J) = [-1, 1)$, where J is a subinterval in $[-1, 1)$;
2. f is topologically transitive;
3. f has sensitive dependence on initial conditions.

In order to prove that the periodic points of f is dense, define $V_n = \{x | f^n(x) = 0, x \in [-1, 1), x \neq 0\}$ and $\hat{x}_n = \min\{x | x \in V_n \cap [0\ 1)\}$. Obviously, the number of the points in V_n is 2^n at most. From equation (4.2), one can obtain that $f^n(-x) = -f^n(x)$ if $f^i(x) \neq 0, i = 1, 2, \ldots, n-1$. In the neighbourhood of the discontinuous point 0, one has $\lim_{x \to 0^-} f^n(x) = -f^n(0)$.

Lemma 4.2: The set $\bigcup_{i=1}^{\infty} V_i$ is dense on $I = [-1, 1)$.

Proof: Owing to $a > 1$, for any open interval U in I which does not include 0, the length of $f^i(U)$ is larger than the length of $f^{i-1}(U)$. Hence there exists an integer n such that f^n is continuous on U and $0 \in f^n(U)$. Then there is a point $x \in U$ such that $f^n(x) = 0$, and thus $x \in V_n$ and $\bigcup_{i=1}^{\infty} V_i$ is dense on I. □

Lemma 4.3: For any integer N, there exists an integer $m > N$ such that $f^m(0) \in [-1, -1/a]$ or $f^m(0) \in [1/a, 1)$.

Proof: If 0 is a periodic point with period k, then $f^{Nk+1}(0) = -1$.

If 0 is not a periodic point and this lemma does not hold, then there exists an integer N_1 such that $f^n(0) \notin [-1, -1/a] \cup [1/a, 1)$ for all the integer $n \geq N_1$. If $x_0 = f^{N_1}(0) \in (-1/a, 0)$, then $x_1 = f^{N_1+1}(0) \in (0, 1/a)$. Following the same way, it is obtained that $x_i = f^{N_1+i}(0) < 0$ when i is even and $x_i = f^{N_1+i}(0) > 0$ when i is odd. After a simple computation, it is obtained that $x_{2i} = [a^{2i}(ax_0 + x_0 + 1) - 1]/(a + 1)$. Because 0 is not a periodic point, $x_0 \neq -1/(a + 1)$. Hence there exists an even integer $2i$ such that $x_{2i} > 0$ or $x_{2i} \leq -1/a$. It contradicts $x_{2i} \in (-1/a, 0)$. For the other case $x_0 \in [0, 1/a)$, the same conclusion is obtained similarly. □

Lemma 4.4: Assume $a > \sqrt{2}$, for any integer $k > 0$, there exist an integer n and $x_{n+1} \in V_{n+1}$, such that $n > k$, $x_{n+1} < \hat{x}_n < \hat{x}_k$ and $(x_{n+1}, \hat{x}_n) \cap V_i = \emptyset$, $i = 1, 2, \ldots, n + 1$.

Proof : For any integer $k > 0$, it follows from Lemma 4.1 that there exists N_k such that $f^{N_k}([0, \hat{x}_k]) = [-1, 1)$. Hence $[0, \hat{x}_k] \cap V_i \neq \emptyset$ for all $i \geq N_k$. Therefore, for any integer k, there exists an integer $N > \max\{k, N_k\}$ such that $\hat{x}_m < \hat{x}_k$ for all $m > N$. Apply Lemma 4.3 for this integer N, then there exists an integer $n > N$ such that $f^n(0) \in [-1, -1/a]$ or $f^n(0) \in [1/a, 1)$. Now the first case of $f^n(0) \in [1/a, 1)$ is considered. This case includes the following two subcases: $(0, \hat{x}_n) \cap V_i = \emptyset$ for all $i < n$ and $(0, \hat{x}_n) \cap V_i \neq \emptyset$ for some $i < n$.

i) If $(0, \hat{x}_n) \cap V_i = \emptyset$ for all $i < n$, then $f^n([0, \hat{x}_n]) = [f^n(0), 0] \supset [-1/a, 0]$ and f^n is continuous on $[0, \hat{x}_n]$. Hence there exists a point $x' \in [0, \hat{x}_n]$ such that $f^n(x') = -1/a$. Then $x' \in V_{n+1}$ and $(x', \hat{x}_n) \cap V_i = \emptyset$ for all $i \leq n + 1$.

ii) If $(0, \hat{x}_n) \cap V_i \neq \emptyset$ for some $i < n$, then there exists a maximal positive integer k_1, such that $0 < n - k_1 < n$ and the point $\hat{x}_{n-k_1} \in [0, \hat{x}_n]$. Thus $f^{n-k_1}([0, \hat{x}_n]) = [f^{n-k_1}(0), f^{n-k_1}(\hat{x}_n)]$ and $f^{n-k_1}(0) < 0 < f^{n-k_1}(\hat{x}_n)$. Now one proves that there exists a point $x_1 \in (\hat{x}_{n-k_1}, \hat{x}_n)$ such that $f^{n-k_1}(x_1) = -f^{n-k_1}(0) < f^{n-k_1}(\hat{x}_n)$. If it does not hold, then there is a point $x_2 \in (0, \hat{x}_n)$ such that $f^{n-k_1}(x_2) = -f^{n-k_1}(\hat{x}_n)$. Hence $f^{k_1}(f^{n-k_1}(x_2)) = 0$ and $x_2 \in V_n$. It contradicts the definition of $\hat{x}_n$, hence $-f^{n-k_1}(0) < f^{n-k_1}(\hat{x}_n)$. Because f^{n-k_1} is continuous and monotonic on $(\hat{x}_{n-k_1}, \hat{x}_n)$, there is a point $x_1 \in (\hat{x}_{n-k_1}, \hat{x}_n)$ such that $f^{n-k_1}(x_1) = -f^{n-k_1}(0)$. To find a point $x' \in V_{n+1}$ in $(x_1, \hat{x}_n)$ such that this lemma holds, it is also considered in two situations. Firstly, if $(x_1, \hat{x}_n) \cap V_i = \emptyset$ for all $i < n$, that is, $(-f^{n-k_1}(0), f^{n-k_1}(\hat{x}_n)) \cap V_i = \emptyset$ for all $i < k_1$, then

$f^{k_1}(-f^{n-k_1}(0)) = -f^n(0) < f^{k_1}(f^{n-k_1}(\hat{x}_n)) = 0$. Since f^{k_1} is continuous on $(x_1, \hat{x}_n)$, there exists a point x' such that $f^{n+1}(x') = f(f^n(x')) = f(-1/a) = 0$. Hence $x' \in V_{n+1}$ and $(x', \hat{x}_n) \cap V_i = \emptyset$ for $i \leq n+1$. Secondly, if $(x_1, \hat{x}_n) \cap V_i \neq \emptyset$ for some $i < n$, then there exists a maximal positive integer $k_2 < k_1$ such that the point $x_{n-k_2} \in (x_1, \hat{x}_n)$, where $x_{n-k_2} \in V_{n-k_2}$. Because the number of points in V_i is finite for all $i \leq n$, one can repeat the above procedure until a point x' is found such that this lemma holds.

As for the second case of $f^n(0) \in [-1, -1/a]$, by the fact that $\lim_{x \to 0^-} f^n(x) = -f^n(0)$, the same conclusion is obtained. □

Lemma 4.5: The set of periodic points of f is dense in $I = [-1\ 1)$ when $a > \sqrt{2}$.

Proof: For any interval $[\alpha, \beta] \subset [0, \delta]$ where $0 < \delta < 1/2$, it follows from Lemma 4.2 that there is an $x_n \in V_n$ in (α, β). Since the number of the points in V_i is finite for all $i \leq n$, there exists also an $x_{n+k} \in V_{n+k}$ in (x_n, β) such that $(x_n, x_{n+k}) \cap V_i = \emptyset$ for all $i \leq n+k$. Hence $f^n([x_n, x_{n+k}]) = [0, \hat{x}_k]$ and continuous on $[x_n, x_{n+k}]$. By Lemma 4.4, there are two points $x_{m+1} < \hat{x}_m$ in $(0, \hat{x}_k)$ such that $(x_{m+1}, \hat{x}_m) \cap V_i = \emptyset$ for all $i \leq m+1$, where x_{m+1} is some point in V_{m+1}. Because f^n is continuous and monotonic on $[x_n, x_{n+k}]$, there are two points $x_2 < x_1$ in (x_n, x_{n+k}) such that $f^n(x_2, x_1) = (x_{m+1}, \hat{x}_m)$ and $(x_2, x_1) \cap V_i = \emptyset$ for all $i \leq m+n+1$. Therefore $f^{m+n}([x_2, x_1]) = [-1/a, 0]$ and f^{m+n} is continuous on $[x_2, x_1]$. Hence there exists a small enough positive ε such that $[x_2, x_1 - \varepsilon] \subset f^{m+n+1}([x_2, x_1 - \varepsilon])$ and f^{m+n+1} is continuous on $[x_2, x_1 - \varepsilon]$. Therefore there is a periodic point in $[\alpha, \beta]$.

Now we consider any interval $K \subset I$. By Lemma 4.1, this K is contained in $f^i([0, \delta])$ for some i. Since the set of periodic points of f is dense in $[0, \delta]$, we can find a periodic point p in $[0, \delta]$ and $f^i(p)$ in K. □

The idea in the proof for Lemma 4.4 comes from [78]. By Lemma 4.1 and 4.5, we have the following theorem:

Theorem 4.6: The map defined in (4.2) is chaotic in $I = [-1, 1)$ when $a \in (\sqrt{2}, 2]$.

4.2.2 Chaotic synchronization combined with cryptographic technique

Basic requirements and the framework of the modified parameter modulation scheme

As mentioned above, security is one of the most important problems in chaotic synchronization. If a chaos-based scheme is secure, it must satisfy the following two basic requirements:

1. The plaintext cannot be extracted when the opponent does not know the keys.
2. The keys have a high degree of security.

Obviously, many parameter modulation methods do not satisfy the first requirement. The parameter in these methods has two states corresponding to '1' and '0'. However, the change of the parameters results in the change of the dynamic properties of the chaotic system. Hence the power analysis or return map attack makes it easy to distinguish the two states. With reference to the classical cryptography, the system parameters of the chaotic systems can be treated as the secret key. However, as pointed out in [24], many robust and adaptive control methods could be considered for possible attack against a secure communication and encryption schemes. That is, the keys have a low degree of security. To improve security, an encryption function is used to protect the system parameter.

A continuous chaotic system is considered as below:

$$\begin{cases} \dot{x} &= f(x,p), \\ y &= h(x), \end{cases} \tag{4.3}$$

where $x \in \mathbb{R}^n, y \in \mathbb{R}^m$ and $p \in \mathbb{R}^l$ are the state variable, output, and parameter vector, respectively. The classical parameter modulation method is to change the parameter p with the binary encoded plaintext, namely, p has two states corresponding to '1' or '0' of the plaintext. The modified parameter modulation scheme consists of three steps:

1) encryption: $p = e(P)$, that is, a chaotic encryption function e is applied to encrypt the plaintext P and produce the parameter p;

2) synchronization: It is not difficult to construct an adaptive observer to estimate the state and parameter at the same time, since many papers focus on this topic [51, 38];

3) decryption: $P' = de(p')$, the inverse of the encryption de is applied to recover the plaintext, once the estimated parameter value p' is obtained.

Without the encryption information, the opponents cannot know the plaintext, even if they can estimate the parameters. In the following subsections, the proposed scheme is illustrated by using a cryptographic algorithm introduced in [18].

Chaotic cryptosystem based on a Δ-modulated feedback control system

A chaotic cryptosystem proposed by Pareek *et al.* in [18] is based on the logistic map, $y = g_\lambda(x) = \lambda x(1-x)$. It is a symmetric key block cipher which utilizes the essence of chaos, that is, sensitivity on initial condition as well as on system parameter. It should be noted that the logistic map's chaotic parameter range is $3.57 \leq \lambda \leq 4$.

Now the basic procedure of encryption and decryption is recalled from [18]. Since ASCII is an 8-bit code which represents 256 characters, the plaintext and the ciphertext are divided into blocks of 8 bits,

$$P = P_1 P_2 \ldots P_n \text{ (plaintext) }, \quad C = C_1 C_2 \ldots C_n \text{ (ciphertext) },$$

where P_i and C_i are single blocks of 8-bits, n is the block length of the plaintext/ciphertext. An external 128-bits secret key $K = K_1 K_2 \ldots K_{16}$, is also divided into blocks of 8 bits, where K_i, the session key, consists of 8 bits, and the block length is 128/8=16. Let $i = 1$, and take the following steps:

1) Define two real numbers X_s and N_s by:

$$X_s = \frac{((K_1)_2 \oplus (K_2)_2 \oplus \cdots \oplus (K_{16})_2)_{10}}{M},$$
$$N_s = (K_1 + K_2 + \ldots + K_{16}) \bmod 256,$$

where $M = 256$ (M can be 2^k for any integer $k \geq 8$), K_j and $(K_j)_2$ are the j-th session key's ASCII value and binary equivalent of the ASCII value, respectively, $j = 1 \ldots 16$. The notation $()_{10}$ is the decimal equivalent of the corresponding binary number, and $\oplus$ is the XOR operation. The result of XOR(S,T) is 1 (true) if either S or T, but not both, is nonzero, and 0 (false) if both S and T are zero or nonzero.

2) Choose a K_r randomly from $\{K_1, \dots, K_{16}\}$, and let $X = (X_s + \frac{K_r}{M}) \bmod 1$ and $N = N_s + K_r$, where $x \bmod 1 = x - \lfloor x \rfloor$, and $\lfloor x \rfloor$ is the floor (also called truncation) function.

3) Let $\lambda_i = \big((bY_i + c) \bmod m\big)/200 + 3.57$, where $Y_i = (bY_{i-1} + c) \bmod m$, $b = 16, c = 7, m = 81$, $Y_1 = 0$.

4) Define the encryption/decryption in the following way:

$$\begin{aligned} C_i &= (P_i + \lfloor X_{new} M \rfloor) \bmod 256, \text{ (encryption)}, \\ P_i &= (C_i + 256 - \lfloor X_{new} M \rfloor) \bmod 256, \text{ (decryption)}, \end{aligned} \tag{4.4}$$

where $X_{new} = g^N_{\lambda_i}(X)$, and $g^N_{\lambda_i}(X)$ is obtained by iterating the logistic map $g_{\lambda_i}(x) = \lambda_i x(1-x)$ for N times at X.

5) Put the symbols corresponding to the ASCII values of C_i/P_i obtained in Step 4) as the ciphertext/plaintext. If $i = n$, then stop the algorithm, otherwise let $X_s := X_{new}$, $N_s := C_i$ and $i := i + 1$, and go to Step 2).

In order to apply the Δ-modulated feedback control system to transmit information by chaotic synchronization, system (4.2) is modified as:

$$x_{j+1} = F_a(x_j) := \begin{cases} \frac{\text{round}(Max_j)}{M} - 1, & x_j \geq 0, \\ \frac{\text{round}(Max_j)}{M} + 1, & x_j < 0, \end{cases} \tag{4.5}$$

where round(x) is the roundoff function, and for any integer $k \geq 10$, x_j belongs to the set:

$$P = C = \{0, \pm\frac{1}{M}, \dots, \pm\frac{M-1}{M}\}, \text{ with } M = 2^k. \tag{4.6}$$

Compared with the chaotic range $[3.57, 4]$ of the logistic map, the parameter of system (4.2) has a wider chaotic range, $(\sqrt{2}, 2]$. Hence, to construct the above cryptosystem, step 3) and step 4) are modified and the other steps are kept:

3′) Let $a_i = \big((bY_i + c) \bmod m\big)/200 + 1.42$, where $Y_i = (bY_{i-1} + c) \bmod m$, $b = 16, c = 7, m = 96$, and $Y_1 = 0$. Obviously, $a_i \in [1.42, 2)$.

4′) Let X_{new} be $F^N_{a_i}(X)$, where $F^N_{a_i}(X)$ is obtained by iterating F_{a_i} for N times at the point X. Then define the encryption/decryption in the following way:

$$\begin{aligned} C_i &= (P_i + \lfloor X_{new} M \rfloor) \bmod 256, \text{ (encryption)}, \\ P_i &= (C_i + 256 - \lfloor X_{new} M \rfloor) \bmod 256, \text{ (decryption)}. \end{aligned} \tag{4.7}$$

To construct a new cryptosystem based on system (4.5), a parameter value $M = 2^k$ is first selected for some $k \geq 10$, then execute step 1), 2), 3′), 4′) and 5) to get a more secure cryptosystem.

Detailed illustration of the modified parameter modulation scheme

Now the modified parameter modulation scheme is illustrated with the help of the celebrated Lorenz system. According to (4.3), the Lorenz system with output is written as

$$\begin{cases} \dot{x}_1 &= -\sigma_1 x_1 + \sigma_2 x_2, \\ \dot{x}_2 &= \rho x_1 - x_2 - x_1 x_3, \\ \dot{x}_3 &= x_1 x_2 - \beta x_3, \\ y &= x_1. \end{cases} \tag{4.8}$$

It is well known that the system exhibits chaotic behaviour with the standard parameters $(\sigma_1, \sigma_2, \rho, \beta) = (10, 10, 28, 8/3)$. For the classical parameter modulation scheme [44], the parameter σ_1 is modulated by binary encoded plaintext, so that it is $\sigma_1 + \delta$ if the plaintext bit is ‘1’ and $\sigma_1 - \delta$ if the plaintext bit is ‘0’, where δ is a constant. The modified parameter modulation scheme consists of three steps.

Step 1 (Encryption) Let $P = P_0 P_1 \ldots P_n$ be the plaintext sequence, where P_i is a plaintext block of length 8 bits. Following the procedure introduced above, X_{new} is generated in step 4′) and C_i is obtained through (4.11). Let $\sigma_1 = 10 + C_i/M$, the index r of K_r can be transmitted through the parameter ρ, that is, $\rho = 28 + r/16$.

Step 2 (Synchronization) Construct an adaptive observer as introduced in [51] to estimate the state and parameters simultaneously. When the synchronization is achieved, one has $|\sigma_1 - \sigma_1'| < \epsilon$ and $|\rho - \rho'| < \epsilon$, where σ', ρ' are the estimated parameters and ϵ is a small enough positive constant.

