Czech Technical University in Prague
Faculty of Electrical Engineering

DOCTORAL THESIS

Prague, 2010

Volodymyr Lynnyk

Czech Technical University in Prague
Faculty of Electrical Engineering
Department of Control Engineering

Chaos-based communication systems

Doctoral Thesis

by

Volodymyr Lynnyk

Prague, 2010

Ph.D. programme: Electrical Engineering and Information Technology
Branch of study: Control Engineering and Robotics

Supervisor: **Doc. RNDr. Sergej Čelikovský, CSc.**

Table of Contents

Acknowledgement

I would like to thank, first and foremost, my supervisor, Doc. RNDr. Sergej Čelikovský, CSc., for his guidance and support throughout my Doctoral degree and during the completion of this thesis.

I would like to acknowledge the support of all staff members in the Department of Control Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague.

I would like to thank all the staff in the Department of Control Theory, Institute of Information Theory and Automation, who helped me all these years.

Thanks also to my family for supporting me in my educational pursuits and to my friends for their encouragement.

Support for this research was provided in part by IGS grant CTU0712813 through the Czech Technical University in Prague. Partly supported by the Czech Science Foundation grant 102/08/0186.

Significant part of the underlying research has been performed in the Institute of Information Theory and Automation of the ASCR.

Introduction

Today, mathematical theory of the chaos is a fundamental base of natural science [65; 74; 77; 32; 53; 71; 72]. It proves that the complexity of the behavior of the chaotic systems stems from the exponentially unstable dynamics, rather than from the fluctuations or big degree of freedom. Classical example of the chaotic behavior are Brownian motion, change of the weather, behavior of the financial markets, the biological processes in the living organisms, the fluctuation of the astronomical orbit, etc.

During the past two decades, there has been tremendous interest worldwide in the possibility of using chaos in communication systems. Many different chaos-based decryption algorithms have been proposed up to date. They can be classified into two basic categories, namely, coherent and noncoherent approaches. In the first approach, the chaotic signal has to be recovered from the received signal by synchronization, while in the second one the demodulation is done solely based on the received signal, i.e. without synchronization [44; 49].

Some researchers have pointed out that there exists close relationship between chaos and cryptography [4; 31; 38]. Many characteristics of chaos, such as ergodicity, mixing, randomness, complexity, unpredictably and the sensitivity to initial conditions, can be connected with the well-known confusion and diffusion properties in the classical cryptography. More precisely, the diffusion is refereed in the cryptography as the ability of the variation of a single bit in the plaintext (i.e. the message) to affect practically all bits of ciphertext (i.e. the encrypted message). At the same time, the confusion ensures that bits of ciphertext are abusively mixed. The

analogues of these concepts in chaos theory are those famous chaos properties: strong sensitivity to initial conditions and topological transitivity. As a consequence, a natural idea arises: to use the chaos to design new cryptographical algorithms, hopefully enhancing the existing ones. Notice, that there is not only conceptual relationship between chaos and cryptography, the chaotical and cryptographical systems are very similar on the practical level, too. The idea of using chaos in cryptography can be traced back to Shannons masterpiece entitled "Communication Theory of Secrecy Systems" published in 1949. He wrote [76]: *"Good mixing transformations are often formed by repeated products of two simple noncommuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc..."* Thus, Shannon noticed, that expanding and compression mechanisms of the chaos can be applied to the secure transformation of data. Nevertheless, the more detailed research in this area was started subsequently together with the evolution of the modern theory of chaos and computer science. Today, during the "information century", cryptography is more actual than before. Scientists are still searching a new technology to be applied in the cryptographical area. Motivation is very simple, it is the dependence of the existing methods on "unsolvable" mathematical problems that might be suddenly solved by scientific community.

Goals of the thesis and methods to achieve them

The main goal of the thesis is to study the novel methods of communication and encryption using chaotic system in order to improve the existing communication schemes. In particular, as these methods depend crucially on chaos synchronization phenomena, some new theoretical properties of chaotic system synchronization will be developed as well. These properties will be used to design and systematically analyze the new communication and encryption scheme, called as the anti-synchronization chaos shift keying (ACSK). Finally, the synchronization and communication aspects in more complex networks are to be studied.

These goals will be achieved using both theoretical analysis by exact mathematical methods as well as by numerical computer simulations and experiments.

The main contribution of the thesis

The present thesis surveys the different chaotic communication techniques that can be implemented with and without synchronization. Encryption methods based on the properties of chaos are reviewed. The main contribution of the thesis is the use of the so-called generalized Lorenz system (GLS) in encryption and communication, in particular to construct message embedded chaotic masking and the novel modulation scheme called as anti-synchronization chaos shift keying (ACSK). ACSK digital communication method has potential of introducing a high degree of security at a low receiver complexity. At the same time, it requires reasonable amount of data to encrypt a single bit, thereby making revolutionary possibility of practical and realistic use of continuous time chaotic system for digital data encryption. As already noticed, the thesis implements the ACSK scheme by using the so-called generalized Lorenz system (GLS) family. GLS has been introduced and studied relatively recently, [20; 81; 10], nevertheless, to use it to ACSK implementation, its further theoretical analysis is performed here. Finally, the ideas about communication using GLS via their synchronization are generalized to study the synchronization of complex networks of chaotic systems.

Organization of the thesis

This thesis is organized as follows. Chapter 1 introduces some preliminary knowledge about chaos and cryptography. Chapter 2 gives a thorough survey of the field of chaos based communication and encryption. It also summarizes the existing methods to analyze the security of the chaotic encryption and possible methods to attack it. These methods will be used later on to analyze the novel scheme being the main contribution of the thesis. Chapter 3 presents the encryption and communication schemes

based on the generalized Lorenz system and describes in detail the anti-synchronization chaos shift keying scheme, including its security analysis. The synchronization and communication in more complex networks are studied in this chapter too. Finally, the thesis results are summarized in Conclusions at the end of thesis where the outlooks for future research are set as well.

Chapter 1

Preliminary knowledge

In this chapter the relationship between cryptographic and chaotic systems is analyzed. Main definitions about cryptography [59; 37; 75] and chaotic dynamics [74; 33] are discussed.

1.1 Cryptography

Cryptography is the study of mathematical techniques related to the aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Practical cryptography is the study of the methods of the encryption of the information, creation of the digital signature, the control of the keys and the certificates. Cryptanalysis is the opposite of the cryptography. Cryptanalysis studies the decryption of the cipher information without knowledge of the key. Cryptology is a part of the mathematics study about the mathematical footing of the cryptography and cryptanalysis methods. In the currently section some preliminary knowledge about cryptography is introduced.

1.1.1 Cryptographical system

From the mathematical point of view, the cryptosystem $\mathcal{S} = \langle \mathcal{X}, \mathcal{Y}, \mathcal{K}, f \rangle$ is the transformation of the information $f : \mathcal{X} \times \mathcal{K} \to \mathcal{Y}$, defined on the spaces $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{K}$, which was the initial states, the final states and the keys respectively. Condition $x \in \mathcal{X}$ encode some useful information. In the

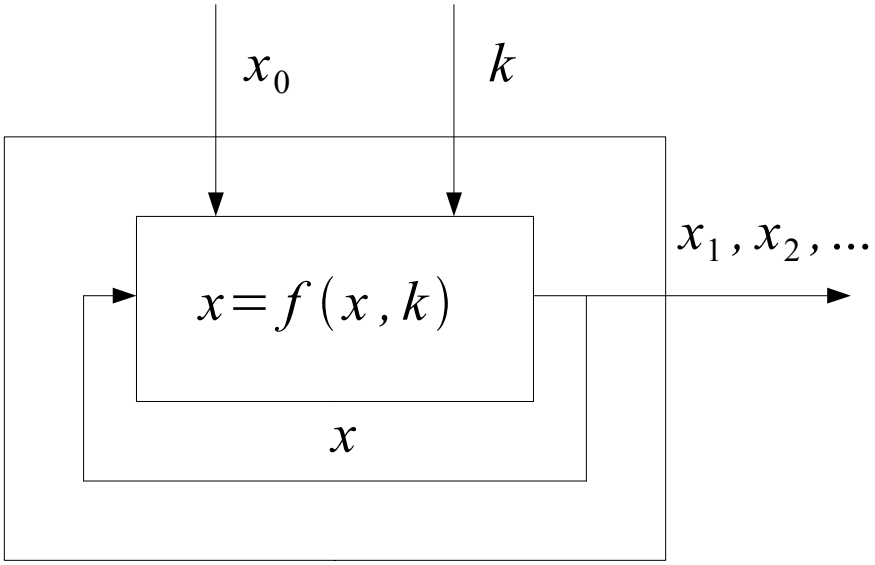


Figure 1.1: The cryptographical system.

computer cryptography spaces $\mathcal{X} \subset \{0,1\}^*$, $\mathcal{Y} \subset \{0,1\}^*$, $\mathcal{K} \subset \{0,1\}^*$, and the transformation f is given by the algorithm realized with a Turing machine. The transformation f can be considered as the iteration function of the cryptographical algorithm (see Fig. 1.1). In this case, the cryptosystem generates the sequences of states $x_0, x_1, x_2, x_3, ..., x_i$, where $x_i = f(x_{i-1}, k) = f^i(x_0, k)$, $x_0 \in \mathcal{X}$, $k \in \mathcal{K}$. This sequence is called a trajectory or the orbit of the system. The overall orbit is determined by the initial state x_0 of the system and the parameter k. Such a subsequent transformation of some state by the application of the same primitive function can be seen in the block ciphers, stream ciphers, pseudo-random bit generators, etc. Thus a cryptosystem can be understood as a dynamic system $\mathcal{S} = \langle f, \mathcal{X}, \mathcal{K} \rangle$ with a nonlinear function f, the state space $\mathcal{X}$, and the parameter space $\mathcal{K}$. As it will be shown below, the requirements for cryptosystems are interrelated with the properties of the chaotic systems.

1.1.2 Main definitions related to cryptography

Main definitions related to cryptography are presented below [59]:

- $\mathcal{A}$ denotes a finite set called the *alphabet of definition*. For example, $\mathcal{A} = \{0, 1\}$, the *binary alphabet*, is a frequently used alphabet of definition. Note that any alphabet can be encoded in terms of the binary alphabet. For example, since there are 64 binary strings of length six, each letter of the Czech alphabet can be assigned a unique binary string of length six.

- $\mathcal{M}$ denotes a set called the *message space*. $\mathcal{M}$ consists of strings of symbols from an alphabet of definition. An element of $\mathcal{M}$ is called a *plaintext message* or simply a *plaintext*. For example, $\mathcal{M}$ may consist of binary strings, computer code, English text, etc.

- $\mathcal{C}$ denotes a set called the *ciphertext* space. $\mathcal{C}$ consists of strings of symbols from an alphabet of definition, which may differ from the alphabet of definition for $\mathcal{M}$. An element of $\mathcal{C}$ is called a *ciphertext*.

- $\mathcal{K}$ denotes a set called the *key space*. An element of $\mathcal{K}$ is called a *key*.

- Each element $e \in \mathcal{K}$ uniquely determines a bijection between $\mathcal{M}$ and $\mathcal{C}$, denoted by E_e. E_e is called an *encryption function*. Note that E_e must be a bijection, i.e. one-to-one mapping as the process is to be reversed and a unique plaintext message recovered for each distinct ciphertext.

- For each $d \in \mathcal{K}$, D_d denotes a bijection from $\mathcal{C}$ to $\mathcal{M}$ (i.e., $D_d : \mathcal{C} \rightarrow \mathcal{M}$). D_d is called a *decryption function* or *decryption transformation*.

- The process of applying the transformation E_e to a message $m \in \mathcal{M}$ is usually referred to as *encrypting* m or the *encryption* of m.

- The process of applying the transformation D_d to a ciphertext c is usually referred to as *decrypting* c or the *decryption* of c.

- An *encryption scheme* consists of a set $\{E_e : e \in \mathcal{K}\}$ of encryption transformations and a corresponding set $\{D_d : d \in \mathcal{K}\}$ of decryption transformations with the property that for each $e \in \mathcal{K}$ there is a unique key $d \in \mathcal{K}$ such that $D_d = E_e^{-1}$; that is, $D_d(E_e(m)) = m$

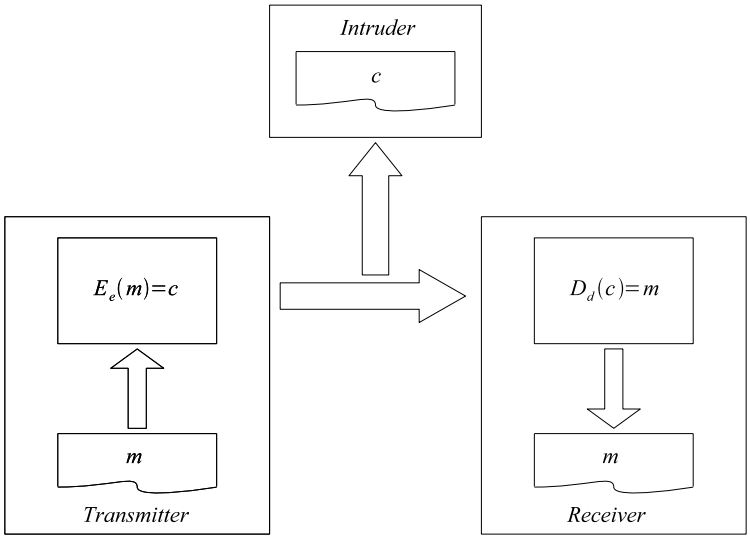


Figure 1.2: The classical encryption/decryption scheme.

for all $m \in \mathcal{M}$. An encryption scheme is sometimes referred to as a *cipher*.

- The keys e and d in the preceding definition are referred to as a *key pair* and sometimes denoted by (e, d). Note that e and d could be the same. If $e = d$, then the cryptosystem is refereed as the *symmetric* one.

- To *construct* an encryption scheme requires one to select a message space $\mathcal{M}$, a ciphertext space $\mathcal{C}$, a key space $\mathcal{K}$, a set of encryption transformations $\{E_e : e \in \mathcal{K}\}$, and a corresponding set of decryption transformations $\{D_d : d \in \mathcal{K}\}$.

Fig. 1.2 illustrates the classical encryption/decryption scheme.

1.1.3 Encryption schemes, their classifications and properties

Encryption scheme can be written in the following form:

$$\mathcal{S} = \langle E, D, \mathcal{M}, \mathcal{C}, \mathcal{K} \rangle, \tag{1.1}$$

where, $E : \mathcal{M}^* \times \mathcal{K} \to \mathcal{C}^*$ and $D : \mathcal{C}^* \times \mathcal{K} \to \mathcal{M}^*$, such that for each key $e \in \mathcal{K}$ exists a unique key $d \in \mathcal{K}$ and $D_d = E_e^{-1}$, thus

$$\forall m \in \mathcal{M}, e \in \mathcal{K}, \quad \exists d \in \mathcal{K} : \qquad m = D(E(m, e), d). \tag{1.2}$$

Practically, scheme is assigned by algorithms E, D and spaces $\mathcal{M}, \mathcal{C}, \mathcal{K}$ (see Sec. 1.1.2).

Security of some cryptosystems is based on the lack of knowledge of the encryption (decryption) algorithm of the cryptosystem. Now, this kind of cryptosystems have only a historical interest and do not have any practical use. Security of the modern ciphers are depended on the key only (Kerckhoffs' principle). Kerckhoffs' principle was stated by Auguste Kerckhoffs in the 19th century: "A cryptosystem should be a secure even if everything about the system, except the key, is public knowledge" [37]. Kerckhoffs' principle was reformulated (perhaps independently) by Claude Shannon as "The enemy knows the system." In this form, it is known as the "Shannon's maxim". Now, let us give classifications of encryption schemes based on the the further two important characteristics.

Symmetric and asymmetric schemes. First, there are symmetric and asymmetric cryptosystems known. In the symmetric cryptosystems (secret key cryptosystems) both of keys e and d are equal (see Sec. 1.1.2). Sender must pass the key by secure channel, for example, with courier. In the asymmetric cryptosystems keys are different and $\forall e \in \mathcal{K}, \exists d \in \mathcal{K}'$. The keys e and d are non equal but they are interconnected. The key e is usually publicly known and is called as the open key, while the key d is kept in the secret. Nevertheless, from the open key e it is practically unrealistic to calculate the second key d.

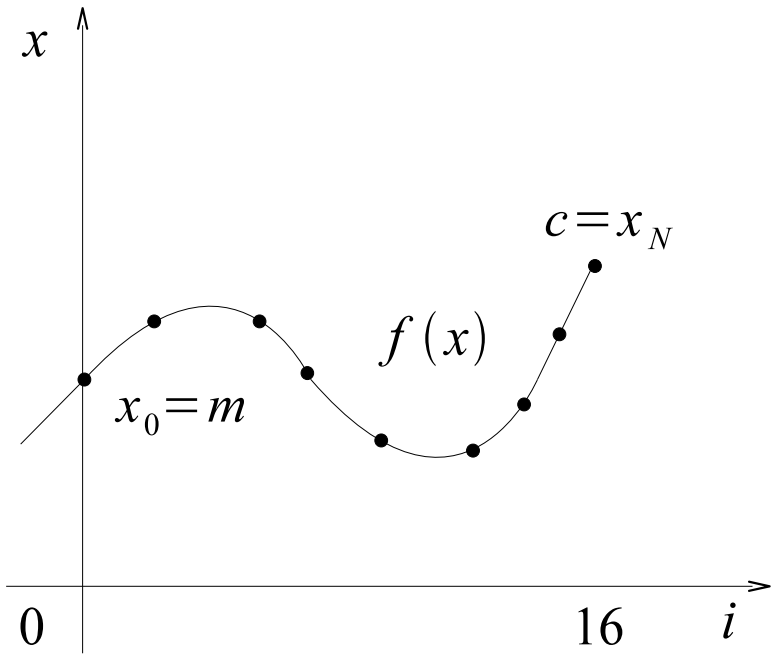


Figure 1.3: The trajectory of the block cipher. Each block is encrypted by the separate trajectory. Initial point is a plaintext m, when a final point is a ciphertext c.

Block and stream ciphers. Secondly, the cryptographic schemes can be classified as the block and stream ciphers. The block cipher is a function which maps n-bit plaintext blocks to n-bit ciphertext blocks; n is called the *blocklength*. Each n-block encrypts (decrypts) independently from another one. Identical block of the plaintext will be transformed to the equal block of the ciphertext. Block ciphers processes the plaintext in the relatively large blocks (e.g., $n \geq 64$ bits). The same function is used to encrypt the successive blocks; thus (pure) block ciphers are memoryless. The corresponding function is, in fact bijection of the set with cardinality 2^{64} and should be sufficient complicated, see later on notions of confusion and diffusion.

In the contrast, stream ciphers process the plaintext in the much smaller blocks (up to a single bit) and the encryption function may vary as plaintext is processed; thus stream ciphers are said to have memory. They are sometimes called as the state ciphers since encryption depends not only on

the key and the plaintext, but also on the current state. Identical symbols (blocks) of the plaintext may be transformed to another symbols (blocks) of the ciphertext.

The cryptography cipher can be interpreted by using the nonlinear dynamical systems theory concepts as follows:

1. The encryption of the plaintext by block cipher algorithm is realized by the repeated application of the some iteration function f. Number of these repeated applications is fixed and not so big, typically equal to 16 [80]. Each iteration transforms the cryptosystem to the next state, $x_{i+1} = f(x_i)$. Initial state is a plaintext ($x_0 = m$), when the final state is a ciphertext ($c = x_N$). Fig. 1.3 illustrates a trajectory of the block cipher, which is in fact the trajectory of discrete dynamical system.

2. Different blocks generate different trajectories of the iteration function f in the block cipher (provided mutually different initial blocks of the plaintext are used). Nevertheless, the stream ciphers are quite different in this respect. Overall the ciphertext of the stream cipher depends on a single trajectory of the iteration function f only. More precisely, the encryption of the piece of the plaintext depends on the current state of the cryptosystem. The number of the iterations n is not fixed and depends on the size of the plaintext. Fig. 1.4 illustrates the trajectories of the stream ciphers.

Example: Vernam cipher and the one-time pad cipher. Vernam cipher is a simple stream cipher [59] where the plaintext is XORed[1] with a random or pseudorandom stream k of data of the same length needed to generate the ciphertext.

$$c_i = m_i \oplus k_i, \quad i = 0, 1, 2, ..., n.$$

[1] Application of the logical operation of the exclusive disjunction, also called exclusive or (symbolized XOR or EOR), is a type of logical disjunction on two operands that results in a value of true if exactly one of the operands has a value of true.