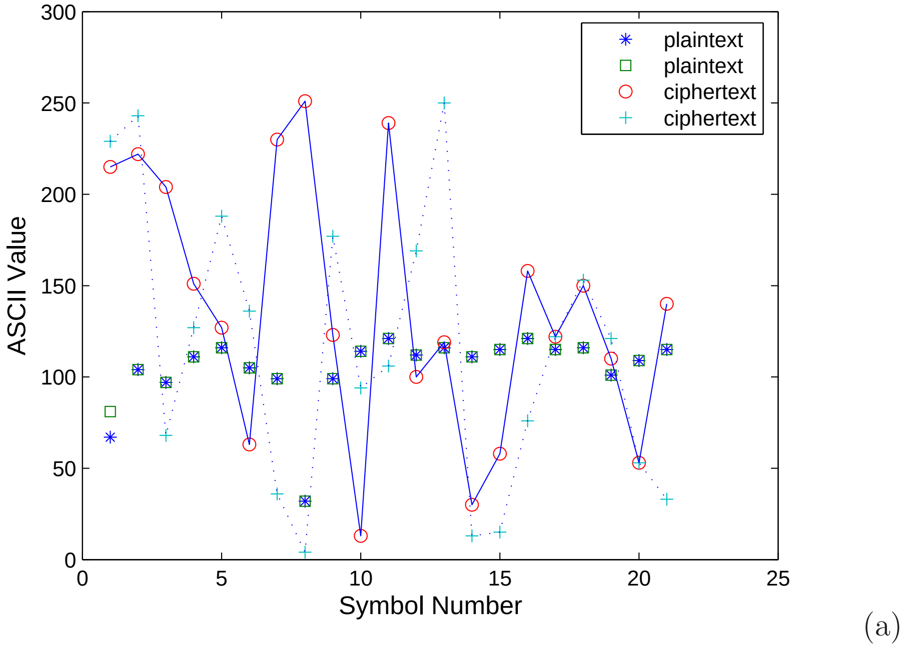
Step 3 (Decryption) At the receiver end, the same X_{new} can be generated by the discrete chaotic system in step 4′), once r is estimated. Then P_i is obtained through (4.11).

Remark 7: In the classical parameter modulation method, the parameter p has two states corresponding to ‘1’ or ‘0’ of the plaintext. This method only transmits one bit when synchronization is achieved. Compared with the classical parameter modulation scheme, σ_1 has more choices in the modified parameter modulation scheme. The plaintext P_i is a block of 8 bits, thus this scheme also can transmit more information. In addition, as pointed out in Section 3.6, the parameters σ_1 and ρ are unidentifiable if $\sigma_1 \neq \sigma_2$. Hence they are secure against parameter identification techniques.

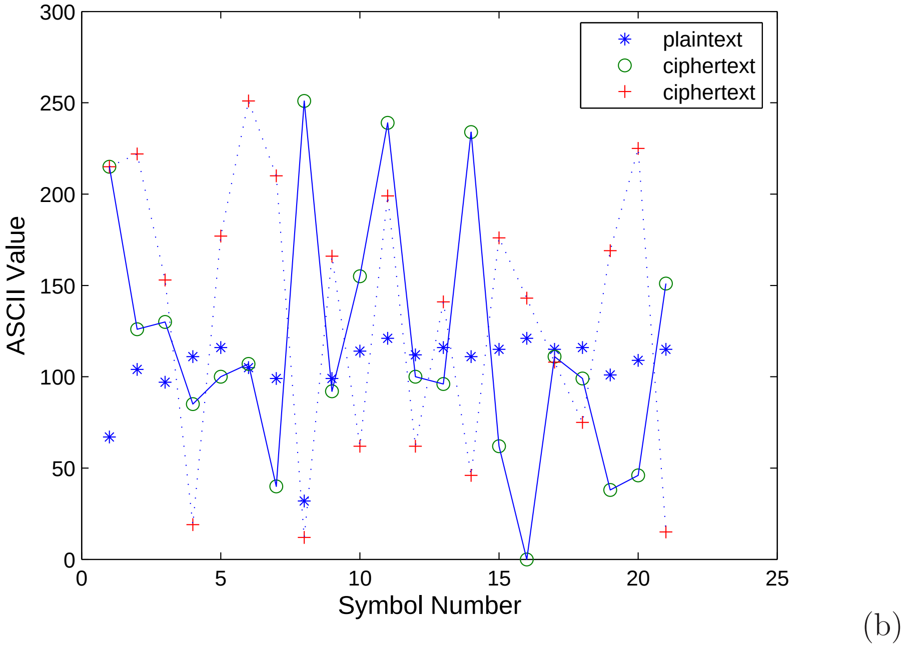
4.2.3 Security analysis with simulation results

Before the efficiency of the modified parameter modulation scheme is illustrated, numerical simulations first show the security of the cryptosystem. In [18], it is mentioned that a good cryptosystem should be sensitive with respect to the plaintext and the secret key, and can map a given plaintext to a random ciphertext. These points are shown through simulation as done in [18]. In the simulation let $M = 2^{10}$. Figure 4.1a) shows the cryptosystem is sensitive to the plaintext. The specific plaintexts chosen are 'Chaotic cryptosystem' and 'Qhaotic cryptosystem'. The 128-bits secret key is 'wh91-qa9g-k*xd/.'. This figure shows that the ciphertexts are completely different although the plaintexts only have one different character. Figure 4.1b) shows the plaintext 'Chaotic cryptosystem' and its ciphertexts using two different keys 'wh91-qa9g-k*xd/.' and 'wh91-q9ag-k*xd/.'. Figure 4.2a) shows the ASCII value distribution of plaintext of approximate 3 000 characters generated randomly. The distribution is in the interval $[97, 122]$. Figure 4.2b) shows the distribution of the corresponding ciphertext of Figure 4.2a). The distribution is almost uniform in the complete interval of ASCII values $[0, 255]$. Hence the cryptosystem maps the plaintext to a random ciphertext. Without the structure and parameters of the cryptosystem, the opponents cannot recover the plaintext, even if they can estimate the parameter σ_1. Hence it improves the security of the parameter.

Now one uses system (5.2) to transfer the plaintext 'Chaotic cryptosystem' with the secret key 'wh91-qa9g-k*xd/.'. Figure 4.3a) is the ASCII value of the plaintext and the corresponding ciphertext. Figure 4.3b) is the estimated value of the ciphertext C_i, which is obtained by the adaptive observer introduced in [51]. The initial conditions of state variables and estimated state variables $\hat{x}$ are [0.1 0.2 0.3] and [0.4 0.5 0.6], respectively. The initial conditions of estimated parameters $\hat{p}$ and $\hat{r}$ are both 1. As for the other variables in the observer, $S_x(0) = I$, $S_\theta(0) = I$ and $\Lambda(0) = [10\ 10\ \ldots\ 10]$. As a comparison, a classical parameter modulation scheme is used to transfer a bit sequence [44], which is plotted in Figure 4.4a). In order to investigate the security of the modified



(a)



(b)

Figure 4.1: ASCII value for plaintexts and the corresponding ciphertexts (connected by lines), (a) using the same secret key; (b) using two different keys.

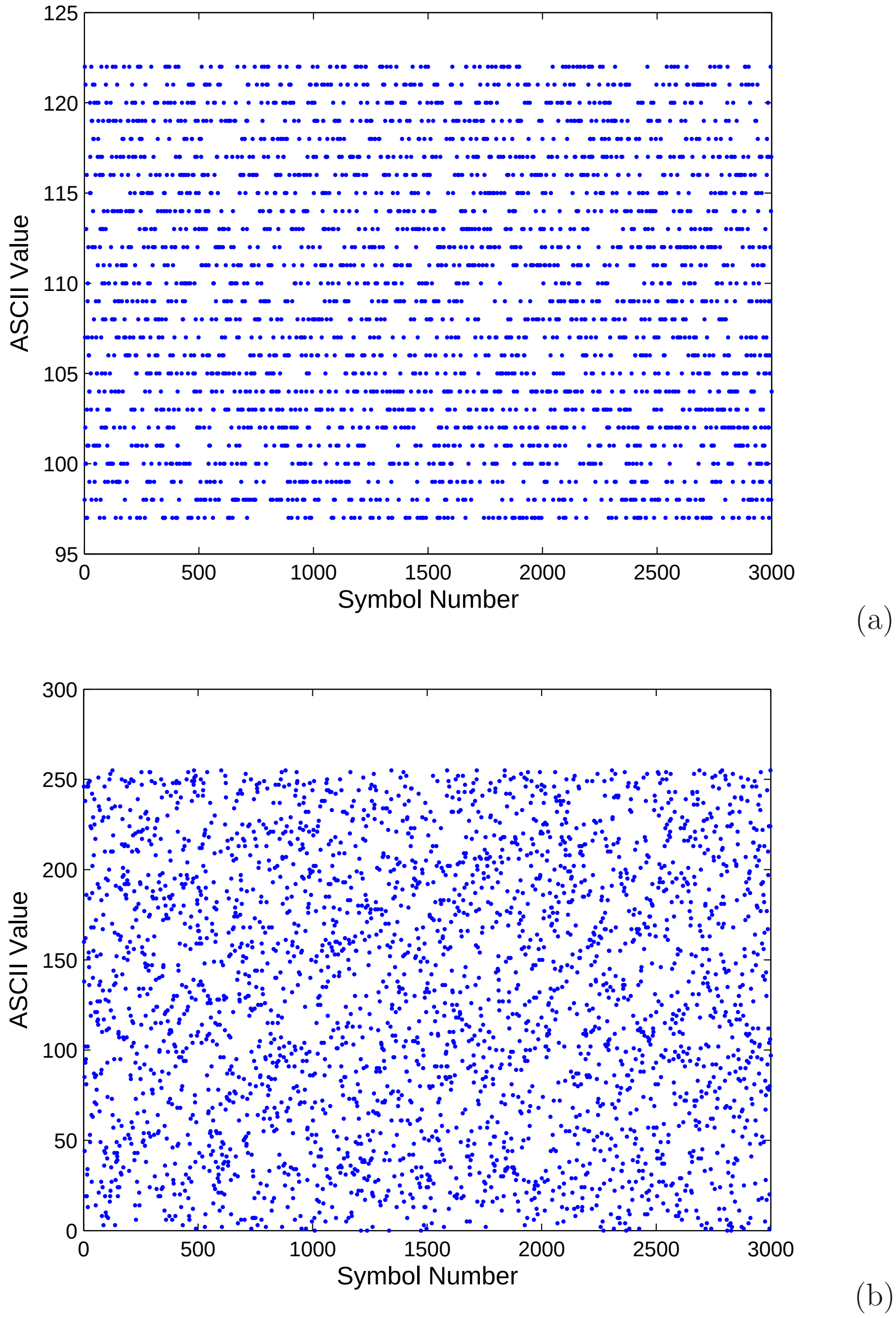
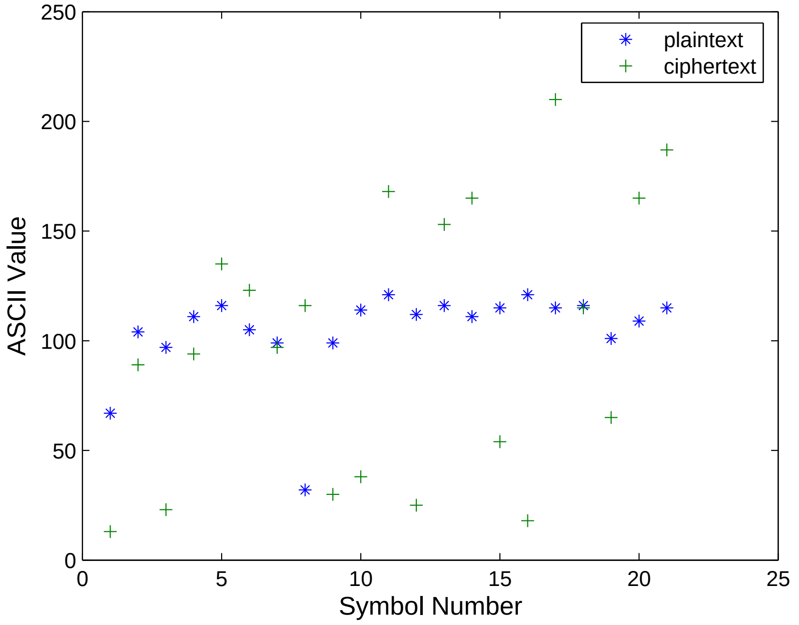
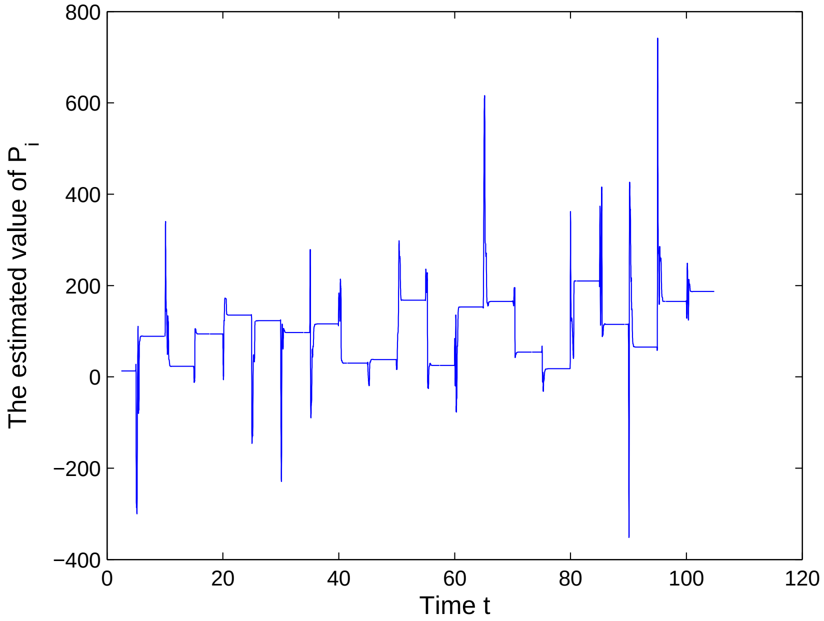


Figure 4.2: (a) The distribution of plaintext; (b) the distribution of ciphertext.

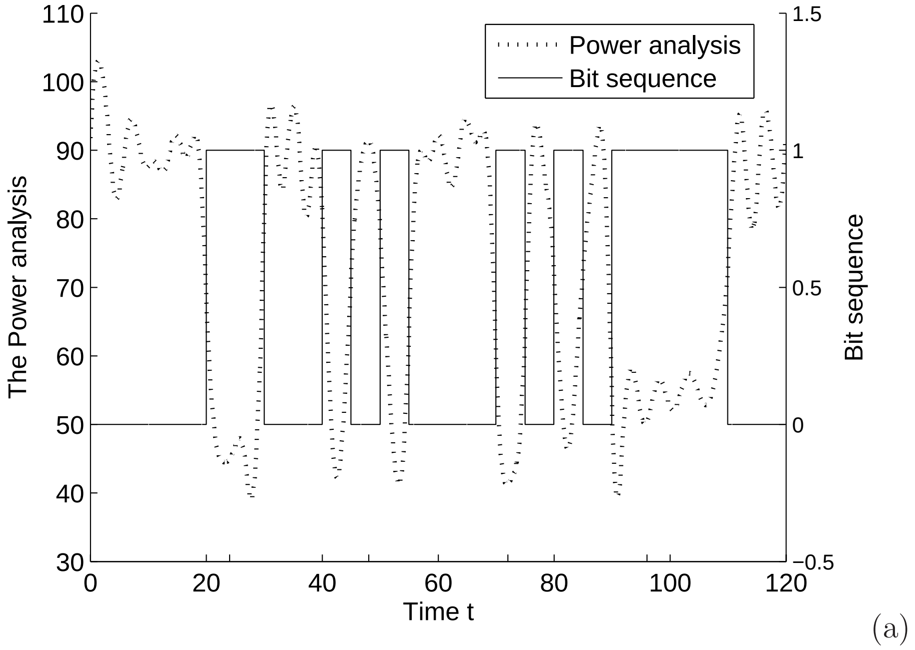


(a)

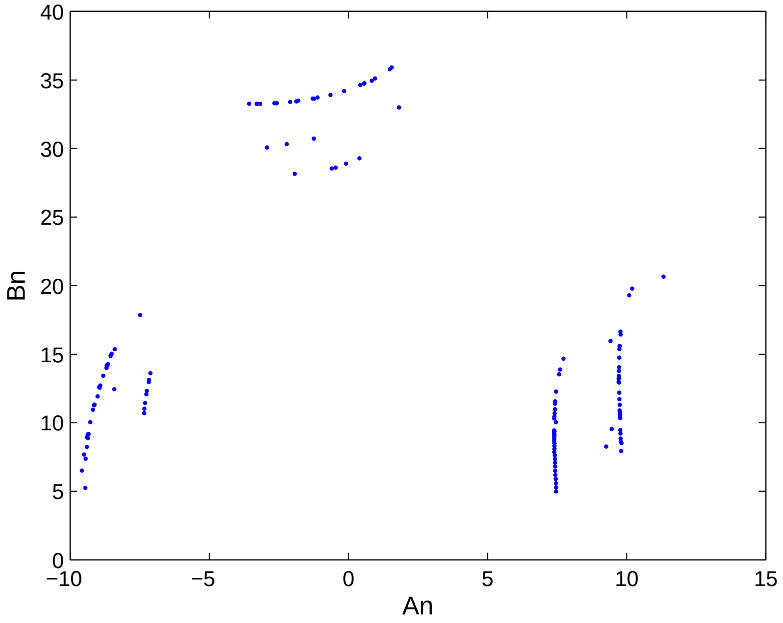


(b)

Figure 4.3: (a) The ASCII value of plaintext and the corresponding ciphertext; (b) the estimated value of P_i.

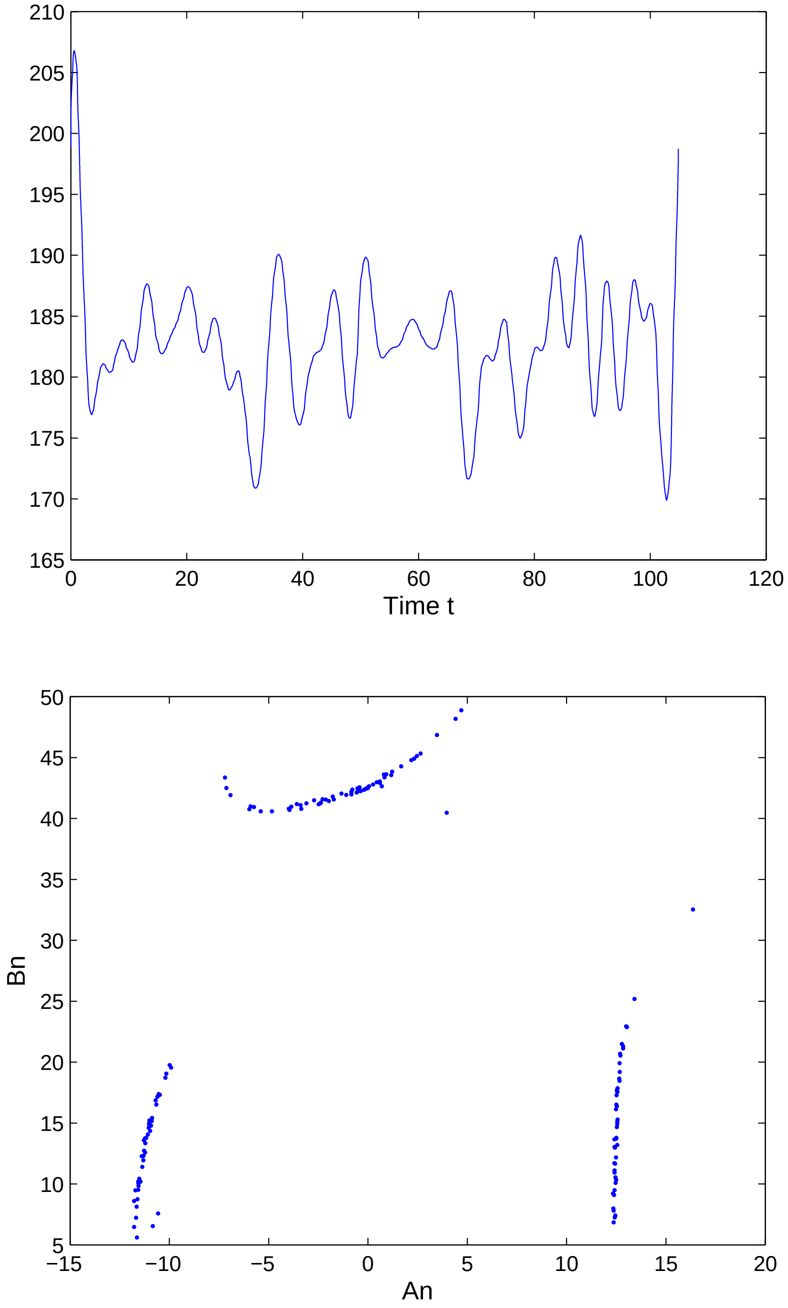


(a)



(b)

Figure 4.4: For the transmitted signal generated by the classical parameter modulation, a) bit sequence and the result of power analysis, b) return map.



(a)

(b)

Figure 4.5: For the transmitted signal generated by the proposed method, a) the result of power analysis, b) return map.

parameter modulation scheme, two popular attacks developed in [29, 28] are considered, that is, power analysis attack and return map attack. For the transmitted signal generated by the classical parameter modulation scheme, the results of two attacks are plotted in Figure 4.4. When the transmitted signal is generated by the modified parameter modulation scheme, the corresponding result is plotted in Figure 4.5. The power analysis attack first filters the transmitted signal by a low-pass filter, and then recovers the plaintext utilizing a binary quantizer. Figure 4.4a) plots the bit sequence and the result of power analysis for the classical parameter modulation scheme. Figure 4.5a) is the result of power analysis for the modified parameter modulation scheme. Compared with Figure 4.4a), it is obvious that the attacker cannot recover the binary sequence '1' or '0' from Figure 4.5a). As described by Perez and Cerdeira [28], a small change in the parameters of the sender affects the attractor of the chaotic system. Hence, a modified return map (A_n, B_n) is defined by $A_n = \dfrac{X_n + Y_n}{2}$, and $B_n = X_n - Y_n$, where X_n and Y_n are the n-th local maximum and minimum of the transmitted signal, respectively. In Figure 4.4b), the plot of the return map shows that all the segments are divided into two parts. Figure 4.5b) shows that all the segments merge together for different parameter. Then the attacker cannot distinguish the parameter variations. Hence, the above two attack methods are ineffective in the modified parameter modulation scheme.

4.3 Robustness of the encryption algorithm with Δ-modulated feedback control system

There is always parameter uncertainty in the practical implementation of the chaos-based communication scheme. For example, there is unavoidable error when the chaotic map is executed by a computer, because the real number is represented by a binary bits sequence of finite length in digital computers. Therefore it is natural to consider the effect of the uncertainty or error during the implementation of a chaos-based communication scheme. It has been reported in [79, 80] that errors could result in serious problems, such as short cycle length or nonideal distribution and correlation function, when a chaotic system is implemented discretely in finite computing precision. The influence of the finite computing precision on security is also studied in [30, 31].

In Section 4.2 a modified parameter modulation communication scheme is presented, where the cryptosystem based on a discretized chaotic map is an important component. In this section, the robustness of the cryptosystem against error is studied. In this thesis, robustness means that the cryptosystem works properly under errors or uncertainties within a certain range. This property is desirable because error will make the chaotic orbits stray from the theoretical ones completely [32]. A subsequent problem is that of what the upper bound of the error is if the cryptosystem is robust.

Before discussing the above problem, the following symbols are defined.

Definition 4: 1) $\lfloor x \rfloor$, floor function, is the maximal integer not greater than x;

2) $\mathrm{frac}(x) := x - \lfloor x \rfloor$;

3) $\mathrm{round}(x)$, round-off function, is the nearest integer of x;

4) $r(x) := x - \mathrm{round}(x)$.

A discretized Δ-modulated feedback control system is defined as

$$x_{j+1} = F_a(x_j) := \begin{cases} \dfrac{\mathrm{round}(Max_j)}{M} - 1, & x_j \geq 0, \\ \dfrac{\mathrm{round}(Max_j)}{M} + 1, & x_j < 0, \end{cases} \tag{4.9}$$

where $a \in [\sqrt{2}, 2]$. For any integer $k \geq 10$, x_j belongs to the set:

$$P = C = \{0, \pm\frac{1}{M}, \ldots, \pm\frac{M-1}{M}\}, \text{ where } M = 2^k. \tag{4.10}$$

The following step 4′) in the encryption algorithm, given in subsection 4.2.2, is considered in this section. The reason is that the encryption process and decryption process are executed in this step, and much attention are paid to the effect of the uncertainties on these processes.

4′) Let X_{new} be $F_{a_i}^N(X)$, where $F_{a_i}^N(X)$ is obtained by iterating F_{a_i} for N times at point X. Then define the encryption/decryption in the following way:

$$\begin{aligned} C_i &= (P_i + \lfloor X_{new}M \rfloor) \bmod 256, \text{ (encryption)}, \\ P_i &= (C_i + 256 - \lfloor X_{new}M \rfloor) \bmod 256, \text{ (decryption)}. \end{aligned} \tag{4.11}$$

Let $X'_{new} = X_{new} + e_{new}$, where e_{new} is the error. There are mainly two possible sources to generate e_{new}. One is an error of the parameter a, the other is an error of the initial value X. To ensure $C_i = C_i'$, it suffices to let $\lfloor X_{new}M \rfloor = \lfloor X_{new}'M \rfloor$, which is equivalent to

$$0 \leq \text{frac}(X_{new}M) + e_{new}M < 1. \tag{4.12}$$

The effect of errors of the parameter a and the initial value X is considered in the following subsections. The notation N is fixed to be the iteration number defined in step 4$'$) from now on.

4.3.1 The influence of initial value

For simplicity, let x_0 be the initial value and $x_0' = x_0 + e_0$, where e_0 is an error. Then $Max_0' = \text{round}(Max_0) + r(Max_0) + Mae_0$ and

$$x_1' = F_a(x_0') = \frac{\text{round}(Max_0')}{M} - \text{sgn}(x_0') = F_a(x_0) + \frac{i_1}{M} + \text{sgn}(x_0) - \text{sgn}(x_0'),$$

where $i_1 = \text{round}(r(Max_0) + Mae_0)$. Let $x_1 = F_a(x_0)$, then

$$x_1' = \begin{cases} x_1, & \text{for } i_1 = 0 \text{ and } \text{sgn}(x_0) = \text{sgn}(x_0'), \\ x_1 + \frac{i_1}{M} + \text{sgn}(x_0) - \text{sgn}(x_0'), & \text{for } i_1 \neq 0 \;\text{ or }\; \text{sgn}(x_0) \neq \text{sgn}(x_0'). \end{cases} \tag{4.13}$$

According to the definition of the round-off function, i_1 does not equal 0 if $|r(Max_0) + Mae_0| \geq 0.5$. Let $e_1 = x_1' - x_1$, then

$$x_2' = \begin{cases} x_2, & \text{for } i_2 = 0 \text{ and } \text{sgn}(x_1) = \text{sgn}(x_1'), \\ x_2 + \frac{i_2}{M} + \text{sgn}(x_1) - \text{sgn}(x_1'), & \text{for } i_2 \neq 0 \;\text{ or }\; \text{sgn}(x_1) \neq \text{sgn}(x_1'), \end{cases} \tag{4.14}$$

where $i_2 = \text{round}(r(Max_1) + Mae_1)$ and $x_2 = F_a(x_1)$. Let $e_j = x_j' - x_j$ and $i_{j+1} = \text{round}(r(Max_j) + Mae_j)$, where $x_j = F_a^j(x_0)$ and $x_j' = F_a^j(x_0')$, $j \geq 1$. Then the following result is obtained:

Proposition 4.7: Assume that $|e_0| < 1/M$ and $|e_j| < (2M-1)/(aM)$, for all $j \geq 1$. If $M \geq 2^8$, $e_1 \neq 0$ and $x_0 \neq 0$, then $|e_j| \geq 1/M$ for all $j \geq 2$.

Proof: It follows from $x_0 \neq 0$ and $|e_0| < 1/M$ that $\text{sgn}(x_0) = \text{sgn}(x_0')$. By (4.13), one has $1/M \leq |e_1| = i_1/M \leq 3/M < (2M-1)/(aM)$. Therefore $6 \geq |Mae_1| \geq \sqrt{2}$. The proof proceeds by induction. When $j = 2$, $1 \leq |i_2| = |\text{round}(r(Max_1) + Mae_1)| \leq 8$. Obviously, $i_2 < 2M - 1$. If $\text{sgn}(x_1) = \text{sgn}(x_1')$, then $|e_2| = |i_2/M| \geq 1/M$. If $\text{sgn}(x_1) \neq \text{sgn}(x_1')$, then

$$|e_2| = |i_2/M + \text{sgn}(x_1) - \text{sgn}(x_1')| > 2 - i_2/M > 2 - (2M-1)/M = 1/M.$$

Assume that $|e_j| \geq 1/M$ for some $j \geq 2$. Then $0.5 < |r(Max_j) + Mae_j| < 2M - 0.5$ and $1 \leq |i_{j+1}| \leq 2M - 1$. Following a similar analysis to the case $j = 2$, it is obtained that $|e_{j+1}| \geq 1/M$. □

Corollary 4.8: Assume that $M \geq 2^8$, $|e_0| < 1/M$ and $|e_j| < (2M-1)/(aM)$, for all $1 \leq j < N$. If $x_0 \neq 0$, then $e_N = 0$ if and only if $e_1 = 0$.

Proof: If $e_1 = 0$, then

$$x'_j = F_a^j(x'_0) = F_a^{j-1}(F_a(x'_0)) = F_a^{j-1}(x'_1) = F_a^{j-1}(x_1) = F_a^j(x_0) = x_j$$

for all $j \geq 2$. Therefore $e_N = x'_N - x_N = 0$. If $e_N = 0$ and $e_1 \neq 0$, it contradicts with the conclusion of Proposition 4.7. Therefore it follows from $e_N = 0$ that $e_1 = 0$. □

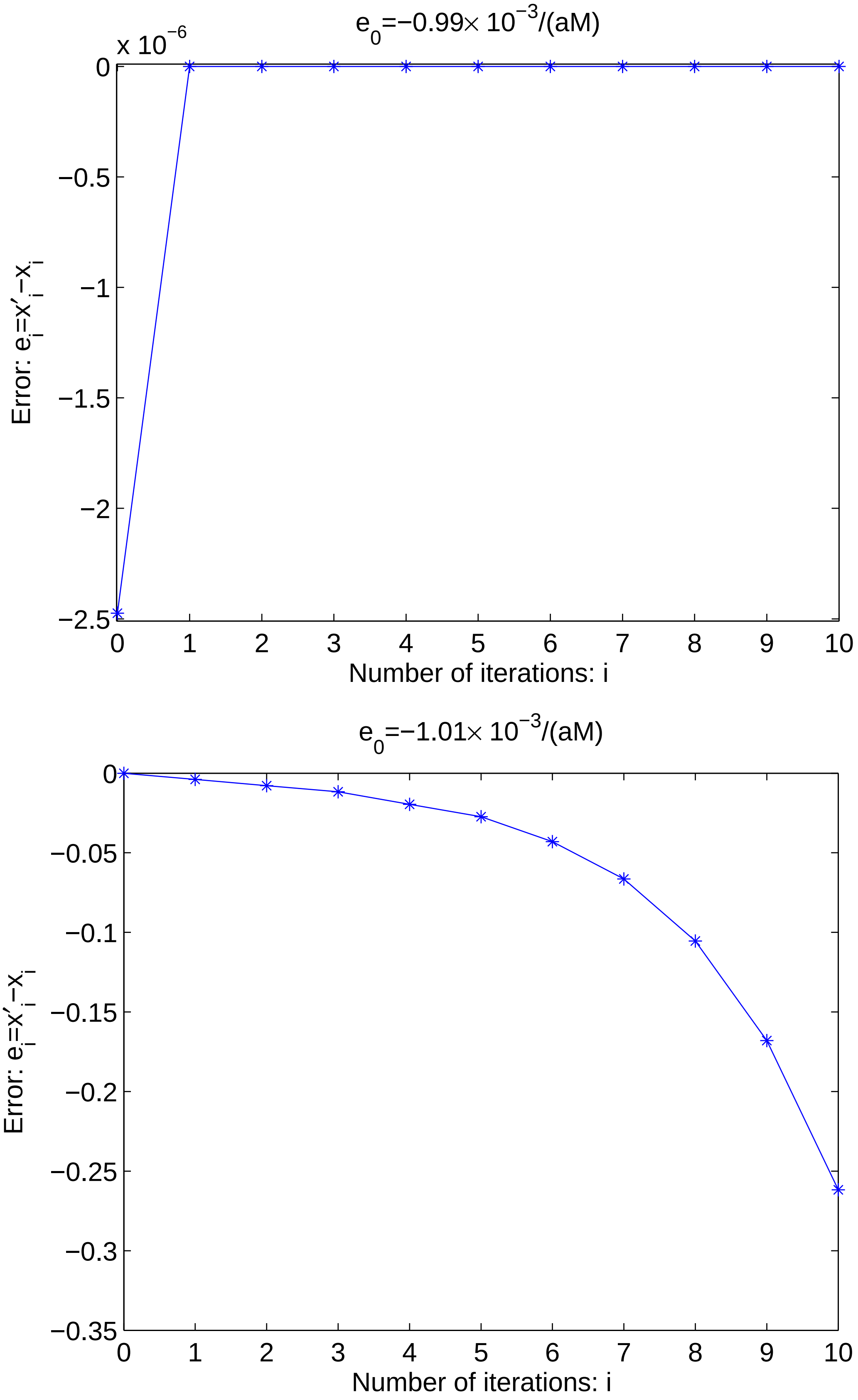
According to Corollary 4.8, $x'_1 = x_1$ guarantees $x'_N = x_N$. Proposition 4.7 and Corollary 4.8 imply that the initial error should be controlled at the second iteration, otherwise it will be transferred to the next iteration and accumulated such that the cryptosystem will not work properly. The following proposition gives an upper bound of e_0 to ensure $x_1 = x'_1$, and thus $x_N = x'_N$.

Proposition 4.9: Assume the parameter a equals $1 + \sum_{i=1}^{n_a} a^i 10^{-i}$, where n_a is a positive integer, $a_i \in \{0, 1, \ldots, 9\}$. If $|e_0| < 10^{-n_a}/(Ma)$ and $r(Max_0) \neq 0.5$, then $x_1 = x'_1$ for any nonzero initial value $x_0 \in P$, and thus $x_N = x'_N$.

Proof: Since $x_0 \in P$ and $|e_0| < 1/M$, $\text{sgn}(x_0) = \text{sgn}(x'_0)$ and Mx_0 is an integer. Hence $r(Max_0) = \sum_{i=1}^{n_a} c^i 10^{-i}$, where $c_i \in \{0, 1, \ldots, 9\}$. Then $\max_{x_0 \in P}(|r(Max_0)|) \leq 0.5 - 10^{-n_a}$. Therefore $|r(Max_0) + Mae_0)| \leq |r(Max_0)| + |Mae_0| < 0.5$. It follows from (4.13) that $x_1 = x'_1$. Then it follows from Corollary 4.8 that $x_N = x'_N$. □

The special case $r(Max_0) = 0.5$ is ignored because this case does not occur for most of the parameter values.

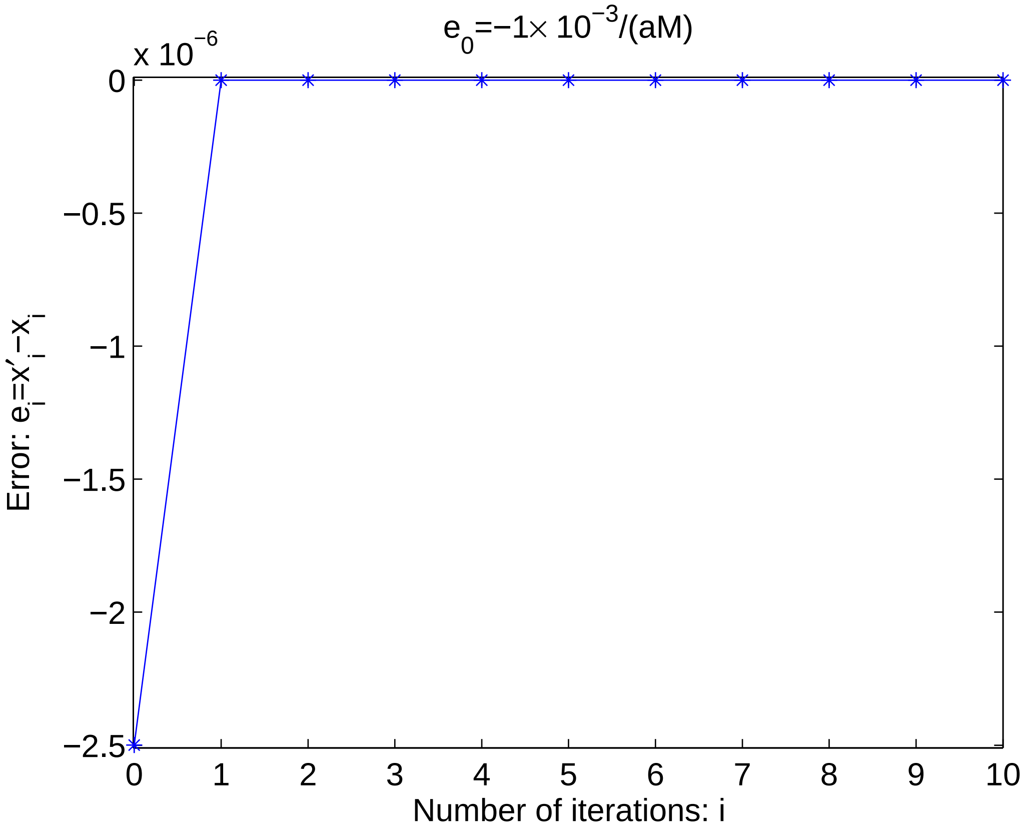
Example 4.3.1. Figure 4.6 and 4.7 plot the errors between the real value x_i and the corrupted value x'_i for different e_0. The X-axis is the number of iterations, and the Y-axis is $x'_i - x_i$. In the simulation, $a = 1.563$, $M = 256$, $x_0 = 127/M$, $n_a = 3$ and $i = 1, 2, \ldots, 10$. For any possible initial value $x_0 \in P$ defined in (4.10), $\max(|r(Max_0)|) = 0.499$. The error is $e_0 = -0.99 \times 10^{-3}/(aM)$ in Figure 4.6a). Figure 4.6b) shows that $x_i \neq x'_i$ when $e_0 = -1.01 \times 10^{-3}/(aM)$. In Figure 4.7 the error is $e_0 = -1 \times 10^{-3}/(aM)$. By Proposition 4.9, if $|e_0| < 10^{-n_a}/(Ma)$, then $x_i = x'_i$ for all $i \geq 1$, which is shown in



(a)

(b)

Figure 4.6: The error between x_i and x'_i for different e_0.