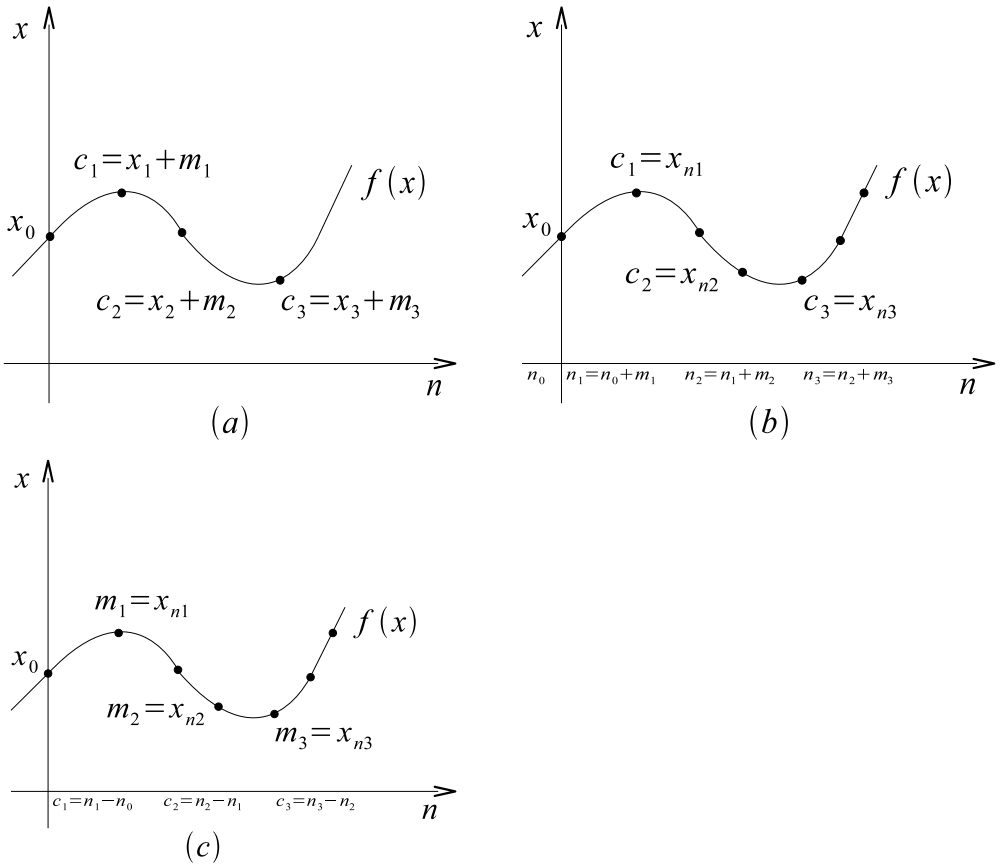


Figure 1.4: The trajectories of the stream ciphers. (a) Ciphertext c is the sum of the plaintext m and the current state x [7]. b) Ciphertext c is a final state of the system after m iterations [30]. c) Ciphertext c is a number of iterations n [6].

The decryption of the plaintext is XORed with k:

$$m_i = c_i \oplus k_i,$$

This is clear, because $m_i \oplus k_i \oplus k_i = m_i$. If the keystream $k = \{k_i\}$ is truly random, then the Vernam cipher is called one-time pad cipher (OTP).

Pseudorandom bit generator (PRBG). Stream ciphers can be viewed as approximating the action of a proven unbreakable cipher, the one-time pad (OTP) cipher introduced in the previous paragraph. The OTP uses a keystream of completely random digits. The keystream is combined with the plaintext digits, one at a time, to form the ciphertext. This system was proved to be secure by Claude Shannon [75]. However, the

keystream must be of (at least) the same length as the plaintext, and generated completely at random. This makes the system very cumbersome to implement in practice, and as a result the OTP has not been widely used, except for the most critical applications. In the practice, the so-called pseudorandom number generators are used. The pseudorandom bit generator (PRBG) is a deterministic algorithm which, uses a truly random binary sequence of length k, to generate a pseudorandom binary sequence of length $l \gg k$. The input to the PRBG is called the *seed*, while the output of the PRBG is called a *pseudorandom bit sequence* [59]. A stream cipher makes use of a much smaller and more convenient key, 128 bits, for example. Based on this key, it generates a pseudorandom keystream which can be combined with the plaintext digits in a similar fashion as the one-time pad. However, this comes at a cost: because the keystream is now pseudorandom, and not truly random, the proof of security associated with the one-time pad no longer holds: it is quite possible for a stream cipher to be completely insecure [83]. According to our approach, let us was consider a PRBG to be a dynamical system. Fig. 1.1 demonstrates a system which reproduces a number stream. Every number stream, generated by system, depends on the initial condition x_0 and parameter k. The important requirement of the dynamical system to be used for the generation of the keystreams is the so-called pseudo-randomness and unpredictability.

Confusion and diffusion. The truly random keystream fully allows to eliminate the statistic invariants of cryptographic transformation. Nevertheless, as it was already noticed, one uses the pseudo-random sequences, therefore some part of information about the plaintext "leaks" into the ciphertext. As the plaintext usually possesses redundancy, cryptanalysis becomes theoretically possible already, as early as one has the information about the statistical properties of the alphabet. Redundancy of the message can be decreased by means of good compression. Incompressible message is characterized by following: the change of any single bit leads to a complete change of the message meaning. If the message can't be compressed up to the theoretical minimum, then according to Shannon [76] it is necessary to use two basic technics for redundancy hiding, namely, the

so-called confusion and so-called diffusion.

Confusion refers to making the relationship between the key and the ciphertext as complex and involved as possible.

Diffusion refers to the property that redundancy in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext. Diffusion is associated with the dependency of the output bits on the input bits. In a cipher with good diffusion, flipping an input bit should change each output bit with a probability of one half.

This concept is realized in the symmetric block ciphers. Iterative function of the typical block-cipher algorithm includes the phases of substitution and permutation. In the classical DES algorithm [80] the substitution and permutation are implemented through lookup tables (s-box and p-box). Effect of substitution provides the confusion, then effect of permutation provides the diffusion. Ultimately, both properties ensures the pseudorandom of ciphertext for any key and any text. Permutation is the effective tool of increasing of the nonlinearity of the iteration function of cryptosystem.

1.2 Chaos and cryptography

In this section, the definitions of the dynamic and chaotic systems are introduced. The relationship between the properties of chaotic and cryptographic systems is going to be discussed as well.

1.2.1 Dynamical system

Continuous dynamical system $S =< X, K, f >$, depending on the parameters, can be presents by the following equation:

$$\frac{dx}{dt} = f(x,k), \quad x \in X \subseteq R^d, k \in K \subseteq R^{d_K}, \tag{1.3}$$

where $f : X \times K \longrightarrow Y$ is smooth vector function, X is a state space and K is a space of the control parameters. For every initial condition x_0 system satisfies the condition of the existence and uniqueness of solutions $x(t, x_0)$,

where $x(0, x_0) = x_0$. Curve $\phi_t(t, x_0)$ which corresponds to the solution is called a trajectory. A discrete-time, dynamical system can be presented by the following iteration function:

$$x_{n+1} = f(x_n, k), \quad x_n \in X \subseteq R^d, k \in K \subseteq R^{d_K}, n = 0, 1, 2, ... \tag{1.4}$$

where x_i are discrete states of the system. Trajectory $\phi(i, x_0)$ is a sequence of $x_0, x_1, x_2....$ It easy do note, that equation (1.4) resembles a cryptographical iteration function used in the pseudo-random number generators, block ciphers, etc. (see Fig. 1.1). Iterative transformation of the information, depends on the control parameter, used in both of the dynamical and cryptographical systems. Further, the control parameter k in the definitions of the system $< X, f >$ and iteration function $f(x)$, will be omitted.

1.2.2 Chaotic system

Several conditions for the chaotic behavior of the dynamical system exist. The topological transitivity and the sensitivity to initial conditions are two necessary criterions for the chaotic behavior of the dynamical system.

Definition 1.2.1. *Dynamical system $< X, f >$ is chaotic when it satisfies the following conditions (here, f^n stands for multiple iteration of the function f, i.e. $f^0 := f, \quad f^{i+1} := f \circ f^i := f(f^i(\cdot))$):*

- *Function $f : X \to X$ is topologically transitive on the bounded subset $\tilde{X}$ of the space $X \subset R^d$, i.e. for every pair of non-empty open sets $U, V \subset \tilde{X}$, there exists $n \geq 0$ such that $f^n(U) \cap V \neq \emptyset$.*
- *A function f has sensitive dependence on initial conditions if there exists $\sigma > 0$ such that, for any x which is an element of X and any neighborhood N of x, there exist $y \in N$ and $n \geq 0$, such that $|f^n(x) - f^n(y)| > \sigma$.*

In the other words, the chaotic dynamic system has property that all trajectories are bounded but rapidly diverge from any point of the state space. At the same time, each chaotic trajectory visits infinitely many times arbitrarily closely any point of the attractor.

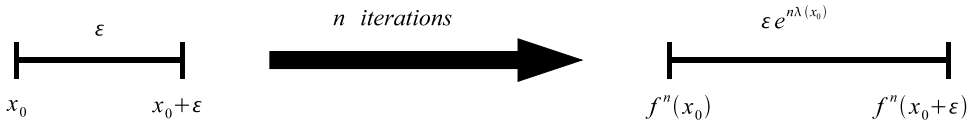


Figure 1.5: Definition of the Lyapunov exponent [74].

1.2.3 Lyapunov exponents

A definition of the sensitive dependence on initial conditions was introduced in Sec. 1.2.2. Lyapunov exponent $\lambda(x_0)$ which is defined for any point $x_0 \in X$ may be used as quantitative measure for the sensitive dependence on initial conditions. Lyapunov exponent may be readily computed for a one-dimensional map such as the logistic map [5]. If a system is allowed to evolve from two slightly differing initial states, x_0 and $x_0 + \varepsilon$, then after n iterations their divergence may be characterized as:

$$|f^n(x_0 + \varepsilon) - f^n(x_0)| = \varepsilon e^{n\lambda(x_0)}, \tag{1.5}$$

where the Lyapunov exponent λ_0 gives the average rate of divergence (see Fig. 1.5). In general case, λ depends on the initial conditions, therefore the average value is determined. Practically, the Lyapunov exponent may be calculated as limit [74]:

$$\lambda(x_0) = \lim_{n\to\infty}\lim_{\varepsilon\to 0}\frac{1}{n}\log|\frac{f^n(x_0+\varepsilon) - f^n(x_0)}{\varepsilon}| = \lim_{n\to\infty}\frac{1}{n}\log|\frac{df^n(x_0)}{dx_0}| \tag{1.6}$$

or

$$\lambda(x_0) = \lim_{n\to\infty}\frac{1}{n}\log|\frac{d}{dx_0}f^n(x_0)| = \lim_{n\to\infty}\frac{1}{n}\log\prod_{k=0}^{n-1}|f'(x_k)| =$$

$$= \lim_{n\to\infty}\frac{1}{n}\sum_{k=0}^{n-1}\log|f'(x_k)|. \tag{1.7}$$

Derivative $f'(x_k)$ shows the speed of divergence of the function f in relation to the increase of the value x from x_k to x_{k+1}. Limit is equal to

average value of logarithm of the derivative function after n iterations. It shows the speed of diverge of the nearest trajectories during the discrete time n. If λ is negative, slightly separated trajectories converge and the evolution is not chaotic. Otherwise, if λ is positive, nearby trajectories diverge; the evolution is sensitive to initial conditions and therefore chaotic. For higher-dimensional systems, the calculation of Lyapunov exponents is more challenging than in the one-dimensional case. However, the idea is the same: the measurement of the average rate of divergence of neighboring trajectories on the attractor [61]. To account for the accuracy of the observation more useful information gives the Kolmogorov-Sinai entropy, which will be discussed later on in Section 1.2.4.

From the cryptographical point of view, the Lyapunov exponent is a measure of the effectiveness of cryptographic systems. The higher value of λ the smaller iterations are necessary to achieve the required degree of diffusion or confusion of information.

1.2.4 Kolmogorov-Sinai entropy

The Lyapunov exponent (see Sec. 1.2.3) gives a first quantitative information on how rapidly we loose the ability of predicting the evolution of the system. In this respect, the Kolmogorov-Sinai (KS) entropy K supplies a more refined information [42]. The error in the initial state is due to the maximal resolution when is uses for observing the system. K can is defined as follows: consider the trajectory $\mathbf{x}(t) = (x_1(t), x_2(t), ..., x_N(t))$ and partition the phase space into n hypercubes of side ϵ. Let $P_{i_0,i_1,...,i_n}$ be the joint probability that the point $\mathbf{x}(0)$ lies in the i_0-th cell, $\mathbf{x}(\tau)$ in the i_1-th cell, ..., and $\mathbf{x}(n\tau)$ lies in the i_n-th cell. Then, according to Shannon, the quantity

$$K_n = -\sum_{i_0 \ldots i_n} P_{i_0 \ldots i_n} \ln P_{i_0 \ldots i_n} \tag{1.8}$$

is the measure of the amount of information necessary to specify the trajectory to within a precision ϵ, assuming only the probabilities $P_{i_0 \ldots i_n}$ are known a priory. It follows that $K_{n+1} - K_n$ is the additional amount of information required to specify which cell $\mathbf{x}(n\tau + \tau)$ it will fall in. The

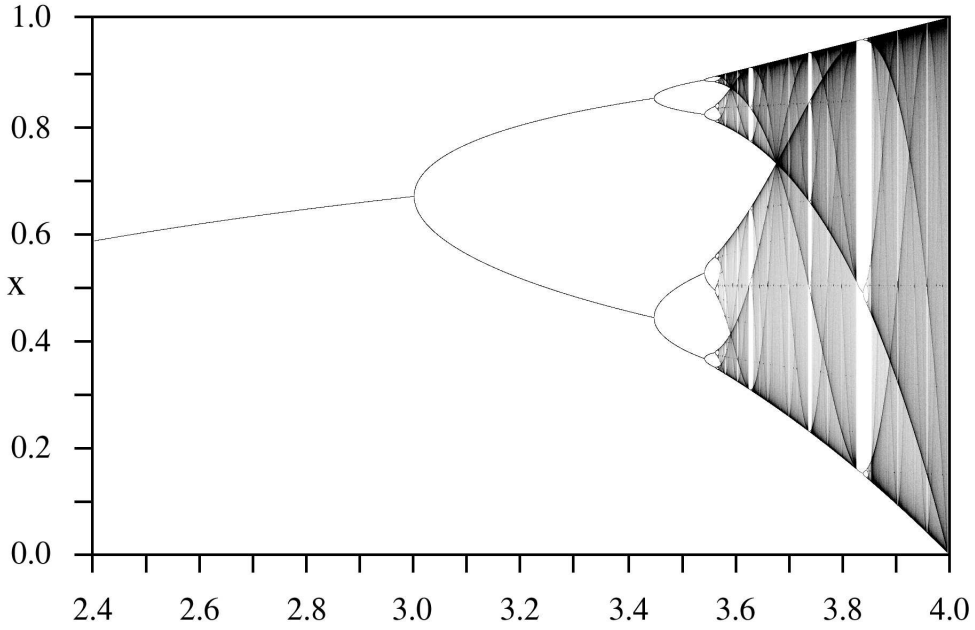


Figure 1.6: A bifurcation diagram for the Logistic map: $x_{n+1} = rx_n(1-x_n)$. The most unpredictable behavior may occur if $r = 4$.

K-entropy is defined as the average rate of loss of information [74]:

$$K = \lim_{\tau\to 0}\lim_{\epsilon\to 0}\lim_{N\to\infty}\frac{1}{N\tau}\sum_{n=0}^{N-1}(K_{n+1}-K_n) = \\ = -\lim_{\tau\to 0}\lim_{\epsilon\to 0}\lim_{N\to\infty}\frac{1}{N\tau}\sum_{i_0\ldots i_{N-1}} P_{i_0\ldots i_N}\ln P_{i_0\ldots i_N}. \qquad (1.9)$$

We see that K is the average rate of the information loss. For non-chaotic systems, $K = 0$, i.e., there is no loss of information because initially close points on a trajectory remain close together as time evolves. For chaotic systems, however, initially close points separate exponentially on average, and therefore joint probabilities for cell occupations decrease exponentially with time. Thus, $K > 0$ for chaotic systems. For truly (non-deterministic) random systems, initially close points take on a statistical distribution over all the allowed new cells. Thus if $P(i_0) \approx \epsilon$, then $P(i_0, i_1) \approx \epsilon^2$, etc., and so $K \to \infty$ as $\epsilon \to 0$ for pure randomness. The K-entropy is therefore useful not only for distinguishing regular from the chaotic behavior, but also for distinguishing deterministic chaos from noise [60].

1.2.5 Bifurcation

Bifurcation is usually referred to as the qualitative transition from regular to chaotic behavior by changing the control parameter [33]. For example, Feigenbaum scenario is one of the types of the bifurcations (see Fig. 1.6). At the bifurcation point the number of stable states is doubling. With the parameter increasing the doubling happens more and more frequently, and leads to chaotic behavior of the system. In cryptographic applications the choice of control parameter value determines the unpredictability of the system. If the parameter is used as the key, then the whole space of possible keys must generate the chaotic behavior of the system.

Chaotic property	**Cryptographic property**
Chaotic system: - nonlinear transformation - infinite number of state - infinite number of iterations	Pseudo-chaotic system: - nonlinear transformation - finite number of state - finite number of iterations
Initial state	Plaintext
Final state	Ciphertext
System parameters	Key
Ergodicity	Confusion
Sensitivity to initial conditions/control parameter	Diffusion with a small change in the plaintext/secret key
Mixing property (topological transitivity)	Diffusion with a small change in one plain-block of the whole plaintext
Structure complexity	Algorithm complexity

Table 1.1: Analogy between chaos and cryptography properties [2].

1.3 Summary

This chapter introduced some preliminary knowledge about cryptography and chaotic dynamics. The main purpose was to show that there is close relation between cryptography and dynamical systems theory. Therefore, methods from automatic control theory can be considered for application in

cryptography. The analogy between dynamical systems theory and cryptography is readily illustrated by Tab. 1.1.

Chapter 2

Chaos-based communication

During the last two decades many chaos based communication schemes have been developed: chaos synchronization (additive mixing, active passive decomposition), chaos shift keying, and more. The security of traditional encryption schemes based on integer number theory have been studied for a long time and is considered to be reliable. In contrast, the security of chaotic communication schemes often relies on a mixture of analytic methods and intuition. Encryption and cryptanalysis using chaotic dynamics is a relatively new field that has been studied for nearly a decade. A description of its current state is given by Tao-Yang et. al in [84]:

> **"In classical cryptology, the cryptography is a systematic science with well established analytical and synthetic principles, and the cryptanalysis is rather like an art depending heavily on intuition and experience than a science. Also, chaotic cryptography has been developed rapidly in recent years while chaotic cryptanalysis is still at its beginning with very few results littered among a huge ocean of chaotic cryptography literature."**

In the sequel we aim to give a more detailed picture of the above quoted situation.

2.1 Overview of chaos-based communication schemes

2.1.1 Schemes requiring chaos synchronization

A large number of communication schemes that are based on chaos synchronization have been proposed during the last two decades [64; 8; 41; 82; 22; 63]. In this section, the phenomena of chaos synchronization will be discussed.

Chaotic synchronization schemes. There are many interpretations and definitions of the synchronization term [70]. Several forms of synchronization have been proposed for the chaotic systems. A typical and most widely-used scenario of the chaotic synchronization is *identical synchronization*, where the state of response system converges asymptotically to the state of the drive system. Recently, two forms of synchronization, called *phase synchronization* [67] and *generalized synchronization* [1; 73] have been introduced.

1. *Identical synchronization*: Two continuous-time chaotical systems

$$\frac{d\mathbf{x}}{dt} = \mathbf{F}(\mathbf{x}) \tag{2.1}$$

and

$$\frac{d\mathbf{x}'}{dt} = \mathbf{F}'(\mathbf{x}') \tag{2.2}$$

are said to *synchronize identically* if

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

for any combination of initial states $\mathbf{x}(0)$ and $\mathbf{x}'(0)$. From a communication point of view, we may think of system (2.1) as the transmitter and system (2.2) as the receiver. If the same initial condition is chosen for the transmitter and the receiver, i.e. $\mathbf{x}(0) = \mathbf{x}'(0)$, the both systems will evolve in a synchrony in the sense that, $\mathbf{x}'(t)$ will continue being equal to $\mathbf{x}(t)$ for all $t > 0$. The signal $s_i(t)$ which is transmitted by a communication channel is a linear combination

of basis functions $g_j(t)$. We consider the case when only one basis function $g(t)$ is used and we assume that $s_i(t) \equiv g(t)$. At the receiver side, we must recover the scalar basis function $g(t) = H(\mathbf{x}(t))$ which has been derived from the state of the drive system (2.1). The basis function $g(t)$ can be recovered by synchronizing the state of the response system identically with the drive system and applying the same function $H(\cdot)$. In particular, if $\mathbf{x}'(t)$ can be made to converge to $\mathbf{x}(t)$ then the estimation $\hat{g}(t) = H(\mathbf{x}'(t))$ will converge to $g(t)$.