(c)

Figure 4.7: The error between x_i and x_i' when $e_0 = -1 \times 10^{-3}/(aM)$.

Figure 4.6a). For these fixed parameter value and initial value, Figure 4.6b) shows that it is possible to result in $x_i \neq x_i'$ even if the error e_0 is lightly larger than the bound, and Figure 4.7 shows that the conclusion of Proposition 4.9 still holds when $|e_0|$ equals $10^{-3}/(aM)$. Therefore the three figures show that the bound provided in Proposition 4.9 is sharp.

4.3.2 The influence of the parameter

Let $a' = a + e_a$, where e_a is the error. Then

$$x_1' = F_{a'}(x_0) = \frac{\text{round}(Ma'x_0)}{M} - \text{sgn}(x_0) = F_a(x_0) + \frac{k_1}{M},$$

where $k_1 = \text{round}(r(Max_0) + Me_a x_0)$. Hence

$$x_1' = \begin{cases} x_1, & \text{if } k_1 = 0, \\ x_1 + \frac{k_1}{M}, & \text{if } k_1 \neq 0, \end{cases} \tag{4.15}$$

where $x_1 = F_a(x_0)$. Obviously, when $|r(Max_0) + Me_a x_0| \geq 0.5$, $k_1 \neq 0$. Let $\epsilon_1 = x_1' - x_1 = k_1/M$, then

$$\begin{aligned} x_2' = F_{a'}(x_1') =& \frac{\text{round}(M(a+e_a)(x_1+\epsilon_1))}{M} - \text{sgn}(x_1') \\ =& \frac{\text{round}(Max_1)}{M} - \text{sgn}(x_1) + \frac{k_2}{M} + \text{sgn}(x_1) - \text{sgn}(x_1'), \end{aligned}$$

where $k_2 = \text{round}(r(Max_1) + Me_a x_1 + M(a+e_a)\epsilon_1)$. Let $x_2 = F_a(x_1)$, then

$$x_2' = \begin{cases} x_2, & \text{for } k_2 = 0 \text{ and } \text{sgn}(x_1) = \text{sgn}(x_1'), \\ x_2 + \frac{k_2}{M} + \text{sgn}(x_1) - \text{sgn}(x_1'), & \text{for } k_2 \neq 0 \ \text{ or } \ \text{sgn}(x_1) \neq \text{sgn}(x_1'). \end{cases} \tag{4.16}$$

Let $\epsilon_j = x_j' - x_j$ and $k_{j+1} = \text{round}(r(Max_j) + Me_a x_j + M(a+e_a)\epsilon_j)$, where $x_j = F_a^j(x_0)$, $x_j' = F_a^j(x_0')$, $j \geq 1$, $j \geq 0$ and $\epsilon_0 = 0$. A similar result to Proposition 4.7 is obtained, as below:

Proposition 4.10: Assume that $|e_a| < 1/(10M)$ and $|\epsilon_j| < (2M-1.1)/((a+0.1)M)$, $j \geq 1$. If $M \geq 2^8$, $\epsilon_1 \neq 0$ and $x_0 \neq 0$, then $|\epsilon_j| \geq 1/M$ for all $j \geq 2$.

Proof: It follows from $x_0 \neq 0$ and $|e_a| < 1/(10M)$ that $|\epsilon_1| = k_1/M = 1/M < (2M-1)/((a-0.1)M)$. In case $j = 2$,

$$1 \leq |k_2| = |\text{round}(r(Max_1) + Me_a x_1 + M(a+e_a)\epsilon_1)| \leq 3 < 2M - 1.$$

According to (4.16),

$$\epsilon_2 = \begin{cases} \frac{k_2}{M}, & \text{if } \operatorname{sgn}(x_1) = \operatorname{sgn}(x_1'), \\ \frac{k_2}{M} + \operatorname{sgn}(x_1) - \operatorname{sgn}(x_1'), & \text{if } \operatorname{sgn}(x_1) \neq \operatorname{sgn}(x_1'). \end{cases} \tag{4.17}$$

Because

$$|k_2/M + \operatorname{sgn}(x_1) - \operatorname{sgn}(x_1')| \geq 2 - k_2/M > 1/M$$

and $k_2 \geq 1$, one has $|\epsilon_2| \geq 1/M$. Suppose that $|\epsilon_j| > 1/M$ for some integer $j \geq 2$, then

$$0.5 < |r(Max_j) + Me_a x_j + M(a + e_a)\epsilon_j| < (2M - 1.1) + 0.5 + 0.1 = 2M - 0.5.$$

Hence $1/M \leq |k_{j+1}| \leq 2M - 1$. Following a similar analysis to the case $j = 2$, it is obtained that $|\epsilon_{j+1}| \geq 1/M$. □

Corollary 4.11: Assume that $M \geq 2^8$, $|e_a| < 1/(10M)$ and $|\epsilon_j| < (2M - 1.1)/((a + 0.1)M)$, $1 \leq j \leq N$. If $x_0 \neq 0$ and $x_N = x_N'$, then $x_i = x_i'$ for all $i < N$.

Note that there is the error e_a in each iteration, thus $\epsilon_1 = 0$ is a necessary condition for ϵ_N=0, which is different from Corollary 4.8. A sufficient condition to ensure $x_N = x_N'$ is

$$k_j = 0 \text{ and } \operatorname{sgn}(x_{j-1}) = \operatorname{sgn}(x_{j-1}'),\ 1 \leq j \leq N, \tag{4.18}$$

that is, $x_j' = x_j,\ 1 \leq j \leq (N - 1)$. The condition $k_j = 0$ is equivalent to $|r(Max_j) + Me_a x_j| < 0.5$. Since $|r(Max_j)| < 0.5$, sufficiently small e_a can be found to satisfy the above condition. Similar to the proof of Proposition 4.9, the following result is obtained:

Proposition 4.12: Assume that parameter a equals $1 + \sum_{i=1}^{n_a} a^i 10^{-i}$, where n_a is a positive integer, $a_i \in \{0, 1, \ldots, 9\}$. If $|e_a| < 10^{-n_a}/M$ and $r(Max_0) \neq 0.5$, then $x_1 = x_1'$ for any nonzero initial value $x_0 \in P$. Hence it is obtained that $x_N = x_N'$ if $x_i \neq 0$, and $r(Max_i) \neq 0.5$ for all $i < N$.

Ensuring $x_N = x_N'$ needs all $r(Max_i) \neq 0.5$, $i < N$, which is different from Proposition 4.9. The reason is that the error e_a is in every iteration step. In addition, it is possible that $x_1 = x_1'$ when $|e_a| = 10^{-n_a}/M$, because $|x_0| < 1$ for most of $x_0 \in P$. Combining Corollary 4.11 and Proposition 4.12 together, the following sufficient and necessary condition is obvious:

Corollary 4.13: Assume that parameter a equals $1 + \sum_{i=1}^{n_a} a^i 10^{-i}$ and $n_a \geq 1$, where n_a is a positive integer, $a_i \in \{0, 1, \ldots, 9\}$. If $|e_a| < 10^{-n_a}/M$, $|\epsilon_j| < (2M -$

$1.1)/((a+0.1)M)$, $x_i \neq 0$ and $r(Max_i) \neq 0.5$ for all $i < N$, then $x_N = x'_N$ if and only if $x_1 = x'_1$.

Corollary 4.13 can be treated as a special case of the last subsection, that is, each value x_i is treated as an initial value, and the initial error e_0 is generated by e_a. Hence the cryptosystem can work well if the condition in Proposition 4.9 holds in every iteration step.

Example 4.3.2. The figures in Figure 4.8 plot the errors between the real value x_i and the corrupted value x'_i for different e_a. The X-axis is the number of iterations, and the Y-axis is $x'_i - x_i$. The parameters M and i are the same as those in Example 4.3.1; the other parameters are $a = 1.751$, $x_0 = 251/M$. The error e_a equals $-10^{-3}/M$ and $-1.02 \times 10^{-3}/M$ in Figure 4.8a) and 4.8b), respectively. Figure 4.8a) shows that the conclusion of Proposition 4.12 still holds when e_a equals the bound given in Proposition 4.12. If e_a does not satisfy the condition in Proposition 4.12, it is possible that $x_i \neq x'_i$. These two figures show that the bound in Proposition 4.12 is quite tight.

4.3.3 The influence of both e_0 and e_a

Let $a' = a + e_a$ and $x'_0 = x_0 + e_0$, where e_a is the error of the parameter, e_0 is the error of the initial value. Then

$$\begin{aligned} x'_1 = F_{a'}(x'_0) =& \frac{\text{round}(M(a+e_a)(x_0+e_0))}{M} - \text{sgn}(x'_0) \\ =& \frac{\text{round}(Max_0)}{M} - \text{sgn}(x_0) + \frac{\eta_1}{M} + \text{sgn}(x_0) - \text{sgn}(x'_0), \end{aligned}$$

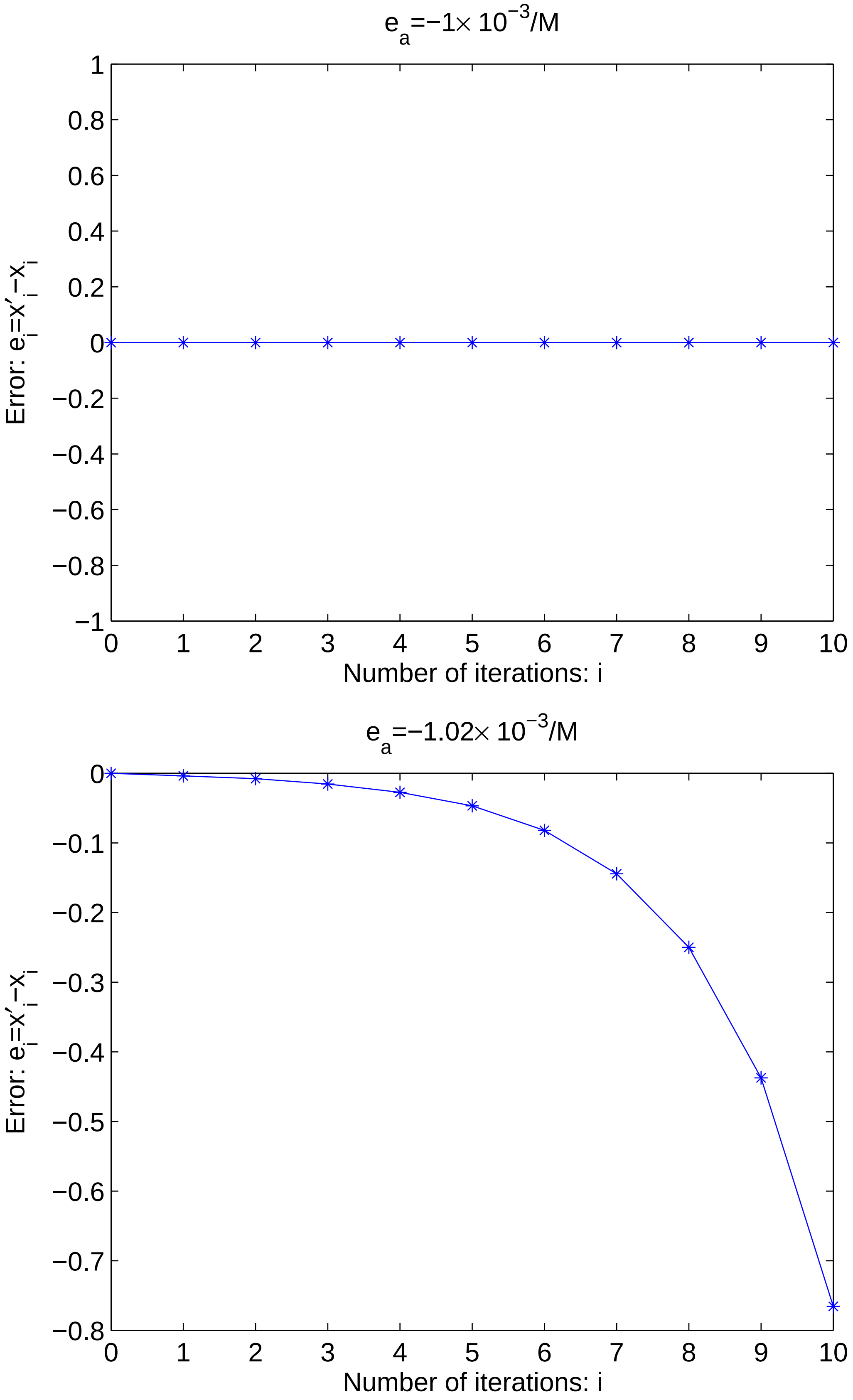
where $\eta_1 = \text{round}(r(Max_0) + Me_a x_0 + M(a+e_a)e_0)$. Hence

$$x'_1 = \begin{cases} x_1, & \eta_1 = 0 \text{ and } \text{sgn}(x_1) = \text{sgn}(x'_1), \\ x_1 + \frac{\eta_1}{M} + \text{sgn}(x_0) - \text{sgn}(x'_0), & \eta_1 \neq 0 \text{ and } \text{sgn}(x_1) = \text{sgn}(x'_1), \end{cases} \tag{4.19}$$

where $x_1 = F_a(x_0)$. Obviously, $\eta_1 \neq 0$ if and only if $|r(Max_0) + Me_a x_0 + M(a+e_a)e_0| \neq 0.5$. Let $\theta_j = x'_j - x_j$ and $\eta_{j+1} = \text{round}(r(Max_j) + Me_a x_j + M(a+e_a)\theta_j)$, where $x_j = F_a^j(x_0)$, $x'_j = F_{a'}^j(x'_0)$, $j \geq 1$, then

$$x'_{j+1} = \begin{cases} x_{j+1}, & \eta_{j+1} = 0 \text{ and } \text{sgn}(x_j) = \text{sgn}(x'_j), \\ x_{j+1} + \frac{\eta_{j+1}}{M} + \text{sgn}(x_j) - \text{sgn}(x'_j), & \eta_{j+1} \neq 0 \quad \text{or} \quad \text{sgn}(x_j) \neq \text{sgn}(x'_j). \end{cases} \tag{4.20}$$

Similar to the analysis in subsections 4.3.1 and 4.3.2, the following results are obtained.



(a)

(b)

Figure 4.8: The error between x_i and x'_i for different e_a.

Proposition 4.14: Assume that $|e_a| < 1/(10M)$, $|\theta_0| < 1/M$, and $|\theta_j| < (2M - 1.1)/((a+0.1)M)$, $j \geq 1$. If $M \geq 2^8$, $\theta_1 \neq 0$ and $x_0 \neq 0$, then $|\theta_j| \geq 1/M$ for all $j \geq 2$.

Proposition 4.15: Assume that parameter a equals $1 + \sum_{i=1}^{n_a} a^i 10^{-i}$, where n_a is a positive integer, $a_i \in \{0, 1, \ldots, 9\}$. If $r(Max_0) \neq 0.5$, $|e_a| < 10^{-n_a}/M$ and $|e_a x_0 + (a + e_a)e_0| < 10^{-n_a}/M$, then $x_1 = x_1'$ for any nonzero initial value $x_0 \in P$. Hence it is obtained that $x_N = x_N'$ if $x_i \neq 0$ and $r(Max_i) \neq 0.5$ for all $i < N$.

Proof: It follows from $x_0 \in P$ and $|e_0| < 1/M$ that $\text{sgn}(x_0) = \text{sgn}(x_0')$. Since Mx_0 is an integer, then $r(Max_0) = \sum_{i=1}^{n_a} c^i 10^{-i}$, where $c_i \in \{0, 1, \ldots, 9\}$. That is, $\max_{x_0 \in P}(|r(Max_0)|) \leq 0.5 - 10^{-n_a}$. Therefore

$$|r(Max_0) + Me_a x_0 + M(a + e_a)e_0| \leq |r(Max_0)| + |Me_a x_0 + M(a + e_a)e_0| < 0.5.$$

It means $\eta_1 = 0$. According to (4.19), one has $x_1 = x_1'$. Then it follows from Proposition 4.12 that $x_N = x_N'$. □

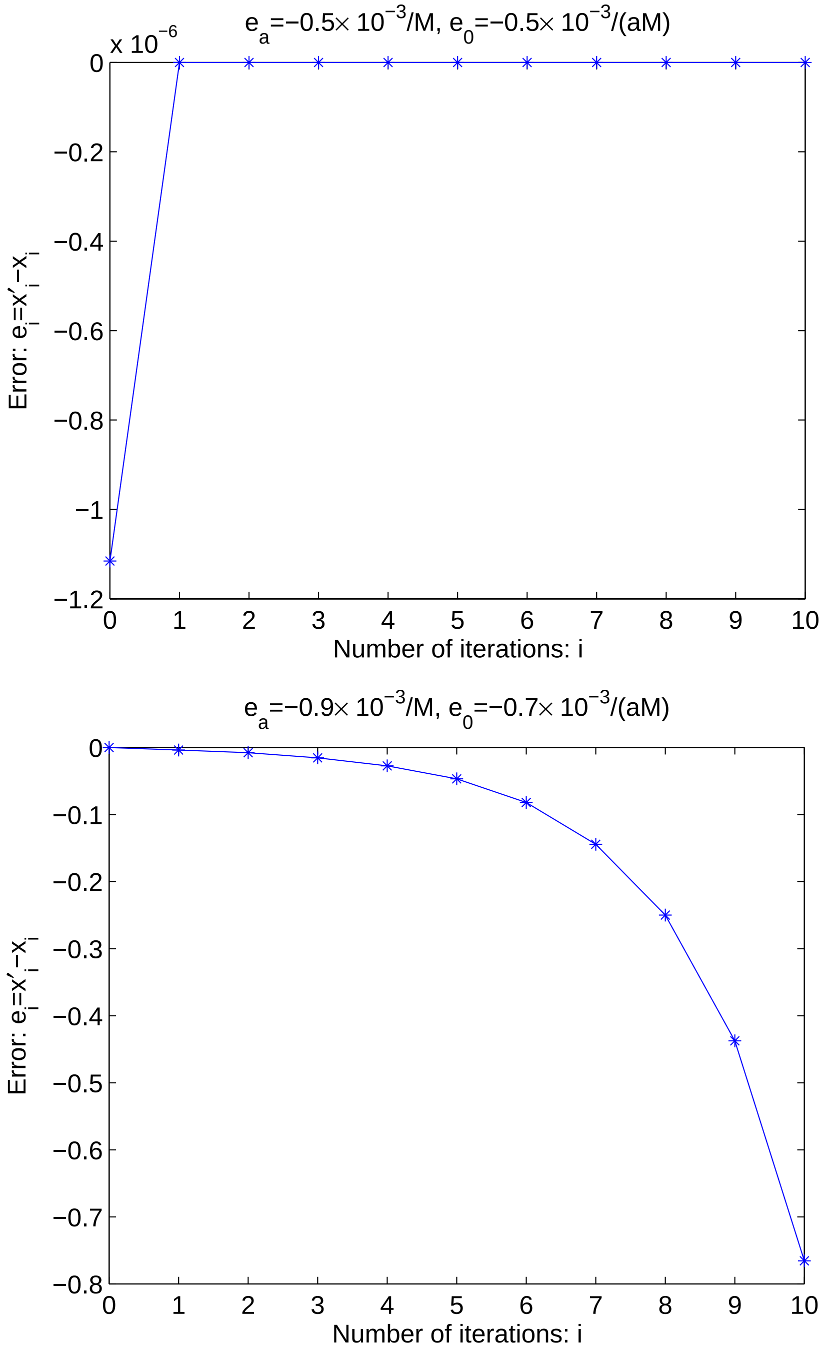
Unlike the previous two cases, the errors e_0 and e_a affect the first iteration step simultaneously. Hence η_1 is more complex than i_1 and k_1, and this additional condition $|e_a x_0 + (a + e_a)e_0| < 10^{-n_a}/M$ is needed to ensure $x_1 = x_1'$.

Example 4.3.3. The figures in Figure 4.9 plot the errors between the real value x_i and the corrupted value x_i'. The X-axis is the number of iterations, and the Y-axis is $x_i' - x_i$. The parameters M, i, a and x_0 are the same as those in Example 4.3.2. The errors e_a and e_0 equal $-0.5 \times 10^{-3}/M$ and $-0.5 \times 10^{-3}/(aM)$ in Figure 4.9a), respectively. In Figure 4.9b), $e_a = -0.9 \times 10^{-3}/M$, and $e_0 = -0.7 \times 10^{-3}/(aM)$. In Figure 4.9b), $\theta_i = x_i' - x_i \neq 0$ because the condition $|e_a x_0 + (a + e_a)e_0| < 10^{-n_a}/M$ is violated, although e_0 and e_a are smaller than the bound given in Proposition 4.9 and Proposition 4.12. Hence this condition is important in Proposition 4.15.

4.3.4 Selecting the appropriate parameter to improve the robust property

In the encryption algorithm in [81], parameter a is generated in Step 3′) by

3′) Let $a_i = \big((bY_i + c) \bmod m\big)/200 + 1.42$, where $Y_i = (bY_{i-1} + c) \bmod m$, $b = 16, c = 7, m = 96$, and $Y_1 = 0$.



(a)

(b)

Figure 4.9: The error between x_i and x_i': a) $e_a = -0.5 \times 10^{-3}/M$, $e_0 = -0.5 \times 10^{-3}/(aM)$, b) $e_a = -0.9 \times 10^{-3}/M$, $e_0 = -0.7 \times 10^{-3}/(aM)$.

Step $3'$) generates different a_i corresponding to different P_i, which makes P_i more secure. However, there is an interesting paradox between robustness and security in chaotic communications. For different P_i, the algorithm is more robust if all the parameters $a_i's$ are the same. According to the proof of Proposition 4.9, $|e_0| < 1/M$ and $|r(Max_0) + Mae_0| < 0.5$ ensure that $x_1 = x_1'$ for a fixed parameter a. In order to keep the algorithm robust under the different parameter a_i, $1 \leq i \leq N$, the following inequality should be satisfied,

$$|e_0| < \min_{1\leq i\leq N, x_0\in P} \left(\frac{0.5 - r(Ma_ix_0)}{a_iM} \right) = \min_{1\leq i\leq N} \left(\frac{0.5 - \max_{x_0\in P}(r(Ma_ix_0))}{a_iM} \right). \tag{4.21}$$

When estimating the bound of e_a in Proposition 4.12 for different parameter a_i, the following inequality

$$|e_a| < \frac{0.5 - \max_{1\leq i\leq N, x_0\in P}(r(Ma_ix_0))}{M} < \min_{1\leq i\leq N, x_0\in P} \left(\frac{0.5 - r(Ma_ix_0)}{x_0M} \right) \tag{4.22}$$

should be satisfied to ensure that (4.18) holds. Hence the bound of e_a or e_0 can only be the smallest value so that the algorithm is robust under the different parameter a_i. Since security is still guaranteed by the secret key, step $3'$) is replaced by setting $a_1 = a_2 = \ldots = a_N = a$. That is, the same a is selected to generate x_{new} for a different P_i. This method has two advantages. The first advantage is to exclude the case $\max_{x_0\in P}(|r(Max_0)|) = 0.5$, so that Proposition 4.10 and Proposition 4.12 can be applied. For example, if $a_i = 1.55$ for some i and the initial value $x_0 = 10/M$, then $r(Ma_ix_0) = 0.5$. Hence Proposition 4.10 and Proposition 4.12 are not applicable. The second advantage is that e_0 or e_a has a larger bound than that in Proposition 4.9 or Proposition 4.12. For example, let $M = 256$, $a_1 = 1.561$, $a_2 = 1.563$, $a_3 = 1.567$, according to (4.21) and (4.22),

$$\begin{aligned} |e_0| &< \min\left\{ \frac{0.5 - 0.494}{1.561M}, \frac{0.5 - 0.499}{1.563M}, \frac{0.5 - 0.497}{1.567M} \right\} = \frac{1 \times 10^{-3}}{1.563M}, \\ |e_a| &< \min\left\{ \frac{0.5 - 0.494}{M}, \frac{0.5 - 0.499}{M}, \frac{0.5 - 0.497}{M} \right\} = \frac{1 \times 10^{-3}}{M}. \end{aligned} \tag{4.23}$$

However if $a_1 = a_2 = a_3 = a = 1.561$, then $|e_0| < 6 \times 10^{-3}/(1.561M)$ and $|e_a| < 6 \times 10^{-3}/M$. Obviously, these bounds are larger than those in Proposition 4.9 and Proposition 4.12.

Example 4.3.4. Let $a = 1.561$, $M = 256$, $n = 10$. When $e_0 = 4 \times 10^{-3}/(aM)$ and $x_0 = 127/256$, Figure 4.10a) plots the errors between the real value x_i and the corrupted value x_i'. When $e_a = -4 \times 10^{-3}/M$ and $x_0 = 227/256$, Figure 4.10b) plots the errors between the real value x_i and the corrupted value x'_i. When $a_1 = 1.561$, $a_2 = 1.563$, $a_3 = 1.567$, (4.23) shows that the upper bounds of the errors e_0 and e_a are $1 \times 10^{-3}/(1.563M)$ and $1 \times 10^{-3}/M$, respectively. Obviously, these two errors are smaller than those in this example.

4.4 Summary and conclusion

In this chapter a modified parameter modulation scheme, combined with a cryptographic technique, is proposed to improve security, and the robustness of this scheme against uncertainty is investigated both analytically and experimentally. As a theoretical basis of the proposed communication scheme, a particular one-dimensional discrete system controlled by a Δ-modulated feedback is proved to be chaotic when the parameter a is in $(\sqrt{2}, 2]$. This chaotic map is used to construct a secure cryptosystem, which generates the parameter in the communication scheme. The complex parameter-generating process improves the security of the communication scheme greatly, and numerical simulation shows that the two popular attacks, power analysis attack and return map attack, are ineffective in the modified parameter modulation scheme. Uncertain perturbations are unavoidable in practical implementation of communication schemes. The robustness of the cryptosystem is considered when there are uncertainties in initial condition and system parameter. The upper bounds of the uncertainty are also given to ensure that the iterations of the chaotic map do not stray from real values.

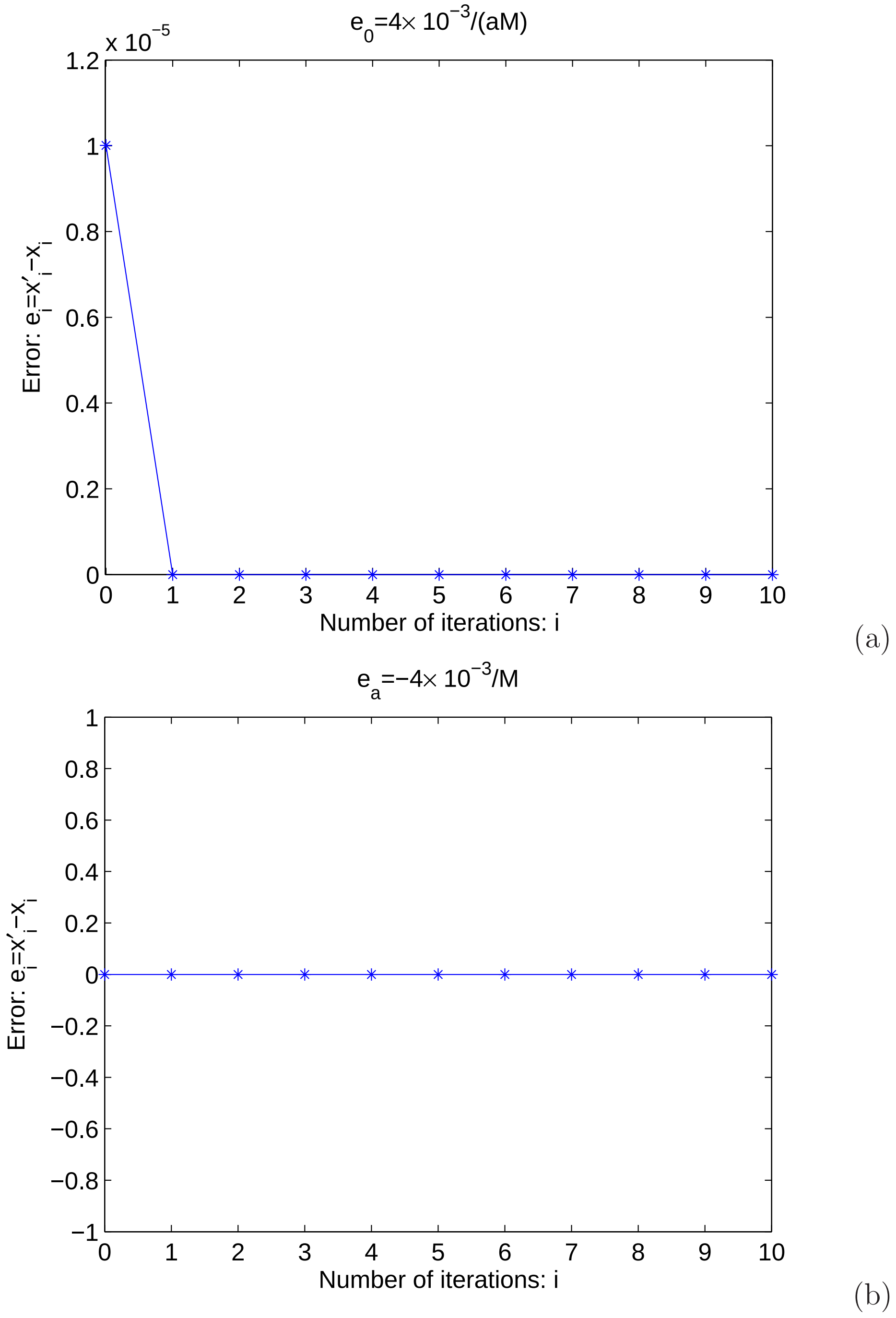


Figure 4.10: The error between x_i and x_i', (a) $e_0 = 4\times10^{-4}/(aM)$; (b) $e_a = 4\times10^{-3}/M$.

Chapter 5

Application of chaotic synchronization in CDMA

5.1 Chapter outline

In this chapter the results in Section 3.6 and Section 4.2 are applied to a direct sequence code-division-multiple-access (DS-CDMA) scheme. The motivation and contribution of this application are given in next section. Section 5.3 introduces the structure of the DS-CDMA scheme. Numerical simulations given in Section 5.4 show that the bit error rate (BER) performance of this scheme is good, even if there is noise in the transmission channel. Section 5.5is the summary and conclusion.

5.2 Introduction

In the past few years, owing to rapid growth of the internet market and a tremendous increase in the demand for wireless services, code-division-multiple-access (CDMA) systems, more generally, spread spectrum signals, have been applied in several existing wireless networks across the world, such as third-generation (3G) cellular systems and wireless local area networks. In a CDMA scheme, all the users transmitted the information simultaneously. A number of different transmitted signals occupy the whole system bandwidth. At the receiver end, code sequences are used to separate different users [82]. Many researchers on spread spectrum communications for wireless personal and computer networks have addressed the CDMA system with the direct sequences approach, where all users transmit on the same band at the same time and are distinguished only by means of a code signature. CDMA is also a promising technique to improve the capacity of the current digital cellular system [83, 84]. In mobile communication systems, multiple access to the common channel resources is vital. CDMA has been selected as the main multiple access technology for 3G wireless systems. The primary digital standards for cell phones in the United States are time-division-multiple-access (TDMA), CDMA, and global system mobile (GSM) [85]. DS-CDMA is a spread spectrum multiple access communication method that is expected to gain a significant share of the cellular market [84].

Owing to its broadband power spectra and quickly decaying correlation functions, chaotic signal is chosen as the spreading signal in the direct sequence spread spectrum communications and has found interesting application in CDMA mobile communications, which contributes to several improvements in communication security and noise elimination. The generation of chaotic spreading sequences and synchronization of chaotic spreading sequences are two important issues in the chaotic CDMA system [86]. Reference [2] is the first work which studies the synchronization of chaotic systems and suggests its application to secure communication. Mutually orthogonal chaotic sequences are generated and applied to spreading spectrum multi-users communication in [87] and [88].

In this chapter the results in Section 3.6 and Section 4.2 are applied to a DS-CDMA scheme. To improve security, an encryption/decryption function introduced in Section 4.2 is employed in the transmitter/receiver, and an unidentifiable parameter of the chaotic system is chosen as one of the secret keys. The generation of spreading sequences is very important to increase the spectrum's efficiency in a multi-user CDMA system. Most chaos-based CDMA schemes use a chaotic map to generate spreading sequences. In this chapter, a continuous chaotic system is employed and the local extrema are chosen from the output of this system to generate spreading sequences. By means of these spreading sequences, numerical simulations show that the DS-CDMA scheme has a good performance, although the improvement of security degrades the BER performance.

5.3 A chaos-based DS-CDMA scheme

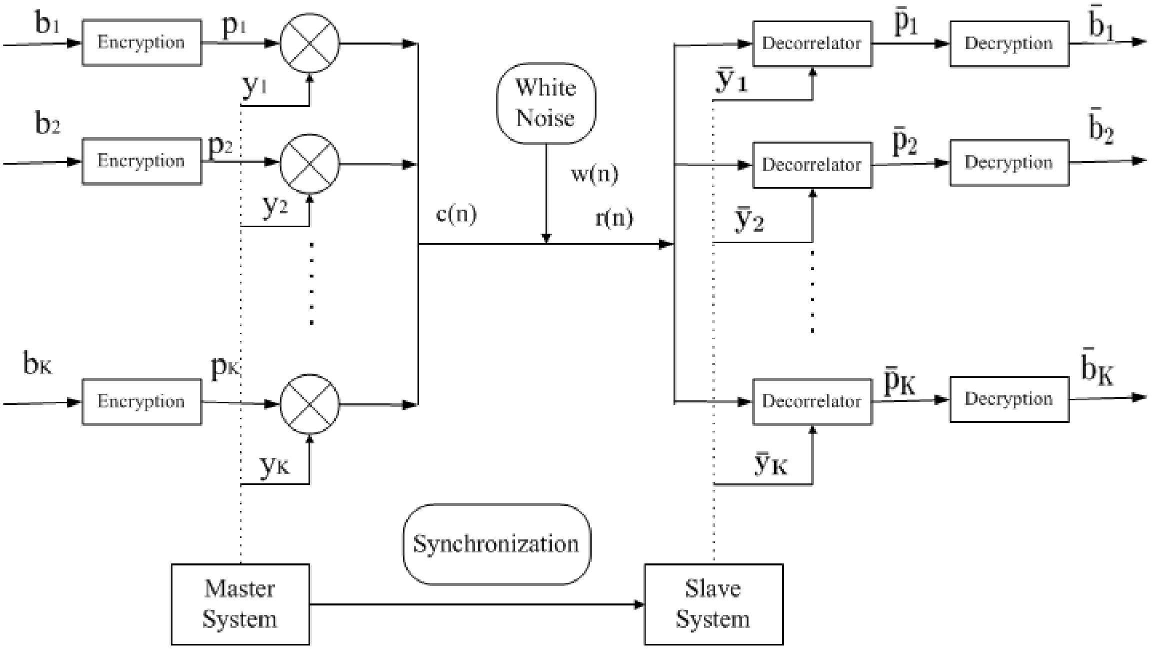


Figure 5.1: The DS-CDMA model.

The structure of the DS-CDMA scheme based on chaotic synchronization is illustrated in Figure 5.1. Generally, chaotic synchronization consists of two parts: the master system and the slave system. The master system sends a driving signal such that the state of the slave system can track the state of the master system. In this scheme the master system generates K spreading sequences $\{y_1(n)\}_{n=1}^N$, $\{y_2(n)\}_{n=1}^N$, $\ldots$, $\{y_K(n)\}_{n=1}^N$. The synchronization in Figure 5.1 means that the signals $\bar{y}_i$ are produced by the slave system such that $\lim_{t\to\infty} \|y_i - \bar{y}_i\| = 0$. Let $E(y_i) = 0$ and $\|y_i\| = 1$, then the autocorrelation function between y_i and y_j is defined as [89]

$$C_{ij} = \sum_{n=1}^{N} \frac{(y_i(n) - E(y_i))((y_j(n) - E(y_j))}{\| y_i \|\| y_j \|} = \sum_{n=1}^{N} y_i(n) y_j(n),$$

where $E(y_i)$ is the mean value of the sequence y_i. These sequences y_i have the following properties:

$$C_{ii} = 1, C_{ij,i\neq j} = \varepsilon_{ij} \approx 0, \quad i,j = 1,2,\ldots,K, \tag{5.1}$$

where the $\varepsilon_{ij}'s$ are sufficiently small positive numbers.

User k sends the information signal b_k, which is encrypted to produce p_k. The elements of b_k and p_k are 1 or -1. The chaotic spreading sequence y_k is multiplied by

p_k. Then the products are summed up to produce signal $c(n)$, which is transmitted through the channel. That is, $c(n) = \sum_{k=1}^{K} p_k y_k(n)$, $n = 1 \ldots N$, where N is the length of the spreading sequences, K is the total number of users. The received signal $r(n) = w(n) + c(n)$, where $w(n)$ is the white noise. For receiver i, the recovery is done by the multiplication of $r(n)$ and $y_i(n)$,

$$\begin{aligned} r_i &= \sum_{n=1}^{N} r(n) y_i(n) = \sum_{n=1}^{N} \Big(\sum_{k=1}^{K} p_k y_k(n) + w(n) \Big) y_i(n) \\ &= \sum_{n=1}^{N} p_i y_i(n) y_i(n) + \Big(\sum_{k=1, k\neq i}^{K} \sum_{n=1}^{N} y_k(n) y_i(n) + \sum_{n=1}^{N} w(n) y_i(n) \Big) = \bar{r}_i + r_e, \end{aligned}$$

where $\bar{r}_i = \sum_{n=1}^{N} p_i y_i(n) y_i(n)$. The decoding information is given

$$\bar{p}_i = \operatorname{sgn}(r_i) = \begin{cases} 1, & \text{if} \quad r_i \geq 0, \\ -1, & \text{if} \quad r_i < 0. \end{cases}$$

If r_e is sufficiently small, the decoding information recovers the accurate binary bit p_i. Hence the success of this detector depends on the amplitude of the noise and the correlations between spreading sequences.