2. *Phase synchronization*: This scenario of the synchronization of two coupled systems occurs if the difference $|\phi'(t) - \phi(t)|$ between the "phases" of the two systems is bounded by a constant [67], where the "phase" $\phi(t)$ is some monotonically increasing function of time suitably chosen.

3. *Generalized synchronization*: This type of synchronization occur mainly when the coupled chaotic systems are different, although it has also been used between identical chaotic systems. Chaotic systems (2.1) and (2.2) are said to exhibit *generalized synchronization* if there exists a transformation Φ such that

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

where the properties of the transformation Φ are independent of the initial conditions $\mathbf{x}(0)$ and $\mathbf{x}'(0)$. If the transformation Φ is invertible, then

$$\hat{g}(t) = H(\Phi^{-1}(\mathbf{x}'(t)))$$

approaches $g(t)$. Identical synchronization is the particular case of generalized synchronization when Φ is the identity [73]. A complete overview of generalized synchronization is given by K. Pyragas in [68]. In some cases the unauthorized receiver can use a receiver with dynamics that is different from the dynamics of the transmitter, and decode the message using generalized synchronization between transmitter and receiver with different parameters. The use of generalized

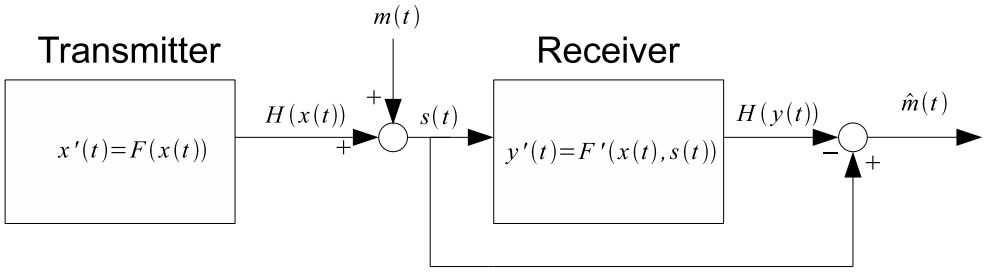


Figure 2.1: Chaotic communication scheme based on chaos synchronization and chaotic masking of a message with a chaotic component. The transmitter state $x(t)$ synchronizes to the receiver state $y(t)$. A scalar $H(x(t))$ is calculated from the transmitter state $x(t)$. A message $m(t)$ is added to the chaotic scalar, and the sum of the two is transmitted. At the receiver the message $\hat{m}(t)$ is reconstructed by subtracting the chaotic scalar $H(y(t))$ from the received signal $s(t)$. The message magnitude $|m(t)|$ has to be kept small compared to the chaotic scalar $H(x(t))$ in order to maintain synchronization between transmitter and receiver.

synchronization for breaking chaotic encryption scheme is described in [85].

In our chaos-based decryption method, that will be introduced later, in the Chapter 3, we are concerned with recovering the basis functions exactly, so we focus only on the *identical synchronization*.

Chaotic masking. Communication schemes that are based on chaos synchronization and chaotic masking of the chaotic signal with a message are described in [22] and illustrated in Fig. 2.1. In chaotic masking communication schemes a message signal is added to a chaotic signal generated by the transmitter dynamics and the sum of the two is transmitted. At the receiver which is synchronized to the transmitter the chaotic component is subtracted from the received signal to recover the original transmitted message. In Fig. 2.1 the transmitter state evolution is given by the chaotic dynamics

$$\frac{dx}{dt} = \mathbf{F}(x(t)). \tag{2.3}$$

A chaotic scalar $H(x(t))$ which is a function of the transmitter state $x(t)$ is added to the message $m(t)$. The transmitted signal $s(t)$ is governed by

$$s(t) = H(x(t)) + m(t). \tag{2.4}$$

The evolution of the receiver state $y(t)$ dynamics is given by the dynamics

$$\frac{dy}{dt} = \mathbf{F}(y(t), s(t)). \tag{2.5}$$

The transmitter state $x(t)$ synchronizes to the receiver state $y(t)$ at the rate of the largest Lyapunov exponent λ, so that

$$|y(t) - x(t)| \approx e^{-\lambda t}.$$

At the receiver, the estimation $\hat{m}(t)$ for the message $m(t)$ is calculated by subtracting the estimation $H(y(t))$ of the chaotic component $H(x(t))$ that was added to the message at the transmitter:

$$\hat{m}(t) = s(t) - H(y(t)). \tag{2.6}$$

The addition of a message signal $m(t)$ to the chaotic scalar $H(x(t))$ at the transmitter can degrade the quality of the synchronization between the transmitter and the receiver. It is assumed that for masking, the power level of massage $m(t)$ is significantly lower than that of $H(x(t))$ added to the message:

$$|m(t)| \ll |H(x(t))|. \tag{2.7}$$

2.1.2 Chaos Shift Keying

Chaos shift keying (CSK) was first proposed in [62; 24]. The idea is to encode digital symbols with chaotic basis signals.

Modulation and Demodulation. Chaos shift keying communication scheme, often termed as parameter modulation scheme, is described in [44] and illustrated in Fig. 2.2. In CSK the transmitter dynamics is dissipative and chaotic and the transmitter state trajectory converges to a strange attractor. A message is transmitted by changing one or more parameters of the transmitter dynamics which results in a change of the attractor dynamics. At the receiver the message is decoded by estimating

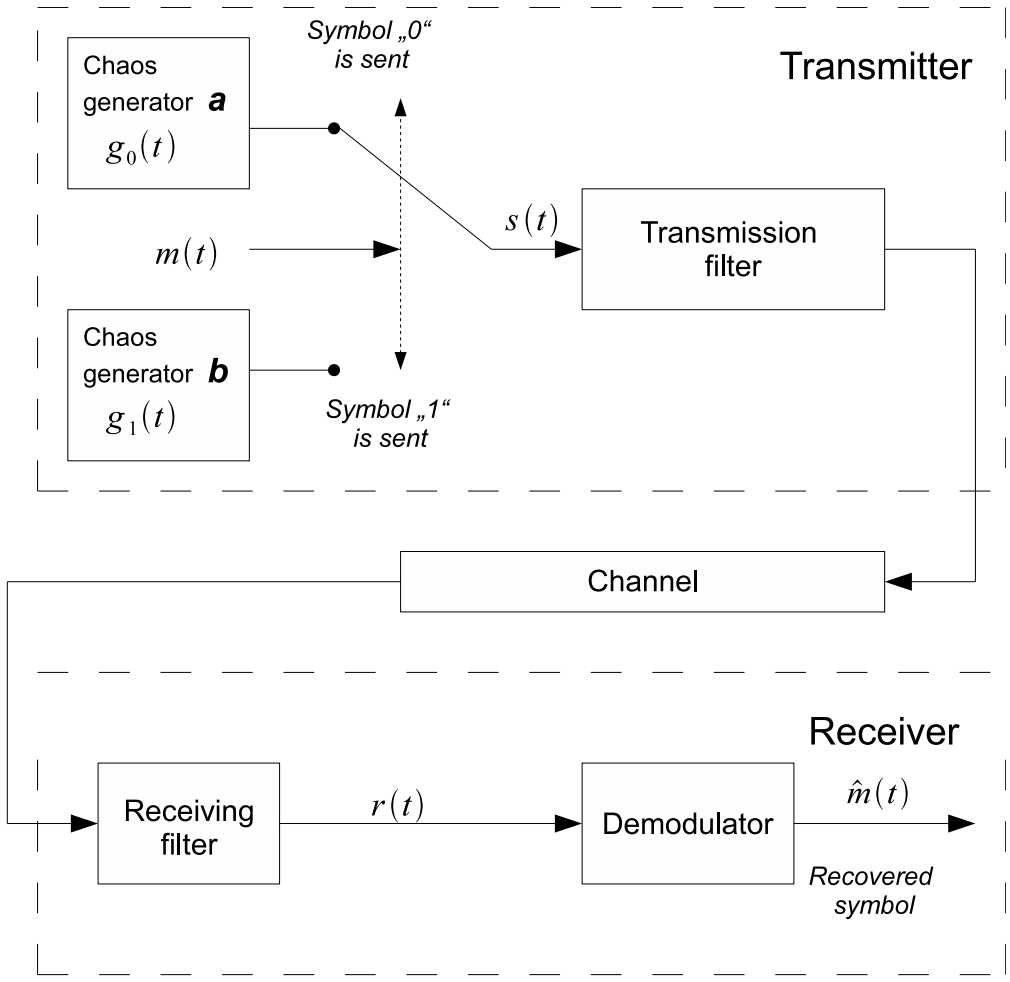


Figure 2.2: Binary chaos shift keying digital communication system.

to which message the received chaotic attractor corresponds. The fundamental principle of the CSK can be described in a more detail as follows. The transmitter consists of M chaos generators. In the case, when we uses a binary alphabet, only two chaos generators are needed. In the Fig. 2.2, the transmitter consists of two chaos generators a and b, producing signals $g_0(t)$ and $g_1(t)$, respectively. If a binary symbol "0" is to be sent during the interval $[(l-1)T_b, lT_b]$, g_0 is transmitted by the communication channel, and if the binary symbol "1" is to be sent, g_1 is transmitted. Here, T_b is the bit duration and l is a number of the transmitted symbol. In [62], the CSK scheme is based on the self-synchronization property of the chaotic systems. In the Fig. 2.3 the receiver structure based on the

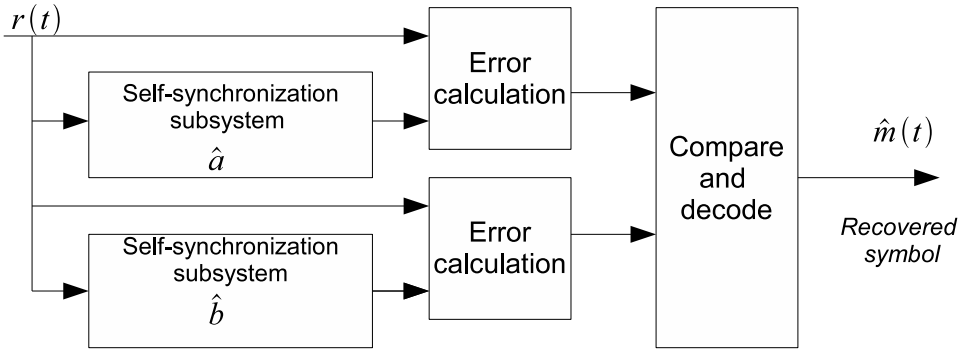


Figure 2.3: Synchronization-error-based CSK demodulator.

self-synchronization property is shown. The incoming signal $r(t)$ is used for drive two self-synchronization subsystems $\hat{a}$ and $\hat{b}$, which are matched to a and b chaos generators, respectively. When the transmitted signal is $g_o(t)$, the subsystem $\hat{a}$ will be synchronized with the incoming signal while $\hat{b}$ is not, and when the transmitted signal is $g_1(t)$, the subsystem $\hat{b}$ will be synchronized with the incoming signal. Therefore, by measuring the error between the incoming signal and the output of the self-synchronization subsystems, the transmitted symbol can be recovered.

In other words, the receiver needs to determine to which of the allowed attractors the transmitter dynamics converged, based on the received signal $r(t)$. The transmitted signal $s(t)$ is typically a scalar, while the transmitter dynamics can be of high dimension. The transmitter can use *coherent* or *non-coherent detection* techniques [44].

Coherent detection. In communication the term *coherent detection* implies that the shape of the transmitted waveforms is known to the receiver which can correlate the noisy received signal with its expected waveform, to maximize the signal to noise ratio at the output of the correlator. Coherent detection of the chaotic signals using correlator-based receivers was studied in detail in [43; 44]. Receivers in which exact copies of all basis functions are known are called coherent receivers. The block diagram of a correlator-based receiver using binary chaos shift keying modulation is shown in the Fig. 2.4.

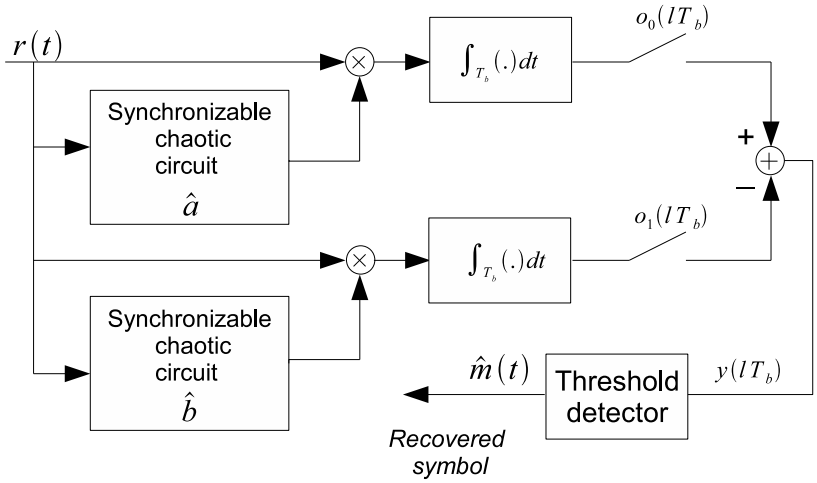


Figure 2.4: Block diagram of coherent correlation CSK receiver.

The two synchronizable chaotic circuits in the receiver attempt to reproduce the two basis functions, given the received noisy sample function $r(t)$. An acuasition time T_s is assumed for the synchronization circuits to lock to the incoming signal. The recovered basis functions are then correlated with the received signal for the remainder of the bit duration T_b. Then, the outputs of the correlators are sampled and compared.

Non-coherent detection. In the case of *non-coherent demodulation* the receiver does not know the shape of the transmitted chaotic basis signals. Detection has to be done based on some distinguishable property of the basis signals. Different attractors may differ in variance, meaning of the absolute value, dynamic range, and many other statistical properties [44]. The main advantage in the using of the non-coherent decoding methods is that the receiver is not required to synchronize with the transmitter. It only needs to determine to which one of the allowed attractors the trajectory has converged. In addition, the non-coherent receivers are often simpler than their coherent counterparts. Suppose chaotic basis signals with different bit energies are used to transmit the binary information. If a binary "0" is to be sent during the interval T_b, a chaotic basis signal $g_0(t)$ with mean bit energy E_0 is transmitted, and if binary "1" is to be sent, a chaotic basis signal $g_1(t)$ with mean bit energy E_1 is transmitted. The required chaotic

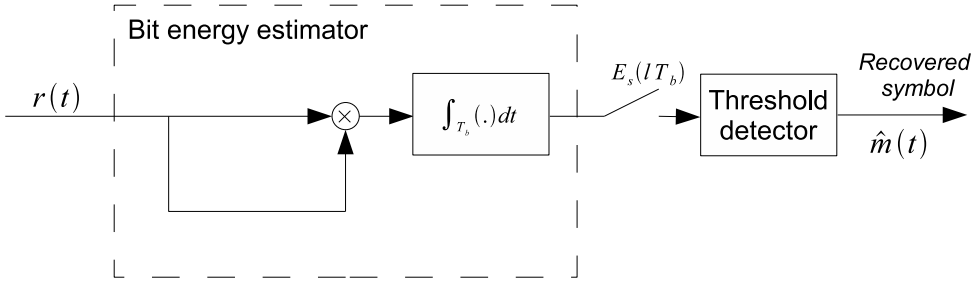


Figure 2.5: CSK receiver based on bit energy estimator.

signals can be generated by two chaos generators with different average bit energies. As alternative, the same chaos generator can be used to produce two signals of different bit energies by using two amplifiers of different gain. In both cases, the bit energy can be estimated by a correlator at the receiver, as shown in Fig. 2.5. Assume that only additive noise corrupts the transmitted signal and the noise power limited by the receiving filter, i.e.,

$$r(t) = s(t) + n'(t), \tag{2.8}$$

where, $s(t)$ denotes the transmitted signal and $n'(t)$ is the noise component at the output of the receiving filter. For the lth received symbol, the energy bit $E_s(lT_b)$, is defined by

$$\begin{aligned} E_s(lT_b) &= \int_{(l-1)T_b}^{lT_b} r^2(t)dt = \\ &= \int_{(l-1)T_b}^{lT_b} s^2(t)dt + 2\int_{(l-1)T_b}^{lT_b} s(t)n'(t)dt + \int_{(l-1)T_b}^{lT_b} [n'(t)]^2 dt. \end{aligned} \tag{2.9}$$

In the noise-free case, the second and third integrals in (2.9) are zero. Therefore, $E_s(lT_b)$ is equal to either one of the following two bit energies:

$$\begin{aligned} E_s^0(lT_b) &= \int_{(l-1)T_b}^{lT_b} g_0^2(t)dt \\ E_s^1(lT_b) &= \int_{(l-1)T_b}^{lT_b} g_1^2(t)dt. \end{aligned} \tag{2.10}$$

In convectional modulation schemes, the bit energy is fixed for a given symbol.

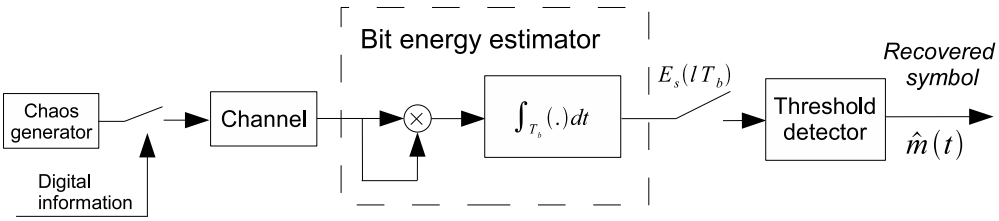


Figure 2.6: Block diagram of non-coherent COOK modulation scheme.

2.1.3 Chaos-On-Off-Keying

Chaos-on-off-keying (COOK) is only a special case of the chaos shift keying scheme (CSK) with non-coherent demodulator [46]. It uses one chaos generator, which is switched "on" or "off" to transmit symbols "1" and "0", respectively, as shown in Fig. 2.6. The major disadvantage of the CSK system is that the threshold value of the decision circuit depends on the noise level, also appears in COOK. This means that using COOK we can maximize the distance between the elements of the signal set, but the threshold level required by the decision circuit depends on the noise level. The threshold can be kept constant by applying the differential chaos shift keying method.

2.1.4 Differential Chaos Shift Keying

The differential chaos shift keying (DCSK) modulation was proposed in [48]. In differential chaos shift keying scheme, every bit to be transmitted is represented by two chaotic sample functions. The first sample function serves as a reference while the second one carries the information. Bit "1" is sent by a chaos generator twice in succession, while for bit "0", the reference chaotic signal is transmitted, followed by an inverted copy of the same signal [36]. Thus for the lth symbol period, we have

$$s(t) = \begin{cases} g(t), & \text{for } (l-1)T_b \leq t < (l-1/2)T_b \\ g(t - T_b/2), & \text{for}(l-1/2)T_b \leq t < lT_b \end{cases} \tag{2.11}$$

if "1" is to be transmitted, and

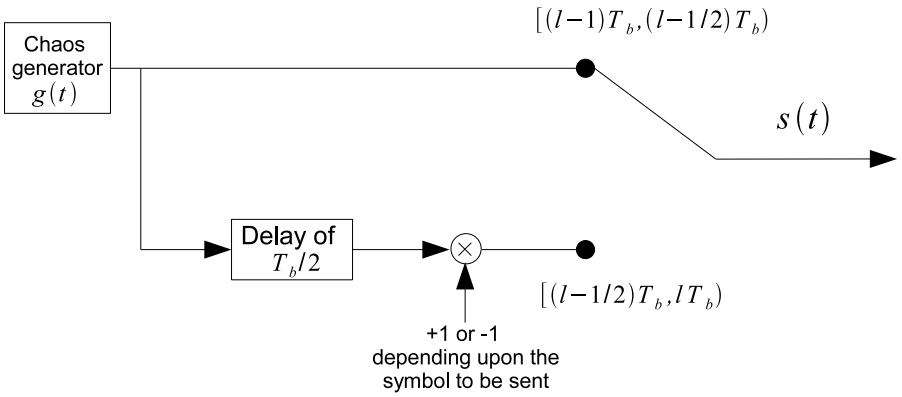


Figure 2.7: Block diagram of differential chaos shift keying modulator.

$$s(t) = \begin{cases} g(t), & \text{for } (l-1)T_b \leq t < (l-1/2)T_b \\ -g(t-T_b/2), & \text{for}(l-1/2)T_b \leq t < lT_b \end{cases} \tag{2.12}$$

if "0" is to be sent [49].