The following Lorenz system is chosen as the master system and generates a series of chaotic sequences such that condition (5.1) is satisfied,

$$\begin{cases} \dot{x}_1 &= -\sigma_1 x_1 + \sigma_2 x_2, \\ \dot{x}_2 &= \rho x_1 - x_2 - x_1 x_3, \\ \dot{x}_3 &= x_1 x_2 - \beta x_3, \\ y &= x_1. \end{cases} \tag{5.2}$$

The output is x_1, which is transmitted to the slave system through the synchronization channel. It should be noted that $\sigma_1 \neq \sigma_2$. In this case, the result in Section 3.6 shows that σ_1 is not identifiable if x_1 is the output. The local maximums of x_2 produce a discrete sequence $\{\tilde{x}\}$, whose i-th element $\tilde{x}(i)$ is the i-th local maximum of x_2. A series of subsequences $\tilde{x}^i$ are defined in the following way:

$$\tilde{x}^1(n) = \tilde{x}(n),\ \tilde{x}^2(n) = \tilde{x}(n+\tau_1),\ \ldots,\ \tilde{x}^K(n) = \tilde{x}(n + \textstyle\sum_{k=1}^{K} \tau_k), \quad n = 1, 2, \ldots, N,$$

where τ_k is the positive integer and $N + \sum_{k=1}^{K} \tau_k$ is less than the length of $\tilde{x}$. The new sequences $\{y_i\}$, $i = 1, 2, \ldots, K$, are obtained from normalized $\tilde{x}^i$,

$$y_i(n) = \frac{\tilde{x}^i(n) - E(\tilde{x}^i)}{\|\tilde{x}^i - E(\tilde{x}^i)\|},$$

where $E(\tilde{x}^i)$ is the mean value of $\tilde{x}^i$. Then it follows that $E(y_i) = 0$ and $\|y_i\| = 1$. When $K = 10$, Figure 5.2 plots C_{1j} and C_{2j}, $j = 1, \ldots, 10$. Figure 5.3 plots the autocorrelation functions C_{1j} and C_{2j} for $K = 20$. The smaller the $C'_{ij}s$ are, the closer the autocorrelation functions become to ideal. The larger N and τ_i are, the smaller the $C'_{ij}s$ are.

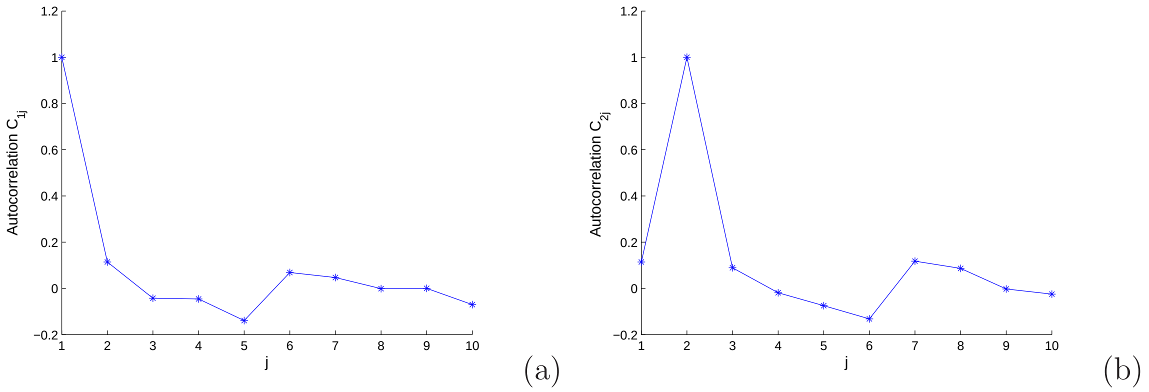


Figure 5.2: The autocorrelation function between y_i and y_j when $K = 10$, (a) $i = 1$ and $j = 1, 2, \ldots, 10$, (b) $i = 2$ and $j = 1, 2, \ldots, 10$.

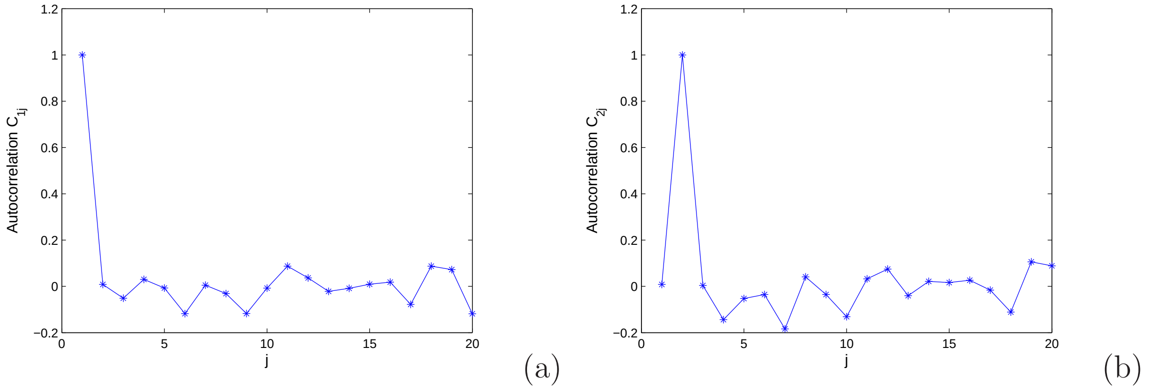


Figure 5.3: The autocorrelation function between y_i and y_j when $K = 20$, (a) $i = 1$ and $j = 1, 2, \ldots, 20$, (b) $i = 2$ and $j = 1, 2, \ldots, 20$.

The encryption and decryption in Figure 5.1 are carried out in the algorithm proposed in Section 4.2. Step 2 and Step 5 are considered mainly.

2) Choose a K_r randomly from $\{K_1, \ldots, K_{16}\}$, and let $X = (X_s + \frac{K_r}{M}) \bmod 1$ and $N = N_s + K_r$, where $x \bmod 1 = x - \lfloor x \rfloor$, and $\lfloor x \rfloor$ is the floor (also called truncation) function.

5) Choose the symbols corresponding to the ASCII values of C_i/P_i obtained in

Step 4) as the ciphertext/plaintext. If $i = n$, then stop the algorithm, otherwise let $X_s := X_{new}$, $N_s := C_i$ and $i := i + 1$, and go to Step 2.

To apply this algorithm in the DS-CDMA scheme, Step 5) needs some modification,

5') Put the symbols corresponding to the ASCII values of C_i/P_i obtained in Step 4) as the ciphertext/plaintext. If $i = n$, then stop the algorithm, otherwise let $N_s := C_i$ and $i := i + 1$, and go to Step 2.

That is, the variable X_s does not change in Step 5'). The reason is that the influence of one symbol on the ciphertext in the decryption process is spread over many plaintext symbols. For example, let the 128-bits secret key K ='wh91-qa9g-k*xd/.', a ciphertext $C = [170\ 161\ 69\ 252\ 176]$, then the corresponding plaintext $P = [243\ 59\ 155\ 124\ 228]$ if K_r choose K_5 in every decryption process. Let $C_1 = [171\ 161\ 69\ 252\ 176]$, then the corresponding plaintext $P_1 = [244\ 68\ 133\ 74\ 145]$. The plaintexts P and P_1 are completely different although only the first characters of the ciphertexts are different. Hence it will worsen the performance of the BER in the CDMA scheme. This modification is a trade-off between security and BER performance. In addition, all the users choose the same K_r in Step 2. The index r of K_r is transmitted through modulating the parameter σ_1 in system (5.2), that is, $\sigma_1 = 10 + r/16$. It is easy to estimate the parameter σ_1 and the state variables simultaneously by the slave system [38]. However, it cannot estimate σ_1 without knowledge of parameter ρ. Hence the parameter σ_1 is secure.

5.4 Numerical simulation

Now numerical simulation is carried on to evaluate the BER performance of the CDMA scheme illustrated in Figure 5.1. The following two definitions are needed in simulation. The signal to noise ratio (SNR) is defined as [90, 91]

$$\mathrm{SNR} = 10 \log_{10} \frac{\sum\limits_{n=1}^{N} \left((c(n) - E(c)\right)^2}{\sum\limits_{n=1}^{N} w^2(n)},$$

where $E(c)$ is the mean value of the transmitted signal c, and the mean value of the noise $w(n)$ is zero. The BER is defined as [92, 93]

$$\text{BER} = 0.5P(b(t) = 1|\bar{b}(t) = -1) + 0.5P(b(t) = -1|\bar{b}(t) = 1).$$

In practical implementations, it is not possible to maintain orthogonal codes for all users, and thus multiple access interference arises. Successive interference cancellation and parallel interference cancellation schemes are two simple methods to reduce multiple access interference, therefore they are frequently used to improve the performance of BER [90]. In the simulation we use the successive interference cancellation proposed in [94].

In the simulation, subsection 5.4.1 is a standard image transmission. The performance of BER is presented through transmitting 2^{13} random data. In order to consider the influence of synchronization on the BER performance, the simulation is carried on in two subsections 5.4.2 and 5.4.3 for the case of the synchronization channel with noise and without noise, respectively. A comparison between the proposed scheme illustrated in Figure 1 and another two CDMA schemes is presented in subsection 5.4.4.

5.4.1 Image transmission in an AWGN channel

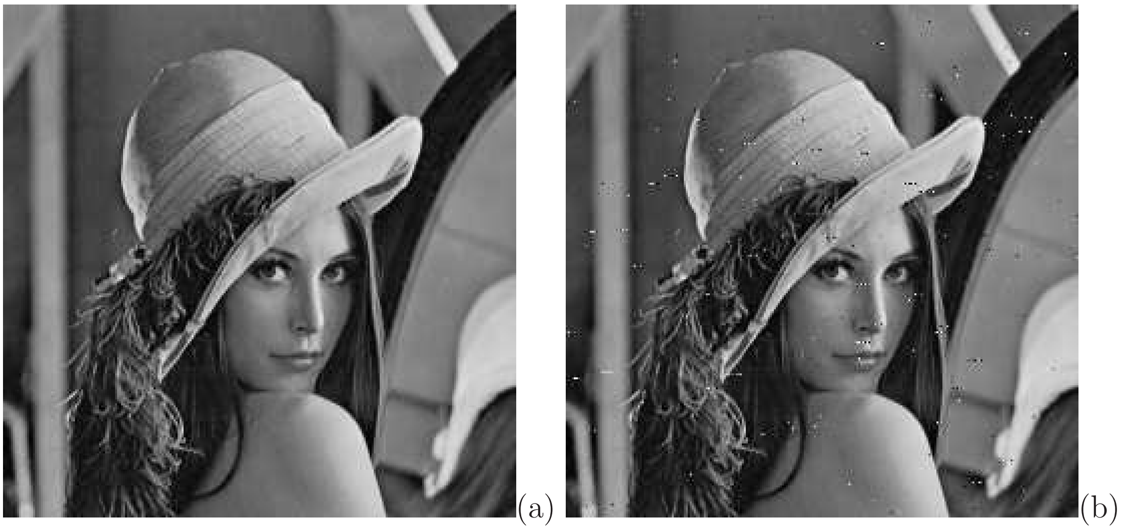


Figure 5.4: The standard Lena (256 × 256) image, a) original, b) recovered.

Since multimedia signals are the main information sources in wireless network applications, a standard image is transmitted by the first user through an additive white gaussian noise (AWGN) channel with SNR= 5. The number of users is $K = 20$. Figure 5.4a) is the original image, and 5.4b) is the corresponding recovered image. Comparing the two figures reveals that the original image is almost recovered even if there is strong noise in the transmission channel, which shows that this scheme is robust to channel noise.

5.4.2 BER performance with perfect synchronization

Perfect synchronization means that the synchronization channel is not corrupted by noise. To evaluate the statistical performance of the proposed scheme, 2^{13} binary data are generated randomly. In Figure 5.5 and 5.6, the length of spreading sequences is $N = 64$. Figure 5.5 shows that the reduction in the BER is in relation to the increase in SNR, where the number of users K equals 20 and 25, respectively. By assuming that the highest acceptable level of BER equals 10^{-3} [95], it can be observed that the performance is satisfactory when the SNR is greater than 5. Figure 5.6 plots the performance of the BER when the number of users $K = 30$, 35 and 40. The level of noise SNR ranges from -10 to 20. These figures show that the performance of the BER becomes worse when the number of users increases. The performance is satisfactory when the SNR is greater than 10. Figure 5.7 plots the performance of the BER when the length of spreading sequences N equals 128. In order to investigate the influence of the encryption algorithm on the BER performance, all these figures include two lines. One line is the performance of the BER without the encryption/decryption process. The other is the performance of the BER with the encryption/decryption process. One ciphertext block influences not only the corresponding plaintext block, but also the next block. Hence the improvement of security degrades the performance of the BER. Figure 5.8 compares the BER performance when the length of spreading sequences is $N = 64$ and $N = 128$, respectively. These figures show that the longer the length, the better the BER performance is.

5.4.3 BER performance with synchronization error

In this case, the synchronization channel is corrupted by noise. For the master system, the output is the first state of system (5.2), that is, x_1. For the slave system, the input is $x_1 + a\sin(60t)$, where a is a positive real number. The performance of BER

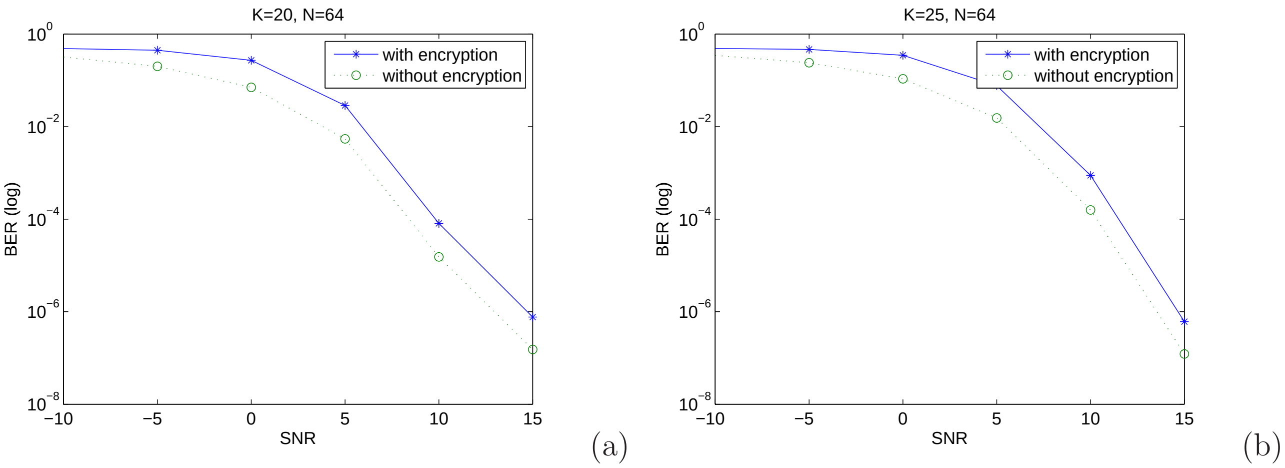


Figure 5.5: BER vs SNR, a) K=20, b) K=25.

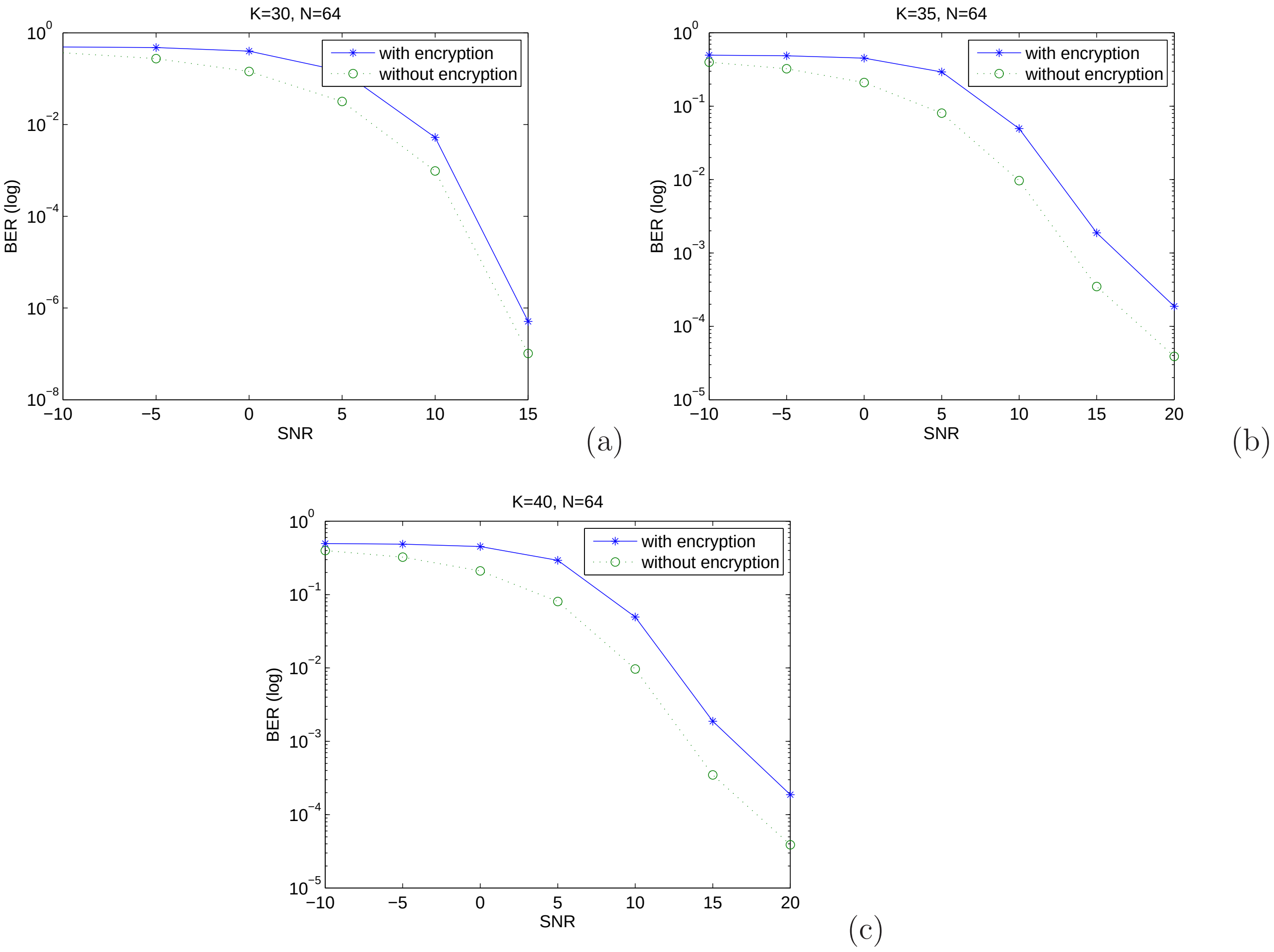
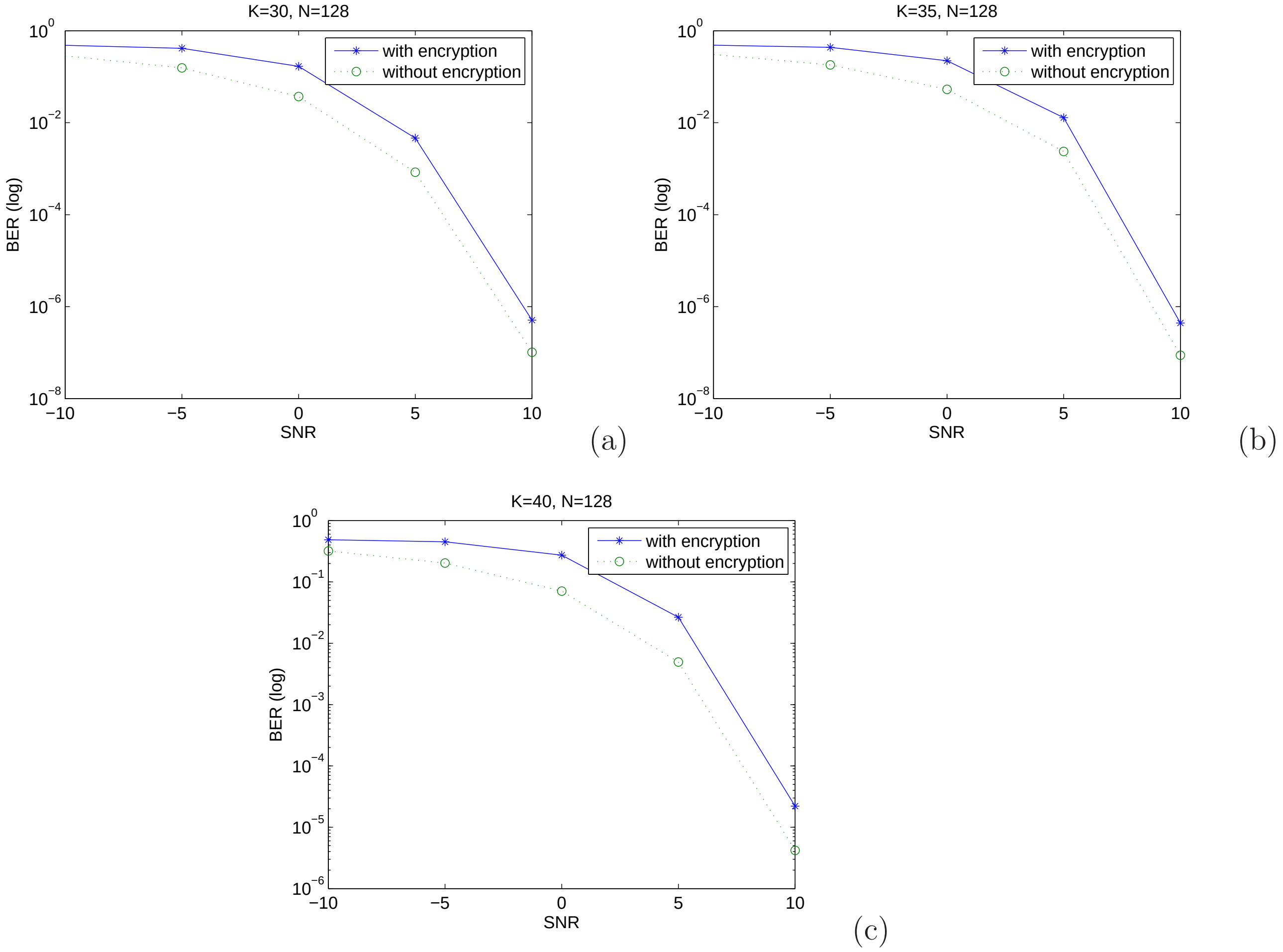


Figure 5.6: BER vs SNR, a) K=30, b) K=35, c) K=40.



(a)

(b)

(c)

Figure 5.7: BER vs SNR, a) K=30, b) K=35, c) K=40.

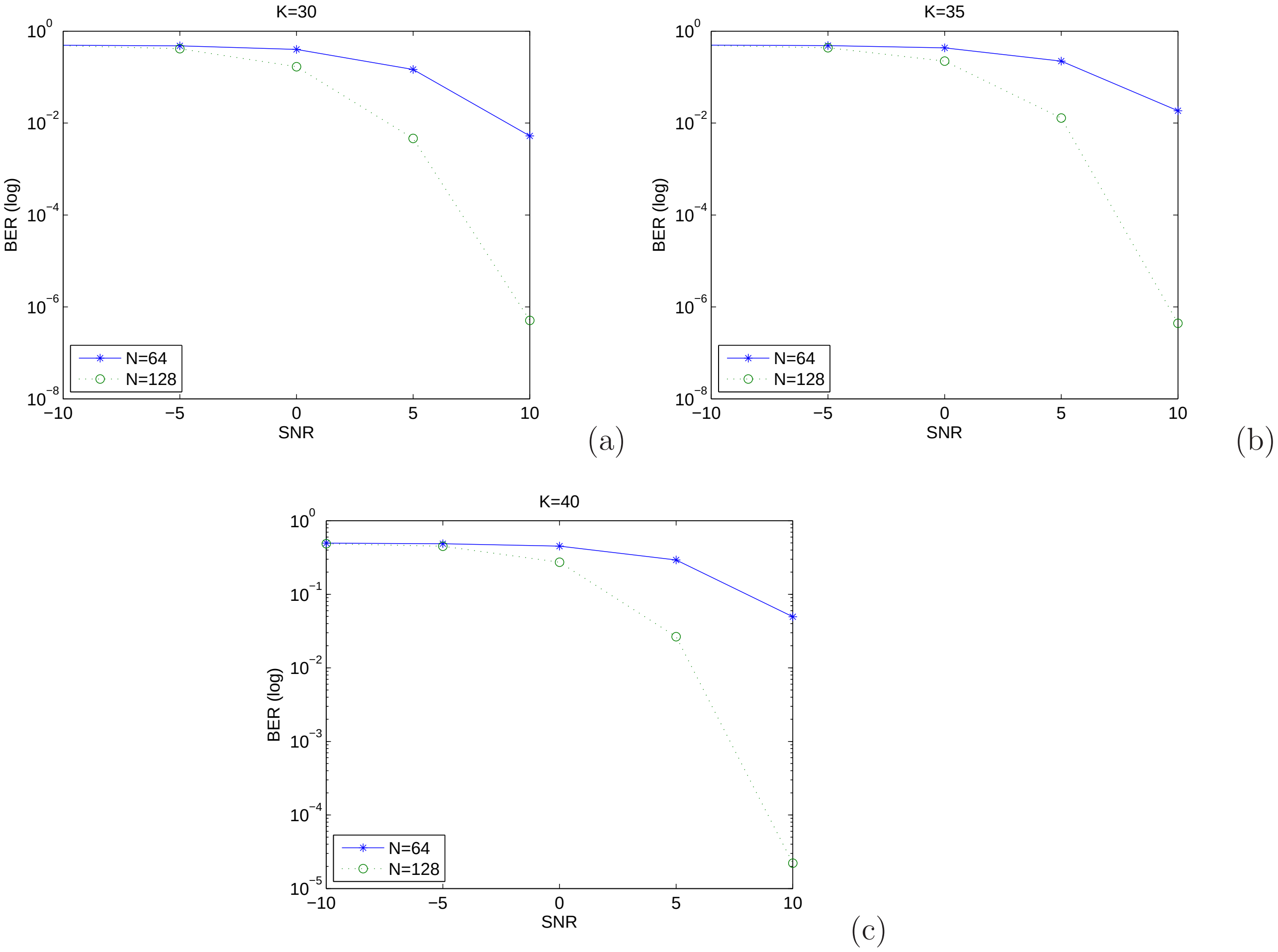
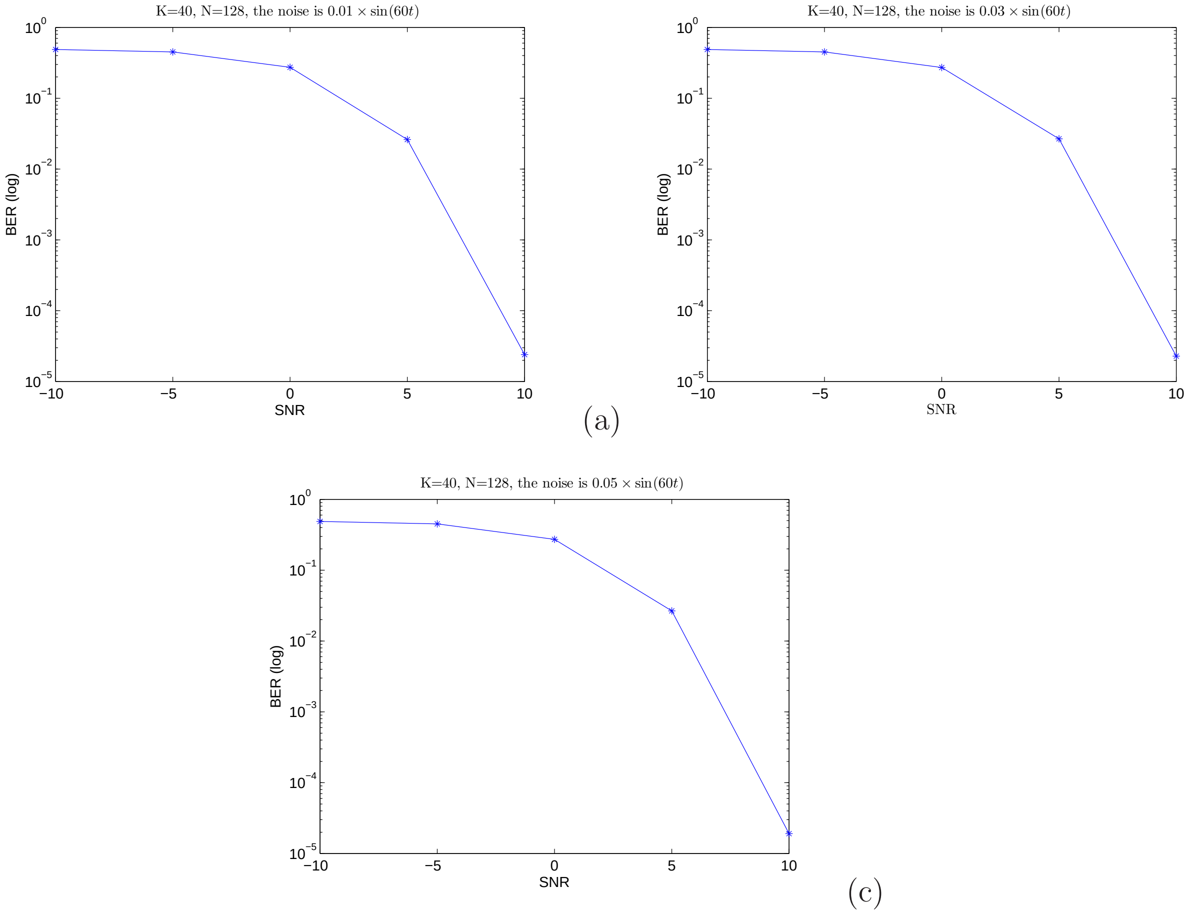


Figure 5.8: The performance of BER when $N = 64$ and $N = 128$, a) K=30, b) K=35, c) K=40.

is shown in Figure 5.9. Although the BER is lower than the performance in Figure 5.7, it is still satisfactory when the SNR is greater than 5, even if there is noise in the synchronization channel.



(a)

(b)

(c)

Figure 5.9: BER vs SNR, synchronization channel with noise, a) the noise is $0.01 \times \sin(60t)$, b) the noise is $0.03 \times \sin(60t)$, c) the noise is $0.05 \times \sin(60t)$.

5.4.4 Comparison with another two chaotic CDMA schemes

Reference [96] proposed a multi-user detection of a quasi-orthogonal chaotic CDMA system based on novel optimal chaos synchronization. Figure 5.10 plots the BER performances of this multi-user detectors and the scheme illustrated in Figure 5.1 in an AWGN channel. These two schemes consider 50 users. The length of spreading sequences of multi-user detectors is $N = 512$, and the length of the scheme in this chapter is $N = 128$. By assuming that the highest acceptable level of BER equals 10^{-3}

[95], it can be observed that the performance of the scheme in this chapter is satisfactory and better than the scheme in [96] when the SNR is greater than 10. Figure 5.11 plots the BER performances of the scheme in [97] and the scheme illustrated in Figure 5.1. The scheme in this chapter considers 40 users with the length of spreading sequences $N = 64$ and $N = 128$. The scheme in [97] considers 20 users with $N = 511$. In comparing with the scheme in [97], the scheme in this chapter considers more users and shorter sequences. However, it achieves lower BER values when SNR≥ 10. Hence the scheme in this chapter is better than the scheme in [97].

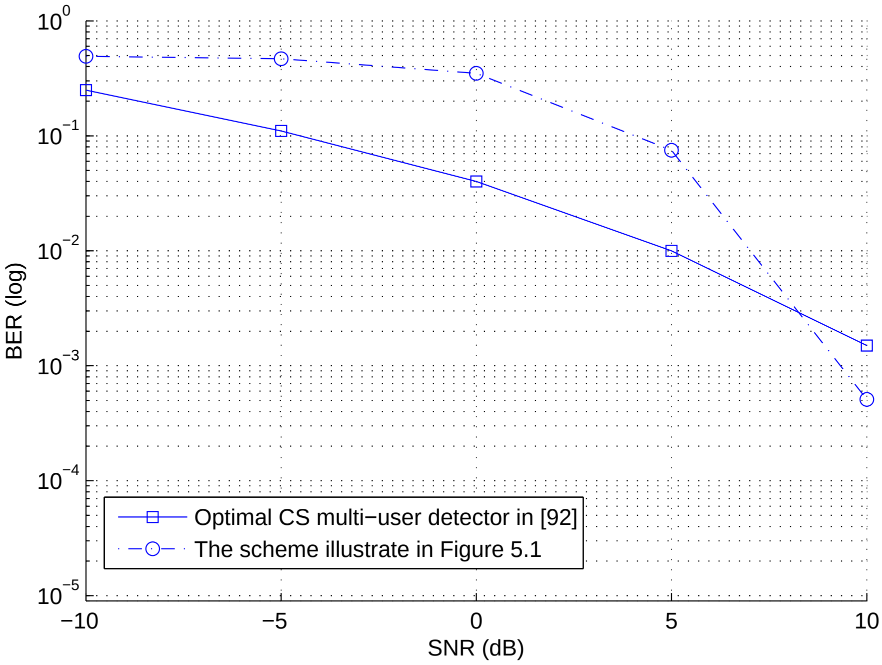


Figure 5.10: BER performance of optimal CS multi-user detectors and the scheme in this chapter.

5.5 Summary and conclusion

In this chapter we apply the results in Section 3.6 and 4.2 to a chaos-based DS-CDMA scheme to improve security. The local extrema of a chaotic signal generated by a continuous chaotic system is utilized to obtain spreading sequences. By means of these spreading sequences, numerical simulation shows that the DS-CDMA scheme combined with the cryptosystem in Section 4.2, constructed based on a chaotic map controlled by Δ-modulated feedback, has a satisfactory performance even if there is noise in

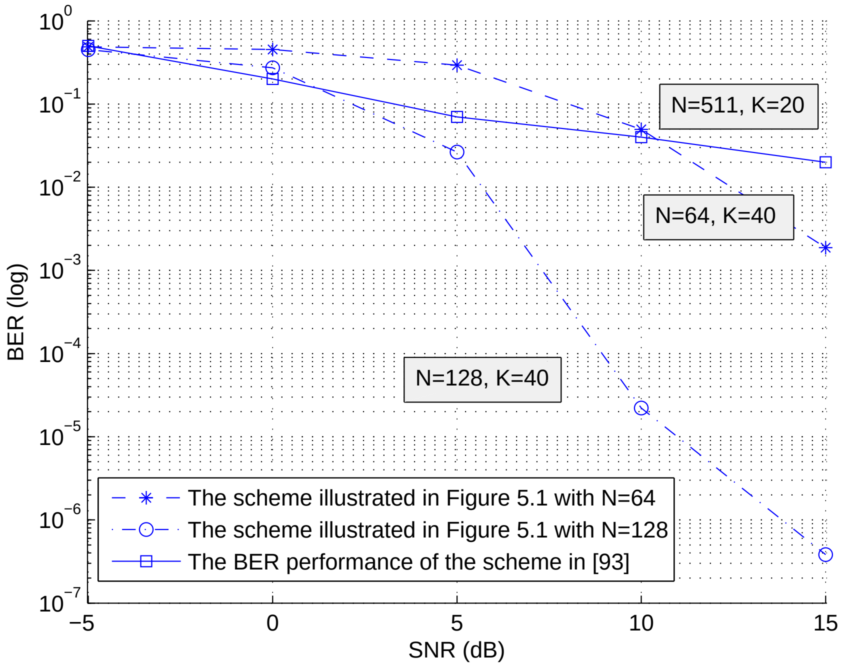


Figure 5.11: The empirical BER curves of the scheme in [97] and the scheme in this chapter.

the transmission channel. There is an interesting paradox between security and BER performance in the communication scheme. Improving the security while maintaining a good BER performance is an interesting and meaningful research topic for future work.

Chapter 6

Conclusions

6.1 Summary

The objectives of this thesis are to give some criteria in the design of chaos-based communication schemes, and to provide such a scheme with high security and robustness as well.

Firstly, some dynamical properties of the generalized Lorenz system are found, and an adaptive observer is constructed and proved to be an exponential observer for the generalized Lorenz system. The dynamical properties are utilized to prove the first state variable of the generalized Lorenz system, $\eta_1(t)$, to be PE. Then another function, $\Upsilon_1(t)$, is also PE, which is vital to estimate exactly the state and unknown parameter of the generalized Lorenz system simultaneously. The results are also shown by numerical simulations. The existence of such an adaptive observer implies that the unknown parameter of the generalized Lorenz system cannot be a password, and more effort is needed to achieve secure synchronization. This is the motivation for the modified parameter modulation scheme in this thesis.

Secondly, it is shown that the unidentifiable parameter is a good choice for a secret key, and a linear algebraic technique based on differential 1-forms is applied to check unidentifiability. In fact, if a system parameter is not identifiable, it is obvious that there is no an adaptive observer which can estimate the real parameter value. A modified Lorenz system is utilized to illustrate this method and to design a chaos-based communication scheme. In the testing of parameter identifiability, the linear algebraic technique based on differential 1-forms simplifies the computation and is applicable to more general systems. In addition, the chaotic system with unidentifiable parameters satisfies the antiadaptive property to a certain extent.

Thirdly, a modified parameter modulation communication scheme is provided in this thesis, and the robustness of this scheme against uncertain disturbance is also investigated both analytically and experimentally. The scheme is based on a cryptosystem constructed by a 1-D Δ-modulated feedback chaotic map. The modulated parameter is generated by this cryptosystem and selected according to the criteria in Section 3.6. As a theoretical basis of the modified parameter communication scheme, one proves that the one-dimensional discrete system controlled by a Δ-modulated feedback is chaotic when the parameter a is in $(\sqrt{2}, 2]$. The modulated parameter has more choices in key space compared with classic parameter modulation schemes. In addition, the complex parameter generating process improves the security of the communication scheme greatly, and numerical simulations show that the two popular attacks, power analysis attack and return map attack, are ineffective in the proposed communication scheme. As for the robustness problem, the upper bounds of uncertainty are found to ensure that this scheme works properly in practical implementation when the uncertainty satisfies the bounds. Numerical simulations also show that the bounds are sharp.