Fig. 2.7 shows a block diagram of a DCSK transmitter. Since each bit is mapped to the correlation between successive segments of the transmitted signal of length $T_b/2$, the information signal can be recovered by a correlator. A block diagram of a DCSK receiver is shown in Fig. 2.8. The output of the correlator at the and of the lth symbol duration is given by

$$\begin{aligned} y(lT_b) &= \int_{(l-1/2)T_b}^{lT_b} r(t)r(t-T_b/2)\,dt = \\ &= \int_{(l-1/2)T_b}^{lT_b} [s(t)+n'(t)][s(t-T_b/2)+n'(t-T_b/2)]\,dt = \\ &= \int_{(l-1/2)T_b}^{lT_b} [s(t)s(t-T_b/2)]\,dt + \int_{(l-1/2)T_b}^{lT_b} [s(t)n'(t-T_b/2)]\,dt + \\ &+ \int_{(l-1/2)T_b}^{lT_b} [n'(t)s(t-T_b/2)]\,dt + \\ &+ \int_{(l-1/2)T_b}^{lT_b} [n'(t)n'(t-T_b/2)]\,dt \end{aligned} \tag{2.13}$$

where $n'(t)$ is the noise component at the output of the receiving filter. The second term in (2.13) can be positive or negative, depending on whether a "1" or "0" has been transmitted. Also, all the other integral terms

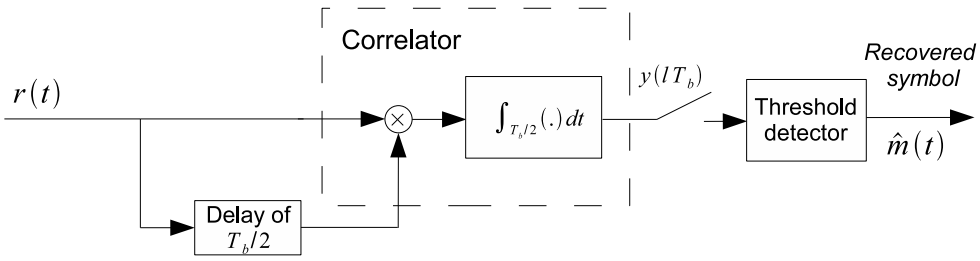


Figure 2.8: Block diagram of differential chaos shift keying demodulator.

have a zero meaning. Thus, the threshold detector can be set optimally at zero, the decision threshold is zero independently of the noise spectral density (E_s/N_0) [49]. By contrast with the CSK and COOK schemes discussed in Section 2.1.2 and Section 2.1.3, DCSK is an antipodal modulation scheme. The main advantage results from the fact that the reference and information-bearing sample functions pass through the same channel so they undergo the same channel distortion. DCSK can also operate over a time-varying channel if the parameters of the channel remain constant for the bit duration T_b. The main drawback of DCSK, however, is that it can only transmit at half of the data rate of the other systems because it spends half of the time transmitting the non-information-bearing reference samples [49]. One way to improve the data rate is to use a multilevel modulation scheme [45]. Alternatively, one may solve the estimation problem directly by modifying the modulation scheme such that the transmitted energy is kept constant. Frequency-modulated differential chaos shift keying scheme is an example of the latter approach.

2.1.5 Frequency-Modulated Differential Chaos Shift Keying

The objective of frequency-modulated differential chaos shift keying (FM-DCSK) is to produce a wideband chaotic signal with constant E_s. The FM-DCSK was proposed by Kolumban et. al. [47]. In this scheme, a chaotic frequency modulated signal generator is needed. The chaotic signal

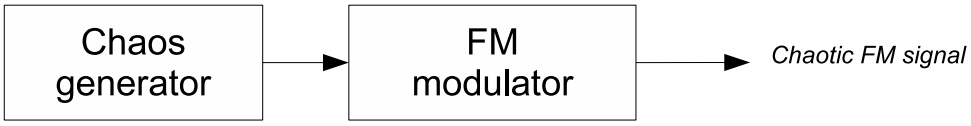


Figure 2.9: Chaos frequency-modulated signal generator.

to be input of an FM modulator. A block diagram of a FM-DCSK generator is shown in Fig. 2.9. The output of this FM modulator is chaotic, bandlimited, and its power spectral density is uniform. The operation of the demodulator is the same as in DCSK, the only difference being that not the chaotic, but the FM modulated signal is the input to the DCSK modulator [49].

2.1.6 Quadrature Chaos Shift Keying

In [29] authors proposed a multilevel version of the differential chaos shift keying (DCSK), the so-called quadrature chaos shift keying (QCSK) communication scheme with double data and higher spectral efficiency. In QCSK a two-bit symbol is encoded as a linear combination of two orthogonal waveforms, sine and cosine. Fig. 2.10 and Fig. 2.11 shows a block diagram of the modulator and demodulator of the QCSK communication system, respectively. In this diagrams, each transmitted symbol consists of two bits of the information. Here, the bit duration is T_b and the symbol duration is $T_s = 2T_b$. The modulation scheme can be described as follows. Let $c(t)$ be a chaotic reference signal defined for $t \in [0, T_s/2]$. This reference signal has a zero mean value. Next, for producing of $d(t)$ we use the $T_s/2$-delayed version of reference signal $c(t)$. Further, we construct the complementary signal $e(t)$ by shifting the phase of all frequency components in $d(t)$ by $\pi/2$, which is accomplished by standard digital signal processing (DSP) techniques. In the QCSK modulation scheme, $c(t)$ is sent during the first half symbol period, i.e., $[0, T_s/2)$ while the information-bearing signal $s(t)$ is sent during the second half symbol period, i.e., $[T_s/2, T_s)$.

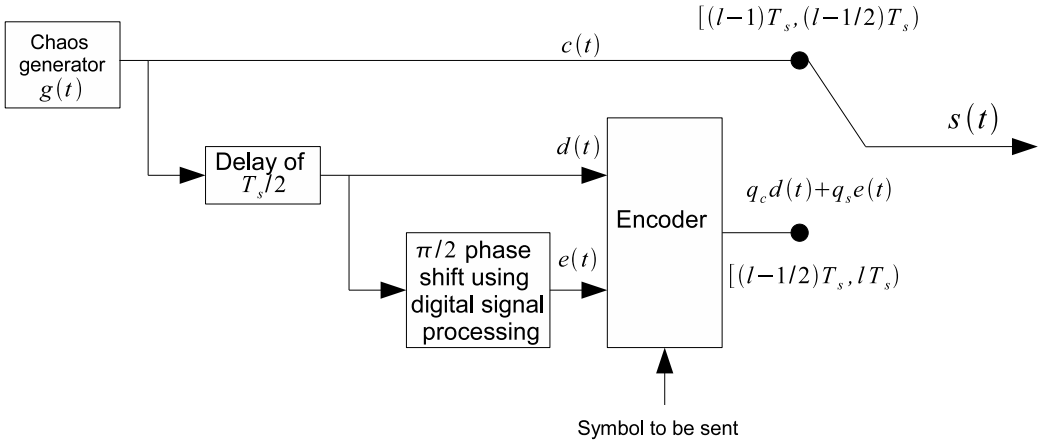


Figure 2.10: Block diagram of the quadrature chaos shift keying scheme. Modulator.

Here, $s(t)$ is a linear combination of two orthogonal waveforms $d(t)$ and $s(t)$.

$$s(t) = q_c d(t) + q_s s(t), \tag{2.14}$$

where q_c and q_s are two bits of information to be sent within the symbol period T_s. At the demodulator, $d(t)$ and $e(t)$ are the first estimated from the noise version of the reference signal $\hat{c}(t)$. Suppose the estimated $d(t)$ and $e(t)$ are $\hat{d}(t)$ and $\hat{e}(t)$ respectively. Then, demodulation can be done by correlating the signal received in the second half symbol period, i.e., $[T_s/2, T_2)$, with $\hat{d}(t)$ and $\hat{e}(t)$ [49]. Based on the correlation results a decision on the symbol s_i (two bits of information) received is taken by a decision circuit according to estimated value $q_c + iq_s$. The QCSK scheme has the advantage over DCSK of double data rate for a given bandwidth with the same bit error rate performance.

2.2 Chaos-based cryptosystems and possible attacks of them

Recent years more attention has been paid to the development of cryptographic systems with chaotic dynamics. As already underline in Chapter

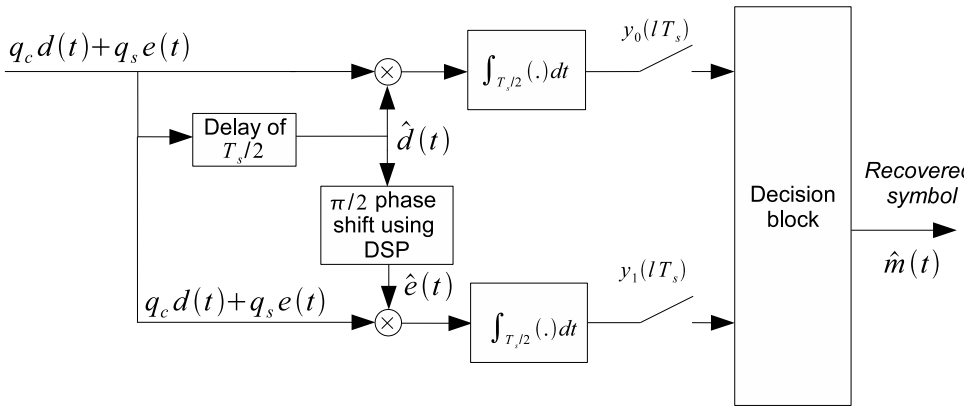


Figure 2.11: Block diagram of the quadrature chaos shift keying scheme. Demodulator.

1, these is the close relationship between chaos and cryptography (see Tab. 1.1). Many cryptographic systems have been proposed by researchers but most of these systems were broken later on. Developers of these systems did not face the cryptography before the invention of their cryptographic systems based on chaotic dynamics. Most of these researchers writing the new cryptographic algorithms have relied on their intuition, but not on the exact methods adopted in the cryptographic community. Such an approach resulted in cryptographically unreliable and slow algorithms.

These original thesis is devoted to the attempt of building of a stream cipher based on synchronization and implemented as a digital cryptosystem. It is an endeavor to use the original properties of chaos in the digital system. Before presenting our novel results on developing continuous time chaos-based digital cryptosystems later on, in Chapter 3, some digital cryptosystems based on chaos and some methods of cryptanalysis will be reviewed here.

2.2.1 Chaos-based encryption systems

Cryptographic systems can be divided into the analog and digital ones. Analog cryptosystems are based, as a rule, on synchronization and can be used in the analog channels with noise [64]. Synchronization details and

its types have been described by us earlier in the Section 2.1.1.

In the chaos-synchronization-based cryptosystems information is transmitted through one or more of random signals. There are several classes of analog systems based on chaotic dynamics: chaos masking [23; 39], chaos switching [62; 24], chaotic modulation [22], chaos control methods [35], inverse system approach [27]. In turn, digital chaos-based cryptosystems are adjusted for use in the computer cryptography. There are some of the methods proposed by researchers for use in the computer cryptography: chaotic stream ciphers via inverse system approach [28], stream ciphers based on chaos-based pseudo random bit generators (PRBG) [58], block ciphers based on chaotic round function or S -boxes [40], block ciphers based on forward/backward chaotic iterations [34], chaotic ciphers based on searching plain-bits in a chaotic pseudorandom sequence [6]. It should be noted that digital cryptosystems, in general, do not depend on synchronization. For more information about digital cryptosystems see [50]. All the computer models of chaos are the approximation of the mathematical chaos. Approximation to some extent transmits the properties of the original system only in the initial iterations, but in the limit ($n \rightarrow \infty$) gives the incorrect asymptotic approximation. Therefore, a more suitable terminology for the chaos implemented by computer approximation is the so-called pseudochaos.

2.2.2 Advantages and disadvantages of chaos-based encryption schemes

Comparing to the traditional encryption schemes, chaos based encryption schemes have several advantages [79]:

- Traditional encryption schemes are limited to integer number fields, while chaos based encryption schemes can be defined over continuous number field. More variety of functions that can be used for encryption is provided by this and can be used for encryption . It is possible to use chaos based encryption schemes that do not require digitization of the message as well (the traditional encryption

schemes require digitization of the data as they are defined over integer number fields).

- Traditional encryption schemes can be implemented only by using digital hardware, while chaos based encryption can be implemented directly using high speed analog component (optical or electrical) such as lasers, etc.

- In traditional encryption two circuits are needed: A digital circuit for encryption, and an analog circuit for broadband modulation. Encoding and broadband modulation in chaos based encryption schemes can be implemented using a single circuit.

- Non-periodic pseudo random waveforms that can be used to mask a message continuous waveform can be generated by chaotic dynamics. Pseudo-random sequences generated by traditional encryption schemes end up being periodic as they are implemented using digital hardware: a period that depends on the number of bits used to represent the state of the pseudo number sequence generator.

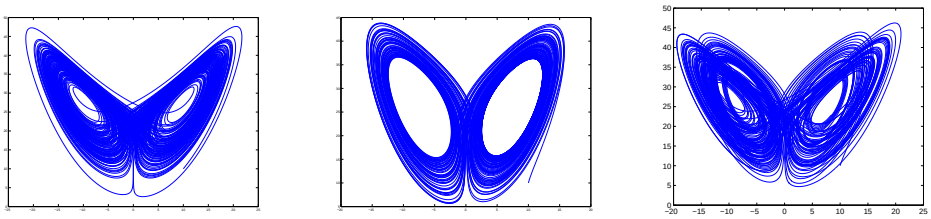
Chaotic encryption schemes disadvantages are following:

- Its security is not proven. Both claims form security and proposed cryptanalysis attacks are typically a mixture of mathematical reasoning with intuition. Chaotic encryption is a relatively new field of research, and it will take some time for its security analysis to mature.

- Typically the power efficiency, bandwidth efficiency, and bit error rate performance of chaos based communication schemes is inferior to that of traditional communication schemes.

2.2.3 Message signal extraction

Different methods have been proposed to attack chaos-cased encryption schemes. In some cases it is possible to break a chaos cryptosystem without



(a) (b) (c)

Figure 2.12: Lorenz attractor with different parameter values: (a) $\sigma_1 = 7.5$; (b) $\sigma_1 = 12.5$; (c) σ_1 is switched between 7.5 and 12.5 by the plaintext.

searching for the secret key k that was used to encrypt the message. This kind of attack is generally possible if $m(t)$ is a periodic signal or if it consists of periodic frames within a sufficiently long duration. This can be accomplished using different methods [2]: autocorrelation and cross-correlation analysis power spectral analysis and filtering technique (both linear and nonlinear), return map analysis, etc.

Power spectral and return map attack methods. As was mentioned in Chapter 2, the security is an important problem in the chaos-based communication systems. Power spectral analysis and return map are two powerful attack methods which permit to brake a chaos based communication schemes without knowing its parameter values and even without knowing the structure of the transmitter. In the sequel, these two methods are illustrated to attack a symmetric secure communication system based on the parameter modulation scheme.

In [26] author proposed a secure communication method based on the parameter modulation of a chaotic system and adaptive observer-based synchronization scheme. The transmitter of secure communication is represented through a Lorenz system generalization described by the following equations:

$$\begin{aligned} \dot{x_1} &= -\sigma_1 x_1 + \sigma_2 x_2 \\ \dot{x_2} &= r x_1 - x_2 - x_1 x_3 \\ \dot{x_3} &= x_1 x_2 - b x_3. \end{aligned} \tag{2.15}$$

In this example the system is implemented with the following standard

parameters $(\sigma_1, \sigma_2, r, b) = (10,\ 10,\ 28,\ 8/3)$. Author supposed that σ_1 is known with an uncertainty $\theta = \Delta\sigma_1 = 2.5$. The signal used for synchronization is x_1. The parameter σ_1 is modulated by a digital informational signal, so that it is $\sigma_1 - 2.5$ if the plaintext bit is "0", and $\sigma_1 + 2.5$ if the plaintext bit is "1". The bit duration T_b must be much larger than the convergence time of the adaptation law. The bit rate in the example is 0.2 bits/sec. The uncertain system (2.15) can be rewritten in a following compact form:

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \end{bmatrix} = \begin{bmatrix} -\sigma_1 & \sigma_2 & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \\ + \begin{pmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{pmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} (-y)\theta. \tag{2.16}$$

An adaptive observer-based receiver to the above system can be constructed as follows

$$C = [\ 1 \quad 0 \quad 0\ ]$$

$$y = C \cdot x = x_1$$

$$\theta = \Delta\sigma_1 = \pm 2.5$$

$$\begin{bmatrix} \dot{\hat{x_1}} \\ \dot{\hat{x_2}} \\ \dot{\hat{x_3}} \end{bmatrix} = \begin{bmatrix} -\sigma_1 & \sigma_2 & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{bmatrix} \begin{bmatrix} \hat{x_1} \\ \hat{x_2} \\ \hat{x_3} \end{bmatrix} + \begin{pmatrix} 0 \\ -\hat{x_1}\hat{x_3} \\ \hat{x_1}\hat{x_2} \end{pmatrix} + L(x_1 - \hat{x_1}) \tag{2.17}$$

$$L = [0\ 38\ 0\ ]^T.$$

The plaintext can be decrypted from the first derivative of the receiver uncertainty defined as:

$$\dot{\hat{\theta}} = -5y(x_1 - \hat{x_1}). \tag{2.18}$$

The dynamics above transmitter and receiver were simulated[1] with the

[1]Here, the MATLAB-SIMULINK ode4 Runge-Kutta procedure with a fixed step size 0.001 is used.

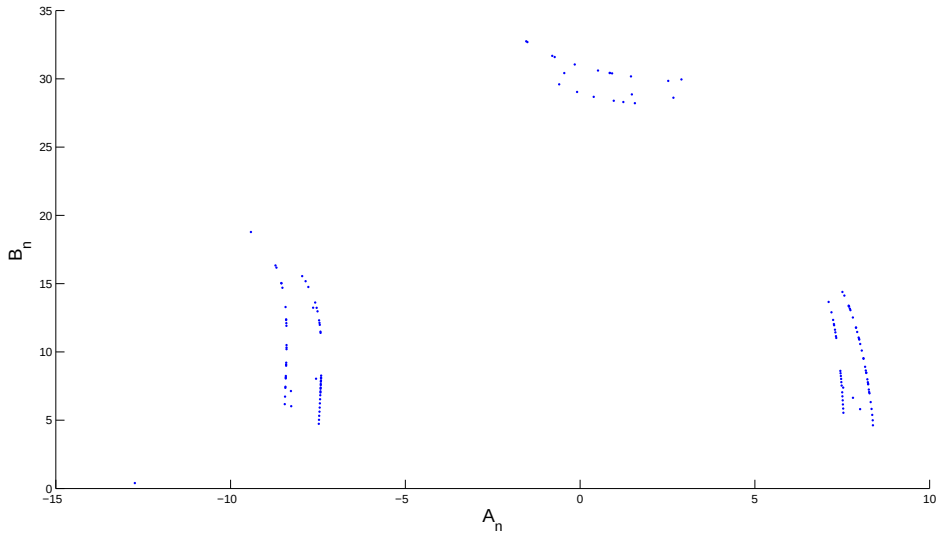


Figure 2.13: The return maps corresponding to σ=10 and σ=12.5.

following initial conditions:

$$x_1(0), x_2(0), x_3(0) = (10, 15, 10)$$
$$\hat{x_1}(0), \hat{x_2}(0), \hat{x_3}(0), \hat{\theta}(0) = (0, 0, 0, 0).$$

Proposed method has a low degree of security and such analysis of security was not included in the original work [26]. Making use of the power analysis attack and return map attack, the transmitted signal can be encrypted without knowing its parameter values and even without knowing the transmitter precise structure. Fig. 2.12 shows the Lorenz chaotic attractor for the different values of σ_1 proposed by the author, strong dependence of the attractor behaviour of the parameter σ_1 is observed. In Fig. 2.12(a) and Fig. 2.12(b) the attractor corresponding to $\sigma_1 = 7.5$ to $\sigma_1 = 12.5$ are shown, respectively. Both of the attractors are quite different and to recover the plaintext from the transmitted signal $y(t)$ the power analysis attack was used, firstly in [3]. This procedure consists of the three steps. First, the transmitted signal $y(t)$ is squared. Secondly, a low pass filter to $y^2(t)$ is employed. Finally, the low-pass filtered $y^2(t)$ is binary quantized. Fig. 2.14 illustrates the power analysis method. The low-pass filter

employed is a four pole Butterworth with a frequency cut-off of 0.5 Hz. The result is a good estimation of the plaintext, with small delays in some transitions. In comparing Fig. 2.14(a) with Fig. 2.14(e), it is obvious that power analysis exhibits good performance in the recovering of the plaintext.

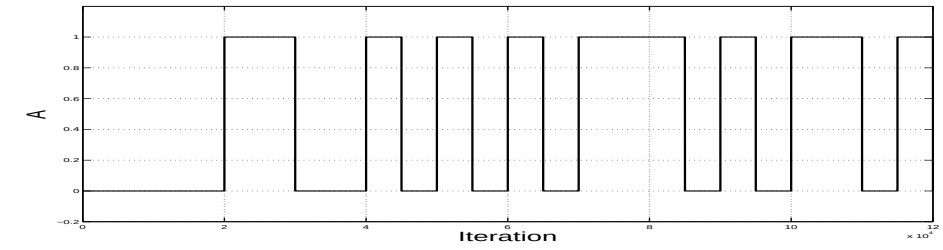
Now consider the return map analysis method. The return map attack method was first proposed by [66] to break chaotic switching and chaotic masking schemes based on the Lorenz system. Later on, this method was studied by [86] and [51]. However, the chaotic scheme proposed in [26] can be easily broken with the return map constructed from y_1 ciphertext as pointed out in [66]. Assuming that X_n and Y_n are the n-th maxima and n-th minima of y_1, respectively. As described by [66], the return maps X_{n+1} vs X_n and Y_{n+1} vs Y_n are not used directly, the linear combinations $A_n = (X_n + Y_n)/2$ and $B_n = X_n - Y_n$ are used to get better results. The return map A_n vs B_n has a very simple attractor, which is shown in Fig. 2.13. Note that there are three segments in the return map, and each segment is splits further into two strips. A small change of the bifurcation parameter σ_1 in the transmitter influences the attractor of the chaotic system. The result of the switching between two parameters value is the switching between two parallel strips of each segment. According to the line in which the point (A_n, B_n) falls on, one can easily unmask the current value of the plaintext. Later on, in the Section 3.5, both of the cryptanalysis methods will be used for security analysis of the anti-synchronization chaos shift keying method.

2.3 Summary

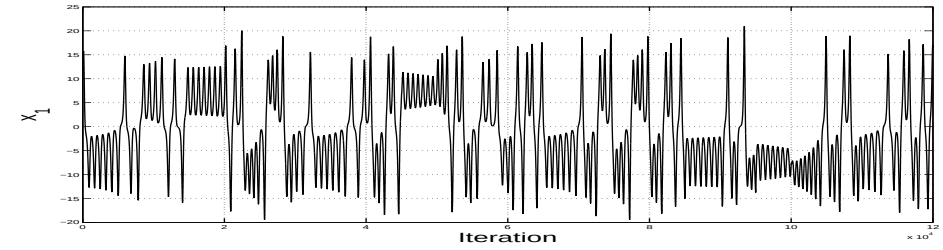
In this chapter, a survey of chaos-based communications has been presented. In particular, the properties of chaotic communication schemes

summarized and different aspects of using a chaotic dynamics in the communications are discussed: chaos synchronization, chaos shift keying, chaos-on-off-keying, differential chaos shift keying, frequency-modulated differential chaos shift keying etc.

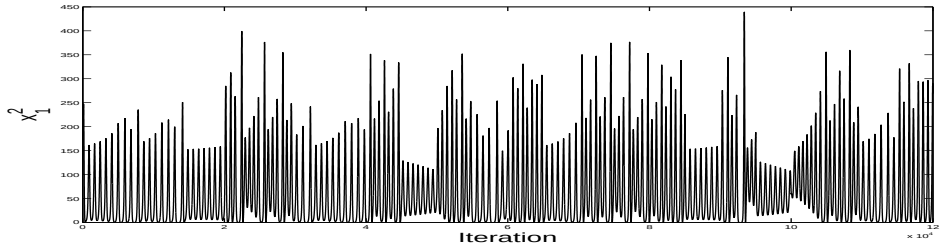
The history of chaotic secure communication is short and while its future uncertain. Despite their problematic security (the level of rigorously prover security is not very high), the chaotic encryption schemes already provide privacy, so required by a large range of applications. A clear advantage in using a chaotic encryption scheme is that it is the only type of encryption that does not require digitization of data and can be implemented using analog (electrical/optical) components. The rapid growth in wireless communications may create a new type of applications that will require cheap encryption of undigitized continuous waveforms using a simple analog hardware.



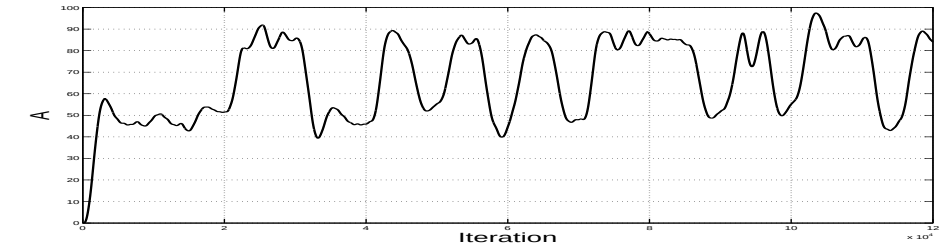
(a)



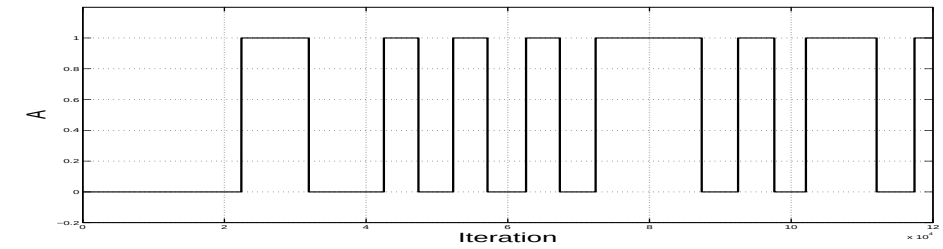
(b)



(c)



(d)



(e)

Figure 2.14: Time histories related with the decryption of the plaintext "000011001010101110101101" using power analysis attack. From up to down: the plaintext; the ciphertext, x_1; squared ciphertext signal, x_1^2; low pass filtered squared ciphertext signal; the reconstructed plaintext.

Chapter 3

Generalized Lorenz system in communication and encryption

This chapter introduces the so-called generalized Lorenz system (GLS) and investigates various encryption and communication schemes based on the GLS. Previously, in the Chapter 1, the relationship between cryptographic and chaotic systems was analyzed, while in the Chapter 2 the chaos-based communication schemes was introduced. The current chapter will present the original contribution of the thesis which is the study of the so-called generalized Lorenz chaotic system and its use for secure encryption and communication. Namely, the message embedded synchronization scheme for generalized Lorenz system will be introduced in Section 3.2. Section 3.4 then provides a novel modification of the general chaos shift keying scheme described in the previous chapter, the so-called anti-synchronization chaos shift keying (ACSK) based on Section 3.3 introducing the thorough theoretical original analysis of anti-synchronization phenomena in GLS. Section 3.5 provides security analysis of ACSK by using return map attack and power analysis, as well as by key analysis. Section 3.6 derives the synchronization results for GLS within dynamical complex networks, useful for possible application in communication. Results are briefly summarized in the final section.

3.1 Generalized Lorenz system and its synchronization

First, let us recall some previously published results on generalized Lorenz system classification and synchronization. Further details may be found in [11; 14; 18; 19].

Definition 3.1.1. *The following general nonlinear system of ordinary differential equations in R^3 is called a generalized Lorenz system (GLS):*

$$\dot{x} = \begin{bmatrix} A & 0 \\ 0 & \lambda_3 \end{bmatrix} x + \begin{bmatrix} 0 \\ -x_1 x_3 \\ x_1 x_2 \end{bmatrix}, \; A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \tag{3.1}$$

where $x = [x_1 \;\; x_2 \;\; x_3]^\top$, $\lambda_3 \in R$, and A has eigenvalues $\lambda_1, \lambda_2 \in R$, such that

$$-\lambda_2 > \lambda_1 > -\lambda_3 > 0. \tag{3.2}$$

The inequality (3.2) goes back to the well-known Shilnikov's chaos analysis near the homoclinicity and can be viewed as the necessary condition for the chaos existence, see more detailed discussion in [10; 44]. GLS is said to be *nontrivial* if it has at least one solution that goes neither to zero nor to infinity nor to a limit cycle. The following result, enabling the efficient synthesis of a rich variety of chaotic behaviors for GLS, has been obtained in [10]:

Theorem 3.1.2. *For the nontrivial generalized Lorenz system* (3.1)−(3.2)*, there exists a nonsingular linear change of coordinates, $z = Tx$, which takes* (3.1) *into the following generalized Lorenz canonical form:*

$$\dot{z} = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} z + cz \begin{bmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & \tau & 0 \end{bmatrix} z\,, \tag{3.3}$$

where $z = [z_1, z_2, z_3]^\top$, $c = [1, -1, 0]$ and parameter $\tau \in (-1, \infty)$.

Actually, the parameter τ plays important role of single scalar bifurcation parameter, while remaining parameters has only qualitative influence

being eigenvalues of the approximate linearization of GLS at the origin. These qualitative parameters are just required to satisfy robust condition (3.2), so that fine tuning may be done using the single scalar parameter τ only. In [9] GLS is further extended to the so-called hyperbolic-type generalized Lorenz systems (HGLS) which has the same canonical form as (3.4) but with $\tau \in (\infty, -1)$. In such a way, the parameter range to be used in the encryption later on is further extended. In [11] complete and nice classification of all related systems is given showing that many recently introduced in the literature classes are actually particular cases of the GLS or the HGLS.

Synchronization of GLS is based on yet another canonical form, the so-called **observer canonical form of GLS** provided by the following

Theorem 3.1.3. *Both nontrivial GLS (3.1) and its canonical form (3.3) are state equivalent to the following form:*

$$\frac{\mathrm{d}\eta}{\mathrm{d}t} = \begin{bmatrix} (\lambda_1+\lambda_2)\eta_1 + \eta_2 \\ -\eta_1[\lambda_1\lambda_2 + (\lambda_1-\lambda_2)\eta_3 + \frac{(\tau+1)\eta_1^2}{2}] \\ \lambda_3\eta_3 + K_1(\tau)\eta_1^2 \end{bmatrix} \tag{3.4}$$

$$K_1(\tau) = \frac{\lambda_3(\tau+1) - 2\tau\lambda_1 - 2\lambda_2}{2(\lambda_1-\lambda_2)}, \tag{3.5}$$

where $\eta = [\eta_1, \eta_2, \eta_3]^\top$, which is referred to as the observer canonical form. The corresponding smooth coordinate change and its inverse are

$$\eta = \begin{bmatrix} z_1 - z_2 \\ \lambda_1 z_2 - \lambda_2 z_1 \\ z_3 - \frac{(\tau+1)(z_1-z_2)^2}{2(\lambda_1-\lambda_2)} \end{bmatrix} \tag{3.6}$$

$$z = \begin{bmatrix} \frac{\lambda_1\eta_1+\eta_2}{\lambda_1-\lambda_2} \\ \frac{\lambda_2\eta_1+\eta_2}{\lambda_1-\lambda_2} \\ \eta_3 + \frac{(\tau+1)\eta_1^2}{2(\lambda_1-\lambda_2)} \end{bmatrix}. \tag{3.7}$$

Indeed, the above observer canonical form, when viewing $\eta_1 = x_1 = z_1 - z_2$ as the output, is almost in the form linearizable by output injection. This leads to the following observer-based synchronization of two copies of GLS.

Theorem 3.1.4. *Consider system (3.4-3.5) with the output η_1 and its uniformly bounded trajectory $\eta(t),\ t \geq t_0$. Further, consider the following system having input η_1^m and state $\hat{\eta} = (\hat{\eta}_1, \hat{\eta}_2, \hat{\eta}_3)^\top$:*

$$\frac{\mathrm{d}\hat{\eta}}{\mathrm{d}t} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} \lambda_1 + \lambda_2 - l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \eta_1^m + \\ + \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\eta_1^m\hat{\eta}_3 - (1/2)(\tau+1)(\eta_1^m)^3 \\ K_1(\tau)(\eta_1^m)^2 \end{bmatrix}, \tag{3.8}$$

where $l_{1,2} < 0$. For all $\varepsilon \geq 0$, assume $|\eta_1(t) - \eta_1^m(t)| \leq \varepsilon$. Then, it holds exponentially in time that

$$\overline{\lim}_{t\to\infty} \|\eta(t) - \hat{\eta}(t)\| \leq C\varepsilon,$$

for a constant $C > 0$. In particular, for $\eta_1^m \equiv \eta_1$, system (3.8) *is a global exponential observer for system* (3.4)-(3.5).

Proofs of the Theorems (3.1.3)-(3.1.4) may be found in [12]. In the sequel, the system (3.4)-(3.5) will be often called as the master while (3.8) as the slave.

3.2 Message embedded synchronization for generalized Lorenz system and its use for chaotic masking

In this section we propose the so-called message embedded synchronization scheme. Such a synchronization may be used for chaotic masking scheme using single channel only. This method was discussed by Lian K.-Y. et. al. in [52] for a particular class of systems. As one of the theoretical results of this thesis let us characterize more general class where message embedded synchronization is possible.

Consider a nonlinear system of the form

$$\begin{bmatrix} \dot{x}^1 \\ \dot{x}^2 \end{bmatrix} = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix} \begin{bmatrix} x^1 \\ x^2 \end{bmatrix} + \begin{bmatrix} \varphi^1(Hx^1, x^2) \\ \varphi^2(Hx^1) \end{bmatrix}, \tag{3.9}$$

where $\begin{bmatrix} x^1 \\ x^2 \end{bmatrix} = x \in R^n$, $x^1 \in R^{n_1}$, $x^2 \in R^{n_2}$, $n_1 + n_2 = n$, F is $(n \times n)$ matrix, H is $(n_1 \times 1)$ matrix, F_1 is $(n_1 \times n_1)$ matrix, F_2 is $(n_2 \times n_2)$ matrix. Suppose (F_1, H) is detectable pair and F_2 is Hurwitz. Further, let nonlinear functions φ^1, φ^2 be such that

$$\varphi^1 : R^{n_2+1} \to R^{n_1}, \varphi^2 : R \to R^{n_2}.$$

Then, the synchronized copy of (3.9) can be obtained using the scalar synchronizing signal $Hx(t)$ as follows

$$\begin{bmatrix} \dot{y}^1 \\ \dot{y}^2 \end{bmatrix} = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix} \begin{bmatrix} y^1 \\ y^2 \end{bmatrix} + \\ + \begin{bmatrix} \varphi^1(Hx^1, y^2) \\ \varphi^2(Hx^1) \end{bmatrix} + \begin{bmatrix} L_1 H(y^1 - x^1) \\ 0 \end{bmatrix}. \tag{3.10}$$

Here L_1 is $(1 \times n_1)$ matrix such that $F_1 + L_1 H$ is Hurwitz. Namely, define $e = (e^1, e^2)^\top = (y^1 - x^1, y^2 - x^2)$. Then, subtracting (3.9) from (3.10) gives

$$\begin{bmatrix} \dot{e}^1 \\ \dot{e}^2 \end{bmatrix} = \begin{bmatrix} F_1 + L_1 H & 0 \\ 0 & F_2 \end{bmatrix} \begin{bmatrix} e^1 \\ e^2 \end{bmatrix} + \\ + \begin{bmatrix} \varphi^1(Hx^1, y^2) - \varphi^1(Hx^1, x^2) \\ 0 \end{bmatrix}. \tag{3.11}$$

Notice, that $e_2 \to 0$ exponentially since F_2 is Hurwitz. Assuming that the synchronization signal $Hx(t)$ of (3.9) is bounded guarantees that

$$\varphi^1(H(x(t)), y^2(t)) - \varphi^1(H(x(t)), x^2(t)) \to 0$$

exponentially as $t \to \infty$ as well. Therefore, $e_1 \to 0$ exponentially as $t \to \infty$, since $F_1 + L_1 H$ is Hurwitz. That is, $e \to 0$ exponentially as $t \to \infty$ and therefore (3.9) and (3.10) are synchronized.

Chaotic masking via precise message embedded synchronization

Consider system

$$\begin{bmatrix} \dot{x}^1 \\ \dot{x}^2 \end{bmatrix} = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix} \begin{bmatrix} x^1 \\ x^2 \end{bmatrix} + \\ + \begin{bmatrix} \varphi^1(Hx^1 + \tilde{m}(t), x^2) \\ \varphi^2(Hx^1 + \tilde{m}(t)) \end{bmatrix} + \begin{bmatrix} L_1\tilde{m}(t) \\ 0 \end{bmatrix} \tag{3.12}$$

and its copy to be synchronized

$$\begin{bmatrix} \dot{y}^1 \\ \dot{y}^2 \end{bmatrix} = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix} \begin{bmatrix} y^1 \\ y^2 \end{bmatrix} + \begin{bmatrix} \varphi^1(Hx^1 + \tilde{m}(t), x^2) \\ \varphi^2(Hx^1 + \tilde{m}(t)) \end{bmatrix} + \\ + \begin{bmatrix} L_1H \\ 0 \end{bmatrix} y_1 - \begin{bmatrix} L_1(Hx^1 + \tilde{m}(t)) \\ 0 \end{bmatrix}. \tag{3.13}$$

Then $|y - x| \to 0$ as $t \to \infty$ exponentially. Namely, define $e = (e^1, e^2)^\top = (y^1 - x^1, y^2 - x^2)$. Then subtracting (3.12) from (3.13) gives

$$\begin{bmatrix} \dot{e}^1 \\ \dot{e}^2 \end{bmatrix} = \begin{bmatrix} F_1 + L_1H & 0 \\ 0 & F_2 \end{bmatrix} \begin{bmatrix} e^1 \\ e^2 \end{bmatrix} + \\ + \begin{bmatrix} \varphi^1(Hx^1 + \tilde{m}(t), y^2) - \varphi^2(Hx^1 + \tilde{m}(t), x^2) \\ 0 \end{bmatrix}. \tag{3.14}$$

Now, assuming synchronization signal $Hx + \tilde{m}(t)$ is bounded, one has again that $e \to 0$ exponentially as $t \to \infty$. The message embedded scheme with precise synchronization can be implemented as follows: Let $m(t)$ be the message to be sent. Let $\tilde{m}(t) = m(t) + \mathcal{M}(x(t))$ be the embedded message. Here, $\mathcal{M}(x(t))$ is arbitrary bounded function of the state $x(t)$, which should be independent of scalar synchronizing signal Hx^1 as much as possible. Then using (3.12) one generates transmitted signal as

$$s(t) = \tilde{m}(t) + Hx^1(t) = m(t) + Hx^1 + \mathcal{M}(x(t)).$$

Recovered message $\hat{m}(t)$ would be $\hat{m}(t) = s(t) - Hy^1(t) - \mathcal{M}(y(t))$. Therefore $\hat{m}(t) - m(t) = H(x^1(t) - y^1(t)) + \mathcal{M}(x(t)) - \mathcal{M}(y(t))$, i.e. $\hat{m}(t) - m(t) \to 0$ as $t \to \infty$ exponentially.

This explain the term "precise" chaotic masking scheme synchronization: in contrast to synchronization and chaotic masking described in the literature (see Chapter 2, Section 2.1.1) where message corrupts synchronization, the method just presented completely filters out the influence of the modulated message on the synchronization.