Finally, a novel chaos-based DS-CDMA scheme is constructed based on the results in Section 3.6 and Section 4.2. To improve security, an encryption/decryption function introduced in Section 4.2 is employed in the transmitter/receiver, and an unidentifiable parameter of the chaotic system is chosen as one secret key. In this scheme, a continuous chaotic system is employed and the local extrema are chosen from the output of this system to generate spreading sequences. By means of these spreading sequences, numerical simulations show that the DS-CDMA scheme combined with the encryption/decryption function performs well even if there is noise in the transmission channel.

6.2 Assessment

In this thesis an adaptive observer is constructed for the generalized Lorenz system with an unknown parameter, which shows that it is not easy to choose a good candidate for secure synchronization. Yet this result does not provide positive suggestions for designing a secure communication scheme. Hence identifiability is chosen to test whether system parameters are suitable for the secret key. It can be treated as a criterion to achieve secure synchronization. Nevertheless, more refined theoretic analysis is expected to be developed.

It should be pointed out that there is no straightforward procedure to prove that a chaos-based communication scheme is secure, although parameter identifiability is used to evaluate the security of the communication scheme. Hence the security of the modified parameter modulation in this thesis against two important attacks does not imply that the scheme is secure: other attacks may occur. On the other hand, provable security against these two attacks is certainly a first step in the right direction [22]. The analysis of the robust problem is presented by investigating the proposed modified parameter scheme, while a general procedure of the robust analysis for general communication schemes is still lacking.

6.3 Future work

To extend the research in this thesis further, one should take note of the following directions.

1. The convergence of estimated parameters to their true values and the rate of convergence are closely related to the PE property of certain signals. In this thesis we only prove that the generalized Lorenz system satisfies the PE condition. It is worth extending the result to more general chaotic systemss.

2. Chaotic synchronization has already been formulated into an observer design problem by control theory. Reference [24] evaluates the security of chaotic synchronization from the viewpoint of control theory. It is interesting to use the concepts of identifiability, observability and inverse system to obtain more re-

fined results on the security of chaotic synchronization.

3. The discrete chaotic systems controlled by a Δ-modulated feedback is an attractive choice for control practitioners. Hence the result achieved in this thesis will be extended to high dimensional discrete chaotic systems to improve security further.

4. There is an interesting paradox between security and robustness in chaos based communication schemes. How to improve the security while maintaining robustness property is an interesting and meaningful research topic for future work.

References

[1] I. I. Blekhman, A. L. Fradkov, H. Nijmeijer, and A. Y. Pogromsky, "On self-synchronization and controlled synchronization," *Syst. Control Lett.*, vol. 31, no. 5, pp. 299–305, 1997.

[2] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–825, 1990.

[3] R. He and P. G. Vaidya, "Analysis and synthesis of synchronous periodic and chaotic systems," *Phys. Rev. A*, vol. 46, no. 12, pp. 7387–7392, 1992.

[4] S. Boccaletti, J. Kurths, G. Osipov, D. Valladares, and C. Zhou, "The synchronization of chaotic systems," *Phys. Reports*, vol. 366, no. 1–2, pp. 1–101, 2002.

[5] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems.* Redwood City: Addison-Wesley, 1989.

[6] F. C. Moon, *Chaotic and Fractal Dynamics: An Introduction for Applied Scientists and Engineers.* New York: Wiley, 1992.

[7] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65–68, 1993.

[8] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE T. Circuits Syst. I*, vol. 40, no. 10, pp. 626–633, 1993.

[9] T.-L. Liao and N.-S. Huang, "An observer-based approach for chaotic synchronization with applications to secure communications," *IEEE T. Circuits Syst. I*, vol. 46, no. 9, pp. 1144–1150, 1999.

[10] T. Yang, "A survey of chaotic secure communication systems," *Int. J. Comput. Cognition*, vol. 2, no. 2, pp. 81–130, 2004.

[11] S. Bowong, F. M. Kakmeni, and M. S. Siewe, "Secure communication via parameter modulation in a class of chaotic systems," *Commun. Nonlinear Sci. Numer. Simulat.*, vol. 12, no. 3, pp. 397–410, 2007.

[12] T. Yang, "Secure communication via chaotic parameter modulation," *IEEE T. Circuits Syst. I*, vol. 43, no. 9, pp. 817–819, 1996.

[13] A. L. Fradkov, H. Nijmeijer, and A. Markov, "Adaptive observer-based synchronization for communication," *Int. J. Bifurcat. Chaos*, vol. 10, no. 12, pp. 2807–2813, 2000.

[14] H. Huijberts, H. Nijmeijer, and R. Willems, "System identification in communication with chaotic systems," *IEEE T. Circuits Syst. I*, vol. 47, no. 6, pp. 800–808, 2000.

[15] Y. Jin and Z. Qu, "Synchronization of Lorenz systems by adaptive observation," in *Proc. American Control Conf.*, Denver, Colorado, 4–6 June 2003.

[16] Z.-P. Jiang, "A note on chaotic secure communication systems," *IEEE T. Circuits Syst. I*, vol. 49, no. 1, pp. 92–96, 2002.

[17] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," *IEEE T. Circuits Syst. I*, vol. 44, no. 5, pp. 469–472, 1997.

[18] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Phys. Lett. A*, vol. 39, no. 1–2, pp. 75–82, 2003.

[19] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[20] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating chaotic map," in *Advances in Cryptology—EUROCRYPT '91.* Berlin: Springer, vol. 547, pp. 127–140, 1991.

[21] M. S. Baptista, "Cryptography with chaos," *Phys. Lett. A*, vol. 240, no. 1–2, pp. 50–54, 1998.

[22] L. Kocarev and G. Jakimoski, "Logistic map as a block encryption algorithm," *Phys. Lett. A*, vol. 289, no. 4–5, pp. 199–206, 2001.

[23] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," *IEEE T. Circuits Syst. I*, vol. 49, no. 1, pp. 28–40, 2002.

[24] S. Čelikovsky and G. Chen, "Secure synchronization of a class of chaotic systems from a nonlinear observer approach," *IEEE T. Automat. Contr.*, vol. 50, no. 1, pp. 76–82, 2005.

[25] C. Zhou and C. H. Lai, "Decoding information by following parameter modulation with parameter adaptive control," *Phys. Rev. E*, vol. 59, no. 6, pp. 6629–6636, 1999.

[26] K. M. Short, "Steps toward unmasking secure communications," *Int. J. Bifurcat. Chaos*, vol. 4, no. 4, pp. 959–977, 1994.

[27] K. M. Short, "Signal extraction from chaotic communications," *Int. J. Bifurcat. Chaos*, vol. 7, no. 7, pp. 1579–1597, 1997.

[28] G. Pérez and H. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, no. 11, pp. 1970–1973, 1995.

[29] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, "Breaking parameter modulated chaotic secure communication system," *Chaos Soliton. Fract.*, vol. 21, no. 4, pp. 783–787, 2004.

[30] C. Grebogi, E. Ott, and J. A. Yorke, "Roundoff-induced periodicity and the correlation dimension of chaotic attractors," *Phys. Rev. A*, vol. 38, no. 7, pp. 3688–3692, 1989.

[31] S. Li, X. Mou, Y. Cai, Z. Ji, and J. Zhang, "On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision," *Comput. Phys. Commun.*, vol. 153, no. 1, pp. 52–58, 2003.

[32] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *Int. J. Bifurcat. Chaos*, vol. 15, no. 10, pp. 3119–3151, 2005.

[33] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcat. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[34] X. Wang, M. Zhan, C.-H. Lai, and H. Gang, "Error function attack of chaos synchronization based encryption schemes," *Chaos*, vol. 14, no. 1, pp. 128–137, 2004.

[35] H. Zhou and X. Ling, "Problems with the chaotic inverse system encryption approach," *IEEE T. Circuits Syst. I*, vol. 44, no. 3, pp. 268–271, 1997.

[36] O. Morguöl and E. A. Solak, "Observer based synchronization of chaotic systems," *Phys. Rev. E*, vol. 54, no. 4, pp. 4803–4811, 1996.

[37] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization," *IEEE T. Circuits Syst. I*, vol. 44, no. 10, pp. 882–890, 1997.

[38] Q. Zhang, "Adaptive observer for multiple-input-multiple-output (MIMO) linear time-varying systems," *IEEE T. Automat. Contr.*, vol. 47, no. 3, pp. 525–529, 2002.

[39] G. Conte, C. H. Moog, and A. M. Perdon, *Nonlinear Control Systems: An Algebraic Setting.* London: Springer-Verlag, 1999.

[40] X. Xia and C. H. Moog, "Identifiability of nonlinear systems with applications to HIV/AIDS models," *IEEE T. Automat. Contr.*, vol. 48, no. 2, pp. 330–336, 2003.

[41] T. Yang, L. B. Yang, and C. M. Yang, "Breaking chaotic secure communications using a spectogram," *Phys. Lett. A*, vol. 247, pp. 105–111, 1998.

[42] C. S. Zhou and T. L. Chen, "Extracting information masked by chaos and contaminated with noise: some considerations on the security of communication approaches using chaos," *Phys. Lett. A*, vol. 234, 429–435, 1997.

[43] A. T. Parker and K. M. Short, "Reconstructing the keystream from a chaotic encryption scheme," *IEEE. T. Circuits Syst. I*, vol. 48, no. 5, pp. 624–630, 2001.

[44] M. Feki, "An adaptive chaos synchronization scheme applied to secure communication," *Chaos Soliton. Fract.*, vol. 18, no. 1, pp. 141–148, 2003.

[45] G. Kolumban, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications using chaos. II. chaotic modulation and chaotic synchronization," *IEEE T. Circuits Syst. I*, vol. 45, no. 11, pp. 1129–1140, 1998.

[46] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths, "Phase synchronization of chaotic oscillators," *Phys. Rev. Lett.*, vol. 76, no. 11, pp. 1804–1807, 1996.

[47] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. Abarbanel, "Generalized synchronization of chaos in directionally coupled chaotic systems," *Phys. Rev. E*, vol. 51, no. 2, pp. 980–994, 1995.

[48] M. P. Kennedy, "Three steps to chaos part I: Evolution," *IEEE T. Circuits Syst. I*, vol. 40, no. 10, pp. 640–656, 1993.

[49] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE T. Circuits Syst. I*, vol. 48, no. 12, pp. 1498–1509, 2001.

[50] G. Hu, Z. Feng, and R. Meng, "Chosen ciphertext attack on chaos communication based on chaotic synchronization," *IEEE T. Circuits Syst. I*, vol. 50, no. 2, pp. 275–279, 2003.

[51] G. Besançon, J. D. León-Morales, and O. Huerta-Guevara, "On adaptive observers for state affine systems," *Int. J. Control*, vol. 79, no. 6, pp. 581–591, 2006.

[52] F. Anstett, G. Millerioux, and G. Bloch, "Chaotic cryptosystems: cryptanalysis and identifiability," *IEEE T. Circuits Syst. I*, vol. 53, no. 12, pp. 2673–2680, 2006.

[53] S. Sastry and M. Bodson, *Adaptive Control : Stability, Convergence, and Robustness.* New Jersey: Prentice–Hall, 1989.

[54] S. Čelikovsky and G. Chen, "On a generalized Lorenz canonical form of chaotic systems," *Int. J. Bifurcat. Chaos*, vol. 12, no. 8, pp. 1789–1812, 2002.

[55] D. Li, J. an Lu, X. Wu, and G. Chen, "Estimating the bounds for the Lorenz family of chaotic systems," *Chaos Soliton. Fract.*, vol. 23, no. 2, pp. 529–534, 2005.

[56] T. Zhou, H. Liao, Z. Zheng, and Y. Tang, "The complicated trajectory behaviors in the Lorenz equation," *Chaos Soliton. Fract.*, vol. 19, no. 4, pp. 863–873, 2004.

[57] T. Zhou and Y. Tang, "Complex dynamical behaviors of the chaotic Chen's system," *Int. J. Bifurcat. Chaos*, vol. 13, no. 9, pp. 2561–2574, 2003.

[58] A. D. Polianin and V. F. Zaitsev, *Handbook of Exact Solutions for Ordinary Differential Equations.* Boca Raton: CRC Press, 1995.

[59] J. B. Conway, *Functions of One Complex Variable II.* New York: Springer, 1995.

[60] K. S. Narendra and A. M. Annaswamy, "Persistent excitation in adaptive systems," *Int. J. Control*, vol. 45, no. 1, pp. 127–160, 1987.

[61] S. Boyd and S. Sastry, "On parameter convergence in adaptive control," *Syst. Control Lett.*, vol. 3, no. 6, pp. 311–319, 1983.

[62] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* New York: Wiley, 1996.

[63] H. Dedieu and M. Ogorzalek, "Identifiability and identification of chaotic systems based on adaptive synchronization," *IEEE T. Circuits Syst. I*, vol. 44, no. 10, pp. 948–962, 1997.

[64] J. B. Geddes, K. M. Short, and K. Black, "Extraction of signals from chaotic laser data," *Phys. Rev. Lett.*, vol. 83, no. 25, pp. 5389–5392, 1999.

[65] P. G. Vaidya and S. Angadi, "Decoding chaotic cryptography without access to the superkey," *Chaos Soliton. Fract.*, vol. 17, no. 2–3, pp. 379–386, 2003.

[66] E. T. Tunali and T. J. Tarn, "New results for identifiability of nonlinear systems," *IEEE T. Automat. Contr.*, vol. 32, no. 2, pp. 146–154, 1987.

[67] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos: An Introduction to Dynamical Systems.* New York: Springer-Verlag, 1997.

[68] P. Palaniyandi and M. Lakshmanan, "Secure digital signal transmission by multistep parameter modulation and alternative driving of transmitter variables," *Int. J. Bifurcat. Chaos*, vol. 11, no. 7, pp. 2031–2036, 2001.

[69] C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurcat. Chaos*, vol. 3, no. 6, pp. 1619–1627, 1993.

[70] S. Bu and B.-H. Wang, "Improving the security of chaotic encryption by using a simple modulating method," *Chaos Soliton. Fract.*, vol. 19, no. 4, pp. 919–924, 2004.

[71] R. Gai, X. Xia, and G. Chen, "Complex dynamics of systems under Delta-modulated feedback," *IEEE T. Automat. Contr.*, vol. 51, no. 12, pp. 1888–1902, 2006.

[72] X. Xia and G. Chen, "On Delta-modulated control: A simple system with complex dynamics," *Chaos Soliton. Fract.*, vol. 33, no. 4, pp. 1314–1328, 2007.

[73] X. Xia and A. S. I. Zinober, "Delta-modulated feedback in discretization of sliding mode control," *Automatica*, vol. 42, no. 5, pp. 771–776, 2006.

[74] X. Xia, R. Gai, and G. Chen, "Periodic orbits arising from Delta-modulated feedback control," *Chaos Soliton. Fract.*, vol. 19, no. 3, pp. 581–595, 2004.

[75] P. Glendinning, *Stability, Instability and Chaos.* Cambridge: Cambridge University Press, 1994.

[76] J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields.* New York: Springer, 1983.

[77] R. F. Williams, "The structure of Lorenz attractors," *Publ. Math. IHES*, vol. 50, 1979.

[78] Y. Choi, "Attractors from one dimensional Lorenz-like maps," *Discret. Contin. Dyn. S.*, vol. 11, no. 2–3, pp. 715–730, 2004.

[79] M. Blank, "Discreteness and continuity in problems of chaotic dynamics," *Translations Math. Monogr.*, vol. 161, 1997.

[80] T. Sang, R. Wang, and Y. Yan, "Perturbance-based algorithm to expand cycle length of chaotic key stream," *Electron. Lett.*, vol. 34, no. 9, pp. 873–874, 1998.

[81] X. Liang, J. Zhang, and X. Xia, "Improving the security of chaotic synchronization with a Δ-modulated cryptographic technique," *IEEE T. Circuits Syst. I*, vol. 55, no. 7, pp. 680–685, 2008.

[82] S. Glisic, *Spread Spectrum CDMA Systems for Wireless Communications.* Boston: Artech House, 1997.

[83] R. M. Buehrer, N. S. Correal-Mendoza, and B. D. Woerner, "A simulation comparison of multiuser receivers for cellular CDMA," *IEEE. T. Veh. Technol.*, vol. 48, no. 4, pp. 1065–1085, 2000.

[84] F. Swarts, P. Rooyan, I. Oppermann, and M. P. Lötter, *CDMA Techniques for Third Generation Mobile Systems.* Boston: Kluwer Academic Publishers, 1999.

[85] K. G. Roberts and J. B. Pick, "Technology factors in corporate adoption of mobile cell phones: a case study analysis," in *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii, 5–8 January 2004.

[86] E. Bollt, Y. C. Lai, and C. Grebogi, "Coding, channel capacity, and noise resistance in communicating with chaos," *Phys. Rev. Lett.*, vol. 79, no. 19, pp. 3787–3790, 1997.

[87] U. Parlitz and S. Ergezinger, "Robust communication based on chaotic spreading sequences," *Phys. Lett. A*, vol. 188, no. 2, pp. 146–150, 1994.

[88] D. Sandoval-Morantes and D. Munoz-Rodriguez, "Chaotic sequences for multiple access," *Electron. Lett.*, vol. 34, no. 3, pp. 235–237, 1998.

[89] R. H. Shumway and D. S. Stoffer, *Time Series Analysis and Its Applications.* New York: Springer, 2000.

[90] F. Argüello, M. Bugallo, and M. Amor, "Multi-user receivers for spread spectrum communications based on chaotic sequences,," *Int. J. Bifurcat. Chaos*, vol. 12, no. 4, pp. 847–853, 2002.

[91] M. Itoh, "Spread spectrum communication via chaos," *Int. J. Bifurcat. Chaos*, vol. 9, no. 1, pp. 155–213, 1999.

[92] W. M. Tam, F. C. M. Lau, and C. K. Tse, "An approach to calculate the bit error rates of multiple access chaotic-sequence spread-spectrum communication systems employing multi-user detectors," *Int. J. Bifurcat. Chaos*, vol. 14, no. 1, pp. 183–206, 2004.

[93] T. Yang and L. O. Chua, "Error performance for chaotic digital code division multiple access ($(CD)^2MA$)," *Int. J. Bifurcat. Chaos*, vol. 8, no. 10, pp. 2047–2059, 1998.

[94] L. K. Rasmussen, T. J. Lim, and A. L. Johansson, "A matrix-algebraic approach to successive interference cancellation in CDMA," *IEEE T. Commun.*, vol. 48, no. 1, pp. 145–151, 2000.

[95] A. J. Giger and W. T. Barnett, "Effects of multipath propagation on digital radio," *IEEE T. Commun.*, vol. 29, no. 9, pp. 1345–1352, 1981.

[96] D. He and H. Leung, "Quasi-orthogonal chaotic CDMA multi-user detection using optimal chaos synchronization," *IEEE T. Circuits Syst. II*, vol. 52, no. 11, pp. 739–743, 2005.

[97] B. Jovic, C. P. Unsworth, G. S. Sandhu, and S. M. Berber, "A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems," *Signal Process.*, vol. 87, no. 7, pp. 1692–1708, 2007.

List of Figures