Remark 3.2.1. *Notice that, observer canonical form of GLS* (3.4) *is the system exactly in the form* (3.9)*, where* $F_1 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $F_2 = \lambda_3$, $H = [1, 0]$, $x^1 = \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix}$, $x^2 = [\eta_3]$, $\varphi^1 = \begin{bmatrix} (\lambda_1 + \lambda_2)\eta_1 \\ -\lambda_1\lambda_2\eta_1 - (\lambda_1 - \lambda_2)\eta_1\eta_3 - \frac{(\tau+1)\eta_1^3}{2} \end{bmatrix}$, $\varphi^2 = K(\tau)\eta_1^2$. *Therefore, GLS in its canonical form can be used for chaotic masking using precise message embedded synchronization.*

3.3 Parameter mismatch influence on the generalized Lorenz system synchronization

This section presents the main theoretical prerequisites, being a novel thesis contribution. More specifically, the analysis of properties of the special class of ordinary differential equation - the so-called generalized Lorenz system (GLS) will be presented. In particular, both the synchronization and the anti-synchronization effects for the GLS system will be studied in detail and the estimates for the synchronization level of two GLS's with mismatched parameters will be obtained in this section. Without piling up formal definitions, by anti-synchronization we will mean loosing synchronization due to sudden parameter mismatch in master and slave. On the other hand, the estimates, how quickly initially mutually perfectly synchronized systems reach such an error level, will be derived as well. More specifically, the following proposition analyzes the influence of mismatching the parameter τ in the master and slave when the master (3.4)-(3.5) with chaotic behavior is considered. Moreover, with a slight abuse of terminology, we assume here that "parameter" τ may be time dependent what will

be used in the sequel when analyzing security of our encryption method.

Proposition 3.3.1. *Consider system* (3.8) *with* $\eta_1 = \eta_1^m$, $\tau = \tau_{sl}(t)$ *and system (3.4-3.5) with* $\tau = \tau_{mast}(t)$, *where* $\tau_{sl}(t)$, $\tau_m(t)$ *are uniformly bounded measurable functions. Further, suppose that for the corresponding state trajectories of* (3.8) *and (3.4-3.5), the Euclidean norm of both* $\eta_1(t)$ *and* $\hat{\eta}_1(t)$ *is uniformly bounded by a constant* R. *Then, for sufficiently small*

$$\overline{\Theta} := \max_{\tau \in R^+} |\tau_{mast}(t) - \tau_{sl}(t)|$$

it holds

$$\overline{\lim}_{t\to\infty} \|\eta(t) - \hat{\eta}(t)\| \leq C\overline{\Theta},$$

where $C > 0$ *is a suitable constant. Moreover, for all values of* $l_{1,2}$, *it holds that*

$$\frac{\mathrm{d}(\eta_3 - \hat{\eta}_3)}{\mathrm{d}t} = \lambda_3(\eta_3 - \hat{\eta}_3) + \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta(t)\eta_1^2, \tag{3.15}$$

$$\Theta(t) := (\tau_{mast}(t) - \tau_{sl}(t)). \tag{3.16}$$

Proof Denoting $e = (e_1, e_2, e_3)^\top = \eta - \hat{\eta}$, one can easily obtain subtracting (3.8) with $\eta_1 = \eta_1^m$, $\tau = \tau_{sl}(t)$ from (3.4-3.5) with $\tau = \tau_{mast}(t)$

$$\dot{e} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2 - \lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} e + \begin{bmatrix} 0 \\ (-\Theta(t))\eta_1^3/2 \\ \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta(t)\eta_1^2 \end{bmatrix}, \tag{3.17}$$

so that the relation (3.15) follows immediately. To prove the remaining estimates, let us realize first that the matrix

$$\begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}, \quad l_1 < 0,\ l_2 < 0,$$

is the Hurwitz one and therefore there exists a suitable (2×2) matrix S solving the following Lyapunov matrix equation

$$\begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}^\top S + S \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix} = -I_2,$$

I_2 being the (2×2) identity matrix. Now, consider the following Lyapunov function candidate

$$V(e) = [e_1, e_2]S \begin{bmatrix} e_1 \\ e_2 \end{bmatrix} + \frac{1}{2}e_3^2,$$

then by straightforward computations

$$\begin{aligned} \frac{\mathrm{d}V}{\mathrm{d}t} &= -e_1^2 - e_2^2 + \lambda_3 e_3^2 + e_3 \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta(t)\eta_1^2 + \\ &+ 2[e_1, e_2]S \begin{bmatrix} 0 \\ e_3(\lambda_2 - \lambda_1)\eta_1 + \Theta(t)\eta_1^3/2 \end{bmatrix}. \end{aligned}$$

Notice, that by (3.15)

$$\frac{\mathrm{d}(e_3^2/2)}{\mathrm{d}t} = -\lambda_3 e_3^2 + e_3 \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta(t)\eta_1^2$$

and therefore there exists $T > 0$, such that

$$|e_3| \le \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\overline{\Theta}\eta_1^2/\lambda_3 \le \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\overline{\Theta}R^2/\lambda_3, \quad \forall t \ge T.$$

Therefore, straightforward computations give $\forall t \ge T$ that

$$\begin{aligned} \|\frac{\mathrm{d}V}{\mathrm{d}t}\| &\le -e_1^2 - e_2^2 + \lambda_3 e_3^2 + \left(\frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\right)^2 \overline{\Theta}R^4/\lambda_3 + \\ &+ 2(|s_{11}|e_1| + |s_{21}|e_2|) \left[\frac{(\lambda_2 - \lambda_1)\frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\overline{\Theta}R^3}{\lambda_3} + \frac{\overline{\Theta}R^3}{2}\right] := \\ &:= -e_1^2 - e_2^2 + \lambda_3 e_3^2 + \alpha(\overline{\Theta})|e_1| + \beta(\overline{\Theta})|e_2| + \gamma(\overline{\Theta}), \text{ i.e.} \\ \|\frac{\mathrm{d}V}{\mathrm{d}t}\| &\le -(e_1 - \alpha/2)^2 - (e_2 - \beta/2)^2 + \lambda_3 e_3^2 + \gamma + \frac{\alpha^2 + \beta^2}{4}\ . \end{aligned}$$

The last inequality means that the Lyapunov-like function $V(e)$ strictly decreases along any trajectory $e(t)$ until this trajectory enters ellipsoid $\mathcal{E}$ given by (recall that by (3.2) $\lambda_3 < 0$)

$$(e_1 - \alpha/2)^2 + (e_2 - \beta/2)^2 - \lambda_3 e_3^2 \le \gamma + \frac{\alpha^2 + \beta^2}{4}\ .$$

As a consequence, any trajectory enters the set where

$$V(e) \le \max_{e\in\mathcal{E}} V(e)$$

and stays within it forever. Now, the crucial observation is that for sufficiently small $\overline{\Theta}$ it holds

$$|\alpha(\overline{\Theta})| < \delta\overline{\Theta}, \quad |\beta(\overline{\Theta})| < \delta\overline{\Theta}, \quad |\gamma(\overline{\Theta})| < \delta\overline{\Theta},$$

where $\delta > 0$ is a suitable fixed real number. Therefore, the above ellipsoid $\mathcal{E}$ is fully located inside the ball of radius $\tilde{C}\overline{\Theta}$, where $\tilde{C} > 0$ is a real constant. In other words, $e(t)$ should ultimately stay within the set where $V(e) \leq \max_{\|e\| \leq \tilde{C}\overline{\Theta}} V(e)$ which ensures the existence of constant $C > 0$ required by the formulation of Proposition 3.3.1. The proof is now complete. ■

Remark 3.3.2. *Using the technique of the above proof, one can obtain more specific estimate for the constant C given in the formulation of Proposition 3.3.1. This constant would be bigger if the mentioned bound R on the first component of the chaotic master system is bigger*[1] *and smaller, when observer gains $l_{1,2}$ and eigenvalue λ_3 have bigger absolute values. Important security feature of GLS is that λ_3 can not be affected, so that parameter mismatch would always have certain minimal influence despite choosing high gains l_1, l_2 in the observer (3.8). Moreover, equality (3.15) shows that for mismatched constant parameters τ_{mast}, τ_{sl} the absolute value of the third error component $e_3(t)$, even with $e_3(0) = 0$, becomes quickly strictly positive, with rate of increase being proportional to constant parameter mismatch $\overline{\Theta}$. As a matter of fact, (3.15) is the simple one dimensional asymptotically stable linear system forced by sign-preserving signal of magnitude proportional to constant parameter mismatch $\overline{\Theta}$. This feature is also crucial for our anti-synchronization chaos shift keying (ACSK) method presented later on since it provides the mentioned anti-synchronization effect. Proposition 3.3.1, as well as this remark, are supported and illustrated by numerous simulations experiments later on.*

The following proposition will provide the estimate **from bellow** of the anti-synchronization effect mentioned at the end of the previous remark. That means, it ensures that synchronization error is not less that certain

[1] *Actually, one can see that there is even dependence on R^3, so that the influence of the attractor size is crucial.*

threshold, depending on parameter mismatch. This property will be used later on for ACSK receiver.

Proposition 3.3.3. *Consider system* (3.8)*, with* $\eta_1 = \eta_1^m$*,* $\tau = \tau_{sl}$ *and system (3.4-3.5) with* $\tau = \tau_{mast}$*, where* τ_{sl}*,* τ_m *are constants and some gains* $l_1 \leq -1, l_2 \leq -1$ *are fixed. Further, let it holds for some state trajectory* $\eta(t) = [\eta_1(t), \eta_2(t), \eta_3(t)]^\top$ *of (3.4-3.5)*

$$0 < E < |\eta_1(t)| < R,\ \forall t \in [0, T^*],\ \ T^* := \min\left(\frac{E^2}{3R^2(2\lambda_1 - \lambda_3)}, |\frac{1}{2l_1}|, |\frac{1}{2l_2}|\right).$$

Then it holds for all $t \in [0, T^*]$

$$|\eta_1(t) - \hat{\eta_1}(t)| \geq \frac{E^3}{12}\Theta t^2, \quad |\eta_2(t) - \hat{\eta_2}(t)| \geq \frac{E^3}{6}\Theta t,$$

where

$$\Theta := |\tau_{mast} - \tau_{sl}|$$

and $\hat{\eta}(t)$ *is any trajectory of (3.8) with* $\hat{\eta}(0) = \eta(0)$*.*

Proof Obviously, the error dynamics (3.17) holds again with $\Theta(t) :\equiv \overline{\Theta} = \tau_{mast} - \tau_{sl}$, namely

$$\dot{e} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2 - \lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} e + \begin{bmatrix} 0 \\ (-\overline{\Theta})\eta_1^3/2 \\ \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\overline{\Theta}\eta_1^2 \end{bmatrix},$$

where $e(t) :\equiv \hat{\eta}(t) - \eta(t)$. Denote

$$\widetilde{A} = \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix} \tag{3.18}$$

and recall that by the assumption of the proposition being proved it holds $e(0) = \hat{\eta}(0) - \eta(0) = 0$. Then

$$e_3(t) = \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\overline{\Theta}\int_0^t \exp(\lambda_3(t-s))\eta_1^2(s)\mathrm{d}s,$$

$$\begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} = \int_0^t \exp(\widetilde{A}(t-s)) \begin{bmatrix} 0 \\ (\lambda_2 - \lambda_1)\eta_1(s)e_3(s) - \Theta\eta_1^3(s)/2 \end{bmatrix} \mathrm{d}s.$$

Recall, that $\lambda_2 < 0, \lambda_3 < 0, \lambda_1 > 0$, therefore it holds

$$|e_3(t)| = \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}\Theta \int_0^t \exp(\lambda_3(t-s))\eta_1^2(s)\mathrm{d}s,$$

as a consequence

$$|e_3(t)| \le \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}\Theta R^2 \int_0^t \exp(\lambda_3(t-s))\mathrm{d}s \le \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}\Theta R^2 t.$$

Further,

$$\begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} = \int_0^t \exp(\widetilde{A}(t-s)) \begin{bmatrix} 0 \\ \alpha(s) \end{bmatrix} \mathrm{d}s \ ,$$

$$\alpha(s) = (\lambda_2 - \lambda_1)\eta_1(s)e_3(s) - \Theta\eta_1^3(s)/2,$$

$$\begin{aligned} |\alpha(s)| &= \left|(\lambda_2 - \lambda_1)e_3(s) - \Theta\eta_1^2(s)/2\right||\eta_1(s)| \ge \\ &\ge \left|\Theta\eta_1^2(s)/2 - (\lambda_1 - \lambda_2)|e_3(s)|\right||\eta_1(s)| \ge \\ &\ge \left|E^2/2 - R^2(2\lambda_1 - \lambda_3)s\right|E\Theta/2, \ \forall s \in [0, T^*]. \end{aligned}$$

Actually, one can easily check that $\forall s \in [0, T^*]$ it holds

$$E^2/2 - R^2(2\lambda_1 - \lambda_3)s \ge 0$$

i.e. one can use

$$|A + B| \ge ||A| - |B|| \ge |C - D|$$

for all real numbers A, B, C, D, such that $|A| \ge C, |B| \le D, C \ge D$. Further, the straightforward computations show that for all $s \in [0, T^*]$

$$|\alpha(s)| \ge \left|1 - (R/E)^2(2\lambda_1 - \lambda_3)s\right|\Theta E^3/2 \ge |E^3/2 - E^3/6|\Theta = \Theta E^3/3, \ \text{ i.e.}$$

$$|\alpha(s)| \ge \Theta E^3/3, \quad \forall s \in [0, T^*]. \tag{3.19}$$

Summarizing, to obtain the desired lower estimate for $e_1(t)$ and $e_2(t)$ one can use

$$\begin{aligned} \begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} &= \int_0^t \exp(\widetilde{A}(t-s)) \begin{bmatrix} 0 \\ \alpha(s) \end{bmatrix} \mathrm{d}s = \\ &= \int_0^t \exp(\widetilde{A}(s)) \begin{bmatrix} 0 \\ \alpha(t-s) \end{bmatrix} \mathrm{d}s, \end{aligned} \tag{3.20}$$

$\forall t \in [0, T^*]$, where $\widetilde{A}$ is given by (3.18), while $\alpha(t)$ by (3.19). This implies easily

$$e_1(t) = \int_0^t \alpha(t-s)\big[s + l_1 s^2/2 + (l_1^2 + l_2)s^3/6 + \cdots\big]\mathrm{d}s,$$

$$e_2(t) = \int_0^t \alpha(t-s)\big[1 + l_2 s^2/2 + (l_1 l_2)s^3/6 + \cdots\big]\mathrm{d}s,$$

$$\begin{aligned}|e_1(t)| &= (1/3)\Theta E^3\big[t^2/2 + l_1 t^3/6 + (l_1^2 + l_2)t^4/24 + \cdots\big]\mathrm{d}s \geq \\ &\geq (1/6)\Theta E^3 t^2\big[1 + l_1 t/3 + (l_1^2 + l_2)t^2/12 + \cdots\big] \geq (1/12)\Theta E^3 t^2,\end{aligned}$$

$$\begin{aligned}|e_2(t)| &= (1/3)\Theta E^3\big[t + l_2 t^3/6 + (l_1 l_2)t^4/24 + \cdots\big]\mathrm{d}s \geq \\ &\geq (1/3)\Theta E^3 t\big[1 + l_2 t^2/6 + (l_1 l_2)t^3/24 + \cdots\big] \geq (1/6)\Theta E^3 t^2,\end{aligned}$$

so that the claim to be proved follows. ■

Remark 3.3.4. *The essence of the anti-synchronization method to be described later on is to detect the anti-synchronization as soon as possible. Therefore, one can actually limit the previously proved proposition to a very small time interval. It is also intuitively clear, as well as rigorously shown during the above proof by the exact arguments, that smaller time interval, the faster anti-synchronization effect. Actually, following the above proof, infinitesimally for $t \to 0$, the above estimates provided by Proposition 3.3.3 may be replaced by the following ones:*

$$|\eta_1(t) - \hat{\eta_1}(t)| \geq \frac{E^3}{4}\Theta t^2 + o(t^3), \quad |\eta_2(t) - \hat{\eta_2}(t)| \geq \frac{E^3}{2}\Theta t + o(t^3).$$

Moreover, the estimates of time T^* for the any reasonable system parameters and gains are much bigger that actually used in our algorithm later on. These time estimates were chosen to facilitate the proposition formulation. Notice also, that on a very short time interval the values E and R are close each to other (recall, that E is the minimal while R is the maximal absolute value of η_1 on some time interval.). The important quantity is E, see Tab. 3.1 later on where distribution of E is studied. Actually, the speed of anti-synchronization depends on E^3! It also depends, though linearly only

on parameter τ mismatch Θ. Finally, the most important observation here is that anti-synchronization is much better visible on e_2, rather than on e_1. Our algorithm later on will therefore use numerical derivation of e_1 combined with equation (3.17) to achieve e_2 (recall, that only η_1 is transmitted through the communication channel).

Proposition 3.3.5. *Let (3.2) holds. Consider system (3.8) with $\tau = \tau_{sl},\ l_1 < l_2 \leq -1$ and system (3.4-3.5) with $\tau = \tau_{mast}$, where $\tau_{sl},\ \tau_m$ are constants. Further, let it holds for some state trajectory $\eta(t) = [\eta_1(t), \eta_2(t), \eta_3(t)]^\top$ of (3.4-3.5) that*

$$0 < E < |\eta_1(t)| < R,\ \forall t \in [0, T^*],$$
$$T^* := \min\left(\frac{1}{2\lambda_1 - \lambda_3}, |\frac{1}{2l_1}|, |\frac{1}{2l_2}|\right).$$

Then it holds for all $t \in [0, T^*]$

$$|\ddot{e}_1(t)| \geq \frac{|\Theta|}{2}\Big[E^3 - R^3\big[2(l_1^2 + l_2)t^2 + (2\lambda_1 - \lambda_3 - 4l_1)t\big]\Big]$$

where $\Theta := \tau_{mast} - \tau_{sl},\ e_1(t) := \hat{\eta}_1(t) - \eta_1(t)$ and $\hat{\eta}(t)$ is any trajectory of (3.8) with $\hat{\eta}(0) = \eta(0)$.

Proof Obviously, the following error dynamics holds:

$$\dot{e} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & (\lambda_2 - \lambda_1)\eta_1 \\ 0 & 0 & \lambda_3 \end{bmatrix} e + \begin{bmatrix} 0 \\ \Theta\eta_1^3/2 \\ -\frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta\eta_1^2 \end{bmatrix},$$

where $e(t) :\equiv \hat{\eta}(t) - \eta(t)$. Recall that by the assumption of the proposition being proved it holds $e(0) = \hat{\eta}(0) - \eta(0) = 0$. Then

$$e_3(t) = \frac{\lambda_3 - 2\lambda_1}{2(\lambda_1 - \lambda_2)}\Theta \int_0^t \exp(\lambda_3(t-s))\eta_1^2(s)\mathrm{d}s,$$

Recall, that $\lambda_2 < 0, \lambda_3 < 0, \lambda_1 > 0$, therefore it holds

$$|e_3(t)| = \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}\Theta \int_0^t \exp(\lambda_3(t-s))\eta_1^2(s)\mathrm{d}s,$$

and by virtue of the assumption $|\eta_1(t)| < R,\ \forall t \in [0, T^*]$

$$|e_3(t)| \leq \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}\Theta R^2 \int_0^t \exp(\lambda_3(t-s))\mathrm{d}s \leq \frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}\Theta R^2 t.$$

Further, let

$$\widetilde{A} = \begin{bmatrix} l_1 & 1 \\ l_2 & 0 \end{bmatrix}, \tag{3.21}$$

then

$$\begin{bmatrix} e_1(t) \\ e_2(t) \end{bmatrix} = \int_0^t \exp(\widetilde{A}(t-s)) \begin{bmatrix} 0 \\ \alpha(s) \end{bmatrix} \mathrm{d}s,$$

$$\alpha(s) = (\lambda_2 - \lambda_1)\eta_1(s)e_3(s) - \Theta\eta_1^3(s)/2,$$

$$|\alpha(s)| = \Big|(\lambda_2 - \lambda_1)e_3(s) - \Theta\eta_1^2(s)/2\Big||\eta_1(s)| \leq$$

$$\frac{\Theta R^3}{2} + |(\lambda_1 - \lambda_2)e_3(s)|R \leq R^3\Theta\frac{1 + \big(2\lambda_1 - \lambda_3\big)s}{2},$$

i.e.

$$|\alpha(s)| \leq \Theta R^3, \quad \forall s \in [0, \big(2\lambda_1 - \lambda_3\big)^{-1}],$$

$$e_1(t) = \int_0^t \alpha(t-s)\big[s + l_1 s^2/2 + (l_1^2 + l_2)s^3/6 + \cdots\big]\mathrm{d}s,$$

$$e_2(t) = \int_0^t \alpha(t-s)\big[1 + l_2 s^2/2 + (l_1 l_2)s^3/6 + \cdots\big]\mathrm{d}s,$$

$$|e_1(t)| = \Theta R^3\big[t^2/2 + l_1 t^3/6 + (l_1^2 + l_2)t^4/24 + \cdots\big]\mathrm{d}s \leq$$

$$\leq \frac{1}{2}\Theta R^3 t^2\big[1 + l_1 t/6 + (l_1^2 + l_2)t^2/24 + \cdots\big] \leq \Theta R^3 t^2,$$

$$|e_2(t)| = \Theta R^3\big[t + l_1 t^3/6 + (l_1 l_2)t^4/24 + \cdots\big]\mathrm{d}s \leq$$

$$\leq \Theta R^3 t\big[1 + l_2 t^2/6 + (l_1 l_2)t^3/24 + \cdots\big] \leq 2\Theta R^3 t,$$

$$t \in [0, T^*],\ T^* := \min\left[\big(2\lambda_1 - \lambda_3\big)^{-1}, \frac{-1}{l_1}, \frac{-1}{l_2}\right].$$

In other words, it holds

$$|e_1(t)| \leq R^3\Theta t^2,\ |e_2(t)| \leq 2R^3\Theta t, \quad \forall t \in [0, T^*].$$

Now, using the derived upper estimates of $|e_{1,2,3}(t)|$ and both the lower and upper estimates of $|\eta_1(t)|$, assumed in the proposition statement, one can finish this proof as follows

$$\ddot{e}_1 = l_1\dot{e}_1 + \dot{e}_2 = (l_1^2 + l_2)e_1 + l_1 e_2 + (\lambda_2 - \lambda_1)\eta_1(t)e_3(t) - \Theta\eta_1^3(t)/2,$$

$$|\ddot{e}_1(t)| \geq |\Theta\eta_1^3(t)/2| - |(l_1^2 + l_2)e_1 + l_1 e_2 + (\lambda_2 - \lambda_1)\eta_1(t)e_3(t)|.$$

Therefore, taking into the account all those previously derived estimates of $e_{1,2,3}(t)$ $\forall t \in [0, T^*]$ and $l_1 \leq l_2 \leq -1$, $-\lambda_2 > \lambda_1 > -\lambda_3 > 0$ from the proposition assumption, it holds

$$|\ddot{e}_1(t)| \geq \Theta E^3/2 - (l_1^2 + l_2)R^3\Theta t^2 + 2l_1 R^3\Theta t -$$
$$- (\lambda_2 - \lambda_1)R\frac{2\lambda_1 - \lambda_3}{2(\lambda_1 - \lambda_2)}\Theta R^2 t,$$

$$|\ddot{e}_1(t)| \geq \frac{\Theta}{2}\Big[E^3 - R^3\big[2(l_1^2 + l_2)t^2 + (2\lambda_1 - \lambda_3 - 4l_1)t\big]\Big],$$

which completes the proof. ■

Remark 3.3.6. *Typical length of the single iteration used during anti-synchronization detection is* 0.001*. Therefore, practically, the anti-synchronization speed of the second derivative of the synchronizing signal error may be taken as*

$$|\ddot{e}_1(t)| \geq \frac{\Theta E^3}{2}. \tag{3.22}$$

As a matter of fact, during this very short time interval one can assume that $R/E \approx 1$ *(i.e. minimum and maximum value of synchronizing signal are practically the same). Therefore, the claim of the current remark follows from the fact that*

$$1 - 2(l_1^2 + l_2)t^2 - (2\lambda_1 - \lambda_3 - 4l_1)t \approx 1 \text{ for } t = 0.001.$$

3.4 Anti-synchronization Chaos Shift Keying scheme

As already mentioned, the anti-synchronization detection analyzed in the previous section will be used to design the realistic encryption and decryption algorithms. Namely, the well known CSK scheme will be modified. The classical CSK was first proposed by [62; 24] and its basic idea is to encode digital symbols with chaotic basis signals. Therefore, switching of chaotic modes provides quite simple configuration of the transmitter/receiver. However, as noted already in [24], synchronization is lost

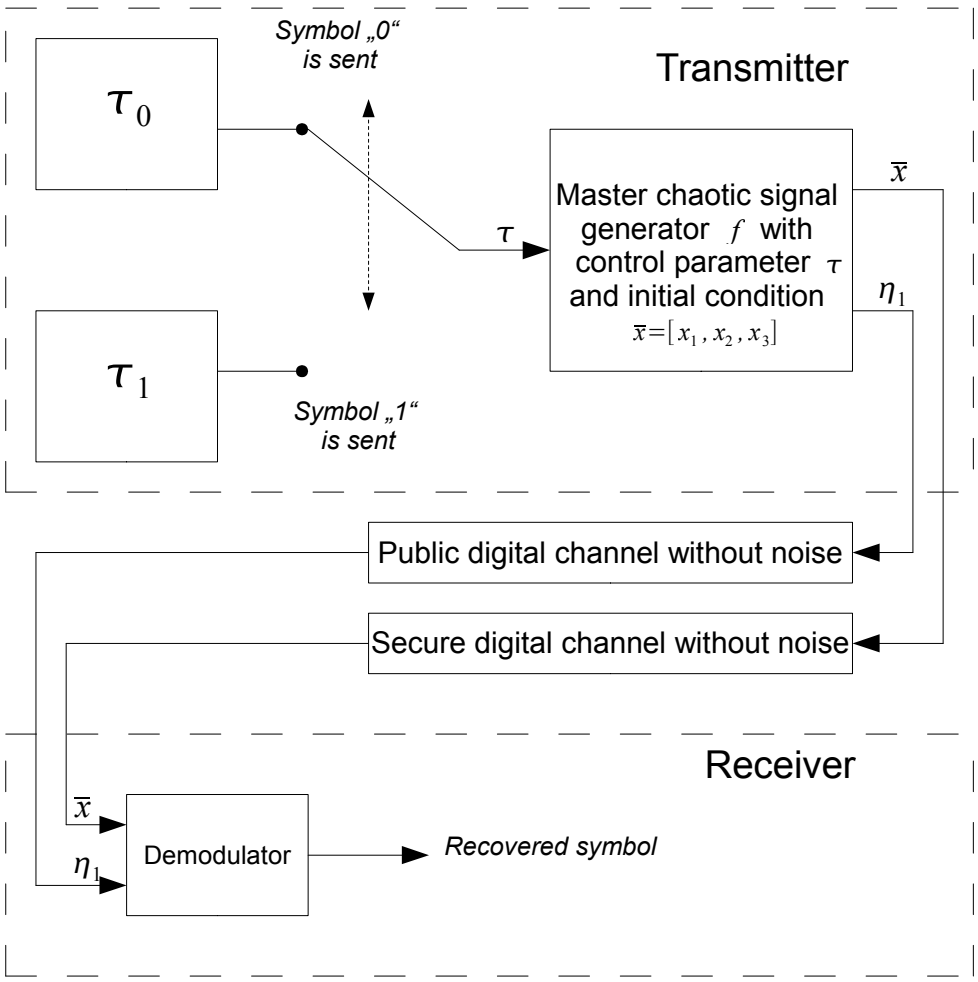


Figure 3.1: ACSK digital communication system with anti-synchronization-error-based demodulator.

and recovered every time the transmitted symbol is changed. In the other words, the classical CSK receiver method needs during switching quite a time for an establishment of synchronization between the transmitter and the receiver, therefore speed of data transmission is rather poor while amount of data to encrypt a single bit quite huge. On the contrary, our novel approach that sharply improves these vital characteristics consists in using anti-synchronization rather than synchronization and will be further referred as the anti-synchronization CSK (ACSK) scheme. Its chart is shown on Fig. 3.1 where public channel is used to send encrypted messages while secure channel a secret key.

On the transmitter side, there is the signal generator being the GLS (3.4)-(3.5) depending on crucial bifurcation parameter τ [10; 81; 20]. To encrypt digital information, one chooses "for a while" $\tau = \tau_0$ for bit "0" while for the bit "1" one chooses $\tau = \tau_1$, where τ_0, τ_1 are suitable selected GLS bifurcation parameters from its known chaotic range, cf. [10; 11; 81; 20]. Then, only the first component of a chaotic signal $\eta_1 = x_1 = z_1 - z_2$ is being transmitted through the public communication channel.

On the receiver side, signal $\eta_1 = x_1 = z_1 - z_2$ is feeded into two synchronized copies of GLS (the so-called slaves), the first one, with parameter τ_0, while the second one with parameter τ_1. Now, the crucial idea of **anti-synchronization** based decryption uses the fact that both slaves are kept synchronized to the numerically best possible level (the so-called **numerical zero**, in most simulations[2] equal to 10^{-4}). Therefore, one can detect almost immediately "the wrong" slave due to the fact that it produces fast increasing error of its first component comparing to the slowly varying error in "the correct" slave. In such a way, the bit value is decrypted, moreover, the state value of the "wrong" slave is overwritten by the value from the "correct" slave, so that prior receiving the next piece of cipher text (i.e., the synchronizing signal $\eta_1(t)$) both slaves are again synchronized to the same best possible level of the "numerical zero" 10^{-4}.

As a matter of fact, as shown by Propositions 3.3.1, 3.3.3, 3.3.5 for the fixed parameter mismatch $\Theta = |\tau_{mast} - \tau_{sl}|$ the anti-synchronization effect crucially depends on the absolute value of the synchronizing signal η_1, namely, on E^3, where E is minimal value of $\eta_1(t)$ over the time interval where anti-synchronization is to be detected. This crucial value has been experimentally thoroughly analyzed and their percentual summary is given in Tab. 3.1.

The receiver or demodulator structure of the ACSK scheme is shown in Fig. 3.2 in a more detail. It detects the correct bit via identifying the

[2]MATLAB-SIMULINK ode4 Runge-Kutta procedure with the fixed step size equal to 0.001 is being used throughout the thesis.

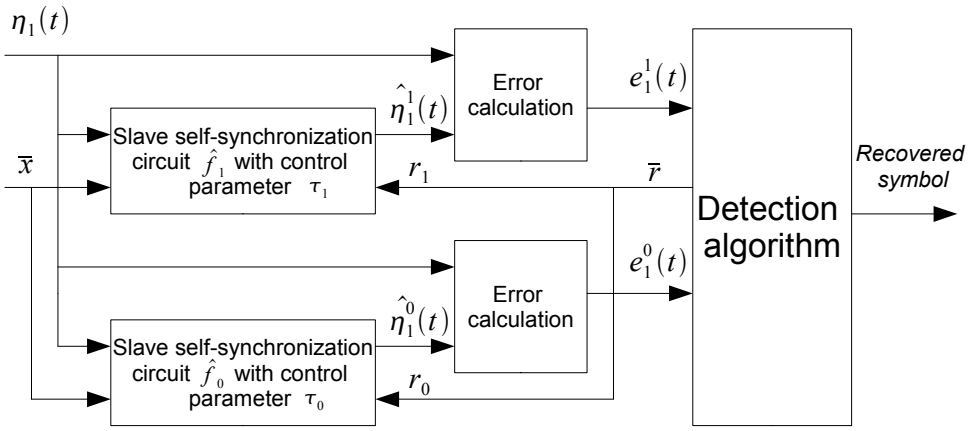


Figure 3.2: Anti-synchronization-error-based ACSK demodulator.

E	$P(E)$	E	$P(E)$	E	$P(E)$
4.0	19.92	1	64.76	0.4	84.44
3.0	28.14	0.8	71.45	0.3	87.44
2.0	38.18	0.6	78.32	0.25	89.08
1.5	47.51	0.5	81.25	0.1	95.07

Table 3.1: Here, $P(E) = \frac{meas\ (A(E))}{T_{max}} \cdot 100$, where $A(E) = \{t \in [0, T_{max} : |\eta_1(t)| \geq E\}$ and T_{max} is the maximal time available during simulation.

correct synchronization signal and then rewrites its value into both self-synchronization circuits (see the back arrows r_0, r_1 in Fig. 3.2). Such a detection in the receiver is based on the effect of the anti-synchronization, namely, three methods of the detection of the binary symbols are possible.

3.4.1 Detection based on the comparison of the synchronization errors

This method that was proposed and studied in [19; 56; 18; 13] is based on the comparison of the absolute value of the first component of the synchronizing error e_1 in the receiver and the threshold value of the error. The threshold value is well-known and depends on the control parameters

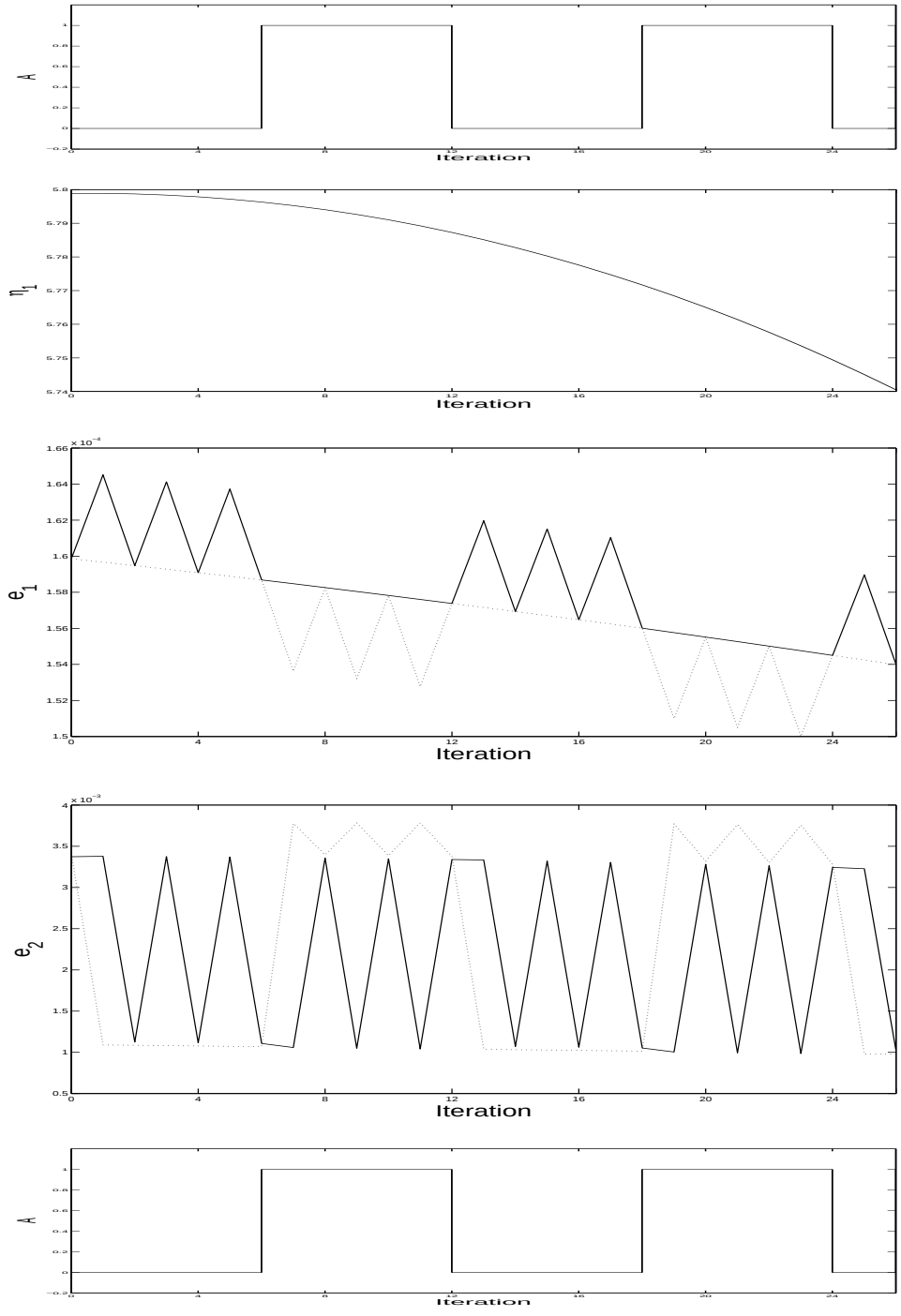


Figure 3.3: Time histories related with the encryption and decryption of the plaintext "0001110001110" using ACSK method and receiver based on detection of e_2 . From up to down: plaintext time signal; ciphertext; $e_1(t)$; $e_2(t)$ and the reconstructed plaintext.

τ_1 and τ_0, gains, step size and solver. Depending on the $|\tau_1 - \tau_0|$ and the absolute value of the synchronizing signal η_1, various quantities of the iterations are needed to detect the binary symbol exactly. Sections with higher absolute value of the synchronizing signal η_1 is more convenient. The higher absolute value of η_1, the fewer iterations for the anti-synchronization effect are needed, and vice versa. It was shown in [19] that for quite close each to other chaotic generators with difference in τ_0 and τ_1 equal to 0.01 13 iterations were needed to distinguish the right slave subsystem from the wrong one. Nevertheless, those 13 iterations were needed for the detection of the single bit only when $|\eta_1(t)| \geq 4$. Otherwise, the correct detection requires even more iterations. The section of $\eta_1(t)$ signal where one can effectively decode the information using 13 iterations only equals to 19.9 percent of the total length of the ciphertext (see Table 3.1). Data rate of this method is therefore 15 bits/1000 iterations only provided only section with $|\eta_1(t)| \geq 4$ is being used. Such a drawback suggests the necessity to look for a more precise analysis of the synchronization error, thereby further minimizing the iteration number needed for 1 bit encryption/decryption.

3.4.2 Detection based on the analysis of the second components of the synchronizing errors

This method of the detection of the binary symbols in the receiver is based on the comparison of the value of the second component of the error e_2 and was first briefly introduced in [14; 57]. Now, this method is justified by the theoretical analysis presented in the previous section. Actually, Proposition 3.3.3 shows that, while the first component of the synchronization error peak triggered by the parameter mismatch is of order $O(t^2)$, the peak of its second component is of the order $O(t)$. For very small t (note, that one iteration is typically per time equal to 0.001) this is a really significant difference. As all data are transferred precisely in the digital form, they don't contain any noise and we can use simple derivative observer to predict the second component of the error. In such a way, the parameter

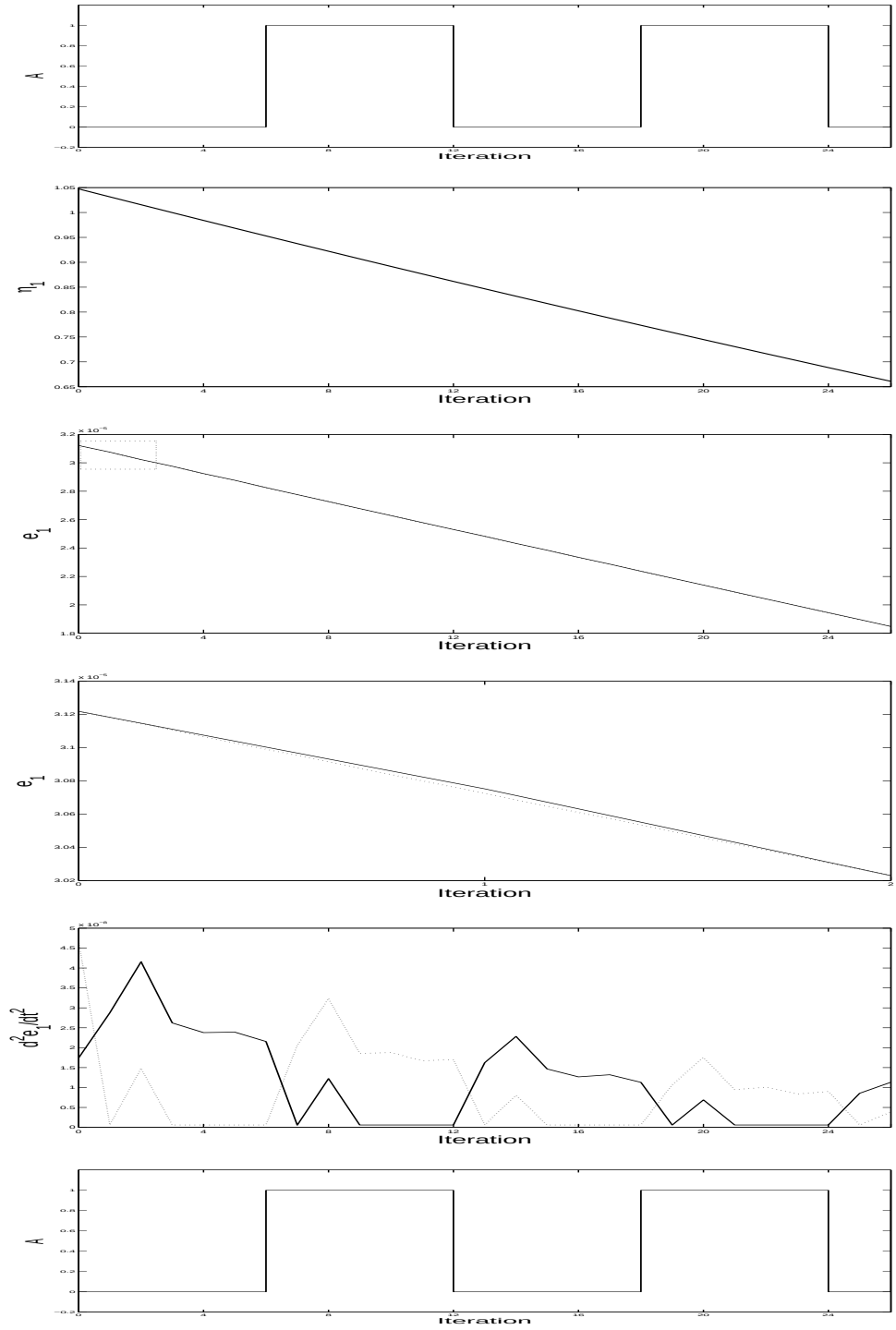


Figure 3.4: Time histories related with the encryption and decryption of the plaintext "0001110001110" using ACSK method. From up to down: plaintext time signal; ciphertext; $e_1(t)$; zoom of $e_1(t)$; $\ddot{e_1}(t)$ and the reconstructed plaintext.

mismatch can be detected almost immediately, looking on a single subsequent iteration only (for $|\eta_1(t)| \geq 3.5$). As a consequence, this second method can decrypt/encrypt efficiently 240 bits/1000 iterations. Let us note here, that in [14] it was reported that for the correct detection of the wrong slave synchronization circuit in the receiver only one iteration is needed for $|\eta_1(t)| \geq 2$. Nevertheless, a recent and more careful experimental analysis shows that the threshold of the safe detection should be increased to $|\eta_1(t)| \geq 3.5$. The reason is that the number of the iterations needed for the correct bit identification depends on the speed of the change of the synchronization signal $\eta_1(t)$, too. When the synchronization signal is increasing/decreasing very fast, one iteration for the correct detection is insufficient. Nevertheless, bit rate can be yet further improved as other signal $\eta_1(t)$ sections can be used subsequently with 2 and 3 iterations (the last one even for $|\eta_1(t)| \geq 1.6$), thereby using up to 46% of this signal, cf. Tab. 3.1. Simple calculation shows then the bit rate of the current method is 346 bits/ 1000 iterations, as in the section with $|\eta_1(t)| \geq 2.1$, only 2 iterations are needed for correct decoding the 1 bit of information.

3.4.3 Detection based on the analysis of the second derivative of the first component of the synchronization errors

This method of the detection uses Proposition 3.3.5 and computes numerically the second derivative $\ddot{e}_1$ in both slaves. This method was first introduced in [15]. As expected by Proposition 3.3.5 and confirmed by the simulations presented in detail later on, it is possible to detect the wrong slave immediately for the higher percentage of synchronizing signal - being, in fact, the cipher text carrier. This method is very useful and better than another proposed methods that we are described before. Only one iteration is needed for the correct detection the information bit in the receiver. As a matter of fact, this method uses a fact that the direction of the error in "wrong" slave changes immediately. Proposed method requires single iteration for $E > 0.25$ (i.e. for 89.08% of signal carrier), and four

iterations for $E > 0.2$ (90.82%). Summarizing, the current method can encrypt/decrypt efficiently 905 bits/1000 iterations, comparing to just 15 bits/1000 iterations for the first method and only 346 bits/1000 iterations for the second method.

3.4.4 Further comparison of detection methods

Examples of the application of the current anti-synchronization chaos shift keying (ACSK) method are shown on Fig. 3.3 and Fig. 3.4. Fig. 3.3 illustrates ACSK communication scheme with receiver based on the detection of the change of the second component of errors. Fig. 3.4 illustrates another method of detection in the receiver based on the calculation the second derivative of the e_1. Both figures use an example of a transmitted base-band signal for the message "0001110001110" encoded by means of two different, but close each to other chaotic GLS generators with different parameters $\tau_0 = 0$ and $\tau_1 = 0.1$. Only ciphertext is available to potential intruder with no clue of encrypted signal. This ciphertext is the synchronizing signal $\eta_1(t)$ sent by GLS either with $\tau_0 = 0$ or $\tau_1 = 0.1$, depending on an encrypted value of the current bit. For easy mutual comparison of all scopes on Fig. 3.3 and Fig. 3.4, their time axes are identical and indicate number of iterations[3], not a real time. It can be seen that the error immediately (during one iteration only) rises (change the direction)in one of the slaves, while in the other one it remains within declared "numerical zero" $\sim 10^{-4}$. Though each symbol on Fig. 3.3 and Fig. 3.4 require two iterations, the methods work perfectly even with a single iteration only (the second iteration is needed just to reset the initial conditions in "the wrong" slave to the initial conditions in "the true" slave.). The ciphertext obviously does not indicate change of bits in any way. There are two reasons: first, the parameterization with respect to τ makes it possible to have signals of both chaotic systems close to each other. Secondly and most importantly, as we use 1-2 bits only, it is impossible to estimate any statistical or other tendency to decrypt the information. The decryption is possible only by

[3]Recall, that the "iteration" is one step of the Runge-Kutta $4th$ order scheme with the fixed step 10^{-3}.

feeding the ciphertext into slave systems producing peaking error picture shown on Fig. 3.3 and Fig. 3.4, which clearly decrypts the corresponding digital information.

Notice that the previously presented Chaos Shift Keying method [62; 24] typically needs up to one second piece of synchronizing signal to encrypt and decrypt a single bit which corresponds usually to thousands of real numbers (iterations). So, the message expansion and speed of encryption-decryption for CSK method are simply unrealistic. For our ACSK, the message expansion is still much bigger than in methods based on discrete time chaos, nevertheless, it is becoming realistic and might be justified if it provides some extra security.

3.5 Security analysis of ACSK method

3.5.1 Power analysis and return map attack

In order to investigate the security of the ACSK scheme, two famous attacks proposed in [66; 3] are considered, that is, return map attack and power analysis attack. Recall, that in Section 2.2.3 we analyzed chaos secure communication scheme proposed in [26] by both of above mentioned methods. Here, Fig. 2.14 and Fig. 2.13 illustrates the effectiveness of return map attack and power analysis attack against our newly proposed ACSK scheme. Fig. 3.5.2 plots the result of power analysis attack to ACSK scheme. This attack first filters the transmitted signal η_1 (ciphertext) by a low-pass filter, and then recovers the plaintext utilizing a binary quantizer. Fig. 3.5.2(c) plots the result of the power analysis attack for ACSK scheme. Compared with Fig. 2.14(d), it is obvious that the intruder cannot recover the binary sequence from Fig. 3.5.2(c). As described in [66], a small change of the parameters of the transmitter affects the attractor of the chaotic system. Assuming that X_n and Y_n are the n-th maxima and n-minima of the transmitted signal, respectively, define the following modified return maps by $A_n = \frac{X_n+Y_n}{2}$, and $B_n = X_n - Y_n$. In Fig. 3.5, the plot of the return map shows that all segments are merge together

for the different values of the bifurcation parameter. Then the intruder cannot decrypt the plaintext by return map analysis. Thus, the above two crystallizing tools are ineffective in the ACSK scheme [16].

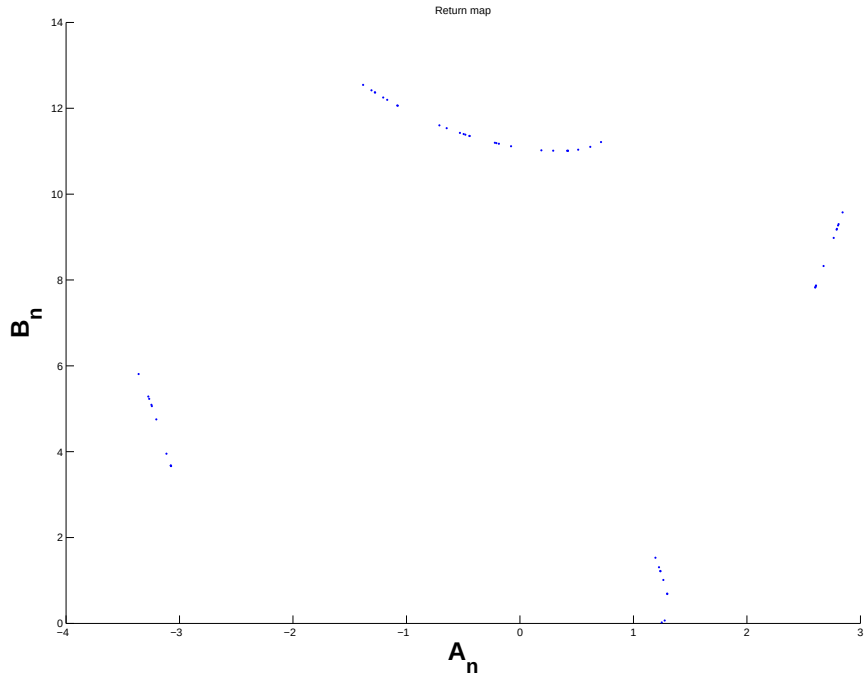


Figure 3.5: Return map analysis of ACSK scheme.

3.5.2 Key analysis

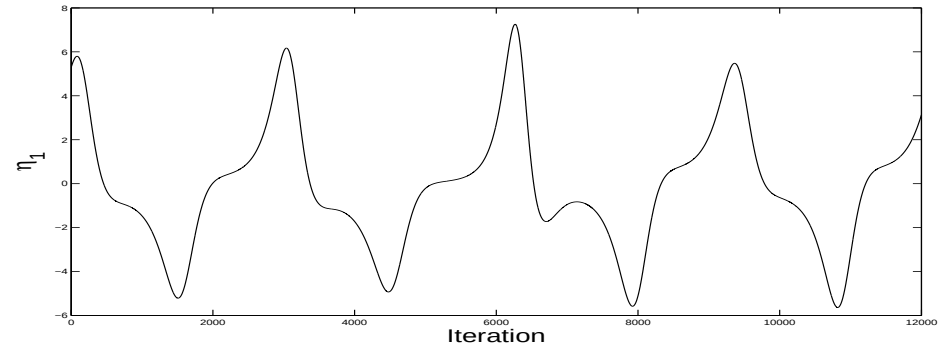
The above described decryption scheme in the ACSK method requires initial synchronization of the master on the transmitter side and both slaves on the receiver side, up to the best available numerical precision, called in the sequel as the "numerical zero". Therefore, the initial condition is the immediate candidate for the secret key. As our "numerical zero" is 10^{-4}, this key space is naturally discretized in the sense that two initial conditions closer each other than numerical zero should be represented by the same key. Assuming the size of the initial conditions interval of $\eta_3(t)$ being 10 gives 10^5 different keys, as only the third component $\eta_3(t)$ is unknown,

while the first one $\eta_1(t)$ is transmitted through the public channel and the second one $\eta_2(t)$ easily obtained by from the first component $\eta_1(t)$ using the first equation in (3.4).

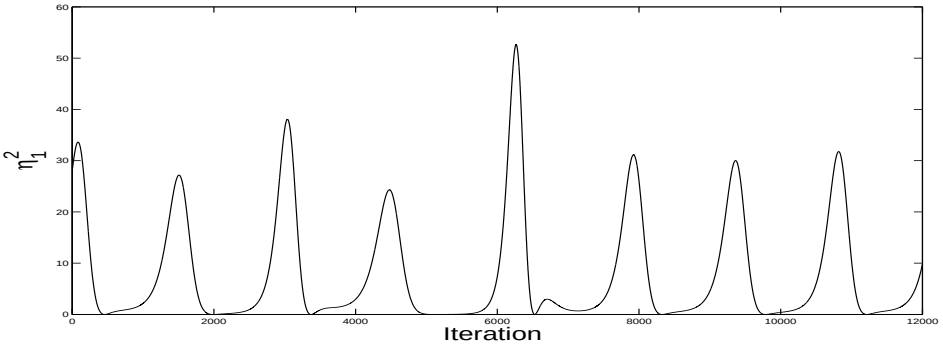
To analyze the security of the key based on the initial condition, assume for simplicity at first that both τ_0 and τ_1 are publicly known. Proposition 3.3.1 implies that at least 10 thousands of iterations of the correct signal are needed to synchronize the slaves if the initial conditions of the master are unknown. Therefore, the initial condition key can be broken only in three ways:

- Attack based on the known plain text and the corresponding cipher text, but both should be at least as of 10 000 bits. Moreover, such a knowledge should be used only for the attack to decrypt some unknown ciphertext **following right after** the above known sequence of both plaintext and the corresponding ciphertext.
- Trying 2^{10000} possible combinations of all 10 000 bits long plaintexts and comparing them with ciphertext at hand.
- Trying all possible keys - 10^5 initial conditions.

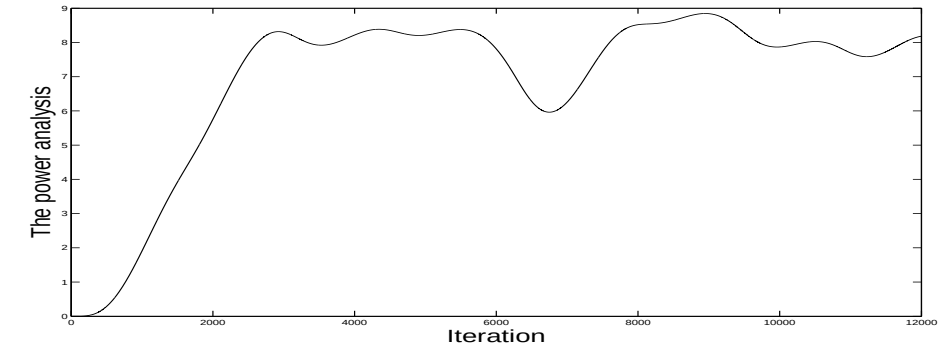
Furthermore, the parameters τ_0, τ_1 can be considered as an additional source for the secret keys. In this case, the current method presents important improvement due to the fact that changes of the parameter may occur during a single iteration. Therefore, one can not see any clue of changing parameter when analyzing signal η_1. Nevertheless, the difference $|\tau_0 - \tau_1|$ can not be arbitrarily small, as the anti-synchronization effect depends on this difference as well, see Propositions 3.3.1, 3.3.3, 3.3.5. Still, this difference was experimentally shown to be possible up to 10^{-3}. Therefore, there are 10^6 possibilities, if values $\tau \in [-0.5, 0.5]$ are considered. As a matter of fact, chaotic range for τ is even broader that the previous interval, see [9]. Finally, notice that secret key based on parameter τ is equally resistant even in case of the known plaintext and the corresponding sequence of ciphertext. In all kinds of attacks, one has to check all 10^6 possibilities of pairs τ_0, τ_1 and one needs to know the initial condition, treated before.



(a)



(b)



(c)

Figure 3.6: Time histories related with the decryption of the plaintext "00110111000100011110001101100" using power analysis attack. From up to down: the ciphertext, η_1; squared ciphertext signal, η_1^2; low pass filtered squared ciphertext signal.

Therefore, combining both the initial condition and parameter τ, one has up to 10^{11} possibilities for the secret key. When checking all possibilities for the secret key trying to perform the brute force attack, one has to take into the account that the amount of computing efforts to be done for each key choice is far from being negligible. Basically, one needs to evaluate error in both slaves during several iterations and compute its second derivative to see if it stays significantly smaller in one of the slaves than in the other one. This leads to a conclusion that brute force attack is unrealistic as well.

Here, an independent use of the τ based key and the initial condition $\eta_3(0)$ based key is guaranteed by the second equation in (3.17). Indeed, τ mismatch level Θ and initial error $e_3(0)$ influence are mixed on the right hand side there, and nonzero value of any of them spoils a possible detection.

3.6 Synchronization of the generalized Lorenz system in dynamical complex networks

The aim of this section is to study synchronization of a dynamical complex network consisting of nodes being generalized Lorenz chaotic systems and connections created with transmitted synchronizing signals. Focus is on the robustness of the network synchronization with respect to its connectional structure. This robustness is analyzed theoretically for the case of two nodes with two-sided (bidirectional connections), and numerically for various cases with many nodes. It is shown that unless a certain minimal coherent connectional structure is present in the network, synchronization is always preserved. While for a minimal connectional configuration where synchronization is global, the resulting synchronization reduces to semi-global if some redundant connections are added. The result of this section first studied in [17].

The research topic of complex networks has revoked considerable interest in the past few years. Examples of complex networks in interest include

the Internet, World Wide Web, food webs, electric power grids, metabolic networks, and biological neural networks, among many others [78; 69]. Traditionally, complex networks were studied by random graph theory, introduced by Erdös and Renyí [25]. In this section, the synchronization phenomenon of dynamical complex networks (DCN), where all nodes are identical chaotic systems (but usually with different parameters and/or initial conditions), is studied. Compared to existing results, there are two novel features in our new approach. First, nonlinear synchronizing connections between nodes are allowed; secondly, an oriented graph as a model for DCN is considered, in contrast to the general studies where only linear coupling and un-oriented networks are discussed [55; 54; 21]. The objective here is to study the synchronizability of the network when some nodes establish some new connections or lose some old connections. This notion is referred to as **structural robustness of DCN synchronization**. The motivation comes from the consideration that in a network numerous participants try to synchronize to each other for some reason (e.g. for chaotic secure communication), but then some participants may connect to or disconnect from some of their partners under certain conditions, while these should not damage the overall synchrony of the network. It will be shown that with an increasing number of connections, synchronization is only semi-global, and this semi-global performance becomes more difficult as the number of connections continue to increase, so it will become even worse in the sense that very high gains (coupling strengths) are needed to maintain the synchrony of the whole network subject to the same initial synchronization errors. All the findings were obtained for a DCN consisting of the generalized Lorenz systems (GLS) [11; 12]. It will be shown that global synchronization can be achieved for two coupled systems in the master-slave configuration [12]. This result will then be extended to the case of any DCN having the so-called minimal connections structure. For more complicated DCN, however, only semi-global synchronization may be achieved. This new synchronization method is simple in the sense that one same communication signal is used for all connections. A theoretical

proof for the case of two coupled nodes with two-sided master-slave connections will be provided, leaving the more complicated cases to be verified by numerical simulations.

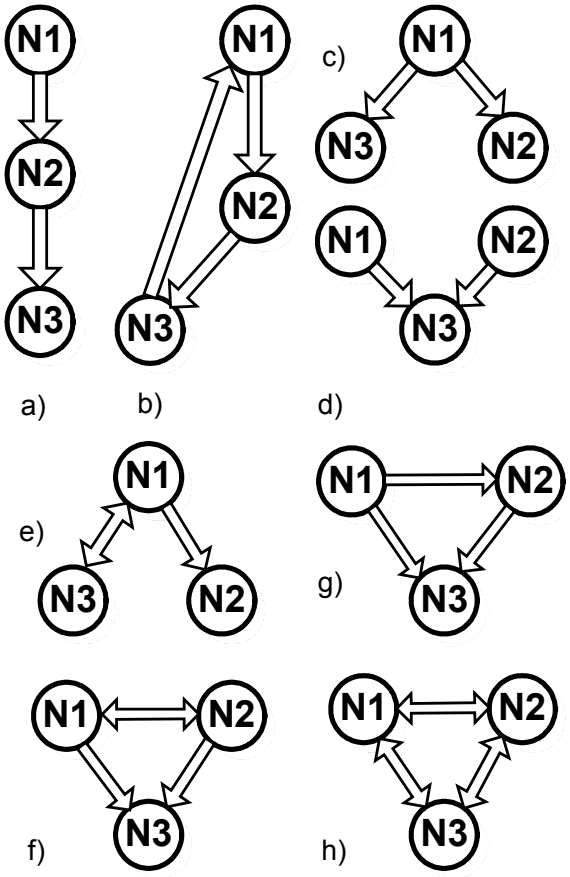


Figure 3.7: Some possible structures of a three-node network with oriented connections among nodes.

Consider a DCN of N identical nonlinear nodes, with each node being a chaotic system, described by

$$\dot{\eta^i} = f(\eta^i) + \sum_{j=1}^{N} c_{ji}\phi(\eta^i, h(\eta^j), L), \tag{3.23}$$

where $\eta^i = (\eta_1, \eta_2, ..., \eta_n,)^\top \in R^n$ is the state vector of node i, $i = 1, \ldots, N$, $L = (l_1, l_2, ..., l_n)^\top$ is the vector of coupling gains, $h(\cdot)$ is scalar synchronizing output of each system, ϕ is nonlinear coupling with $\phi(\eta, h(\eta), L) \equiv$

$0\ \forall \eta, L$ and $C = (c_{ij})_{i,j=1,\dots,n}$ is a constant $\{0,1\}$-valued matrix of linking coupling variables. Namely, there is a connection going from node i to node j, $i \neq j$, if and only if $c_{ij} = 1$. Here, c_{ij} is not always equal to c_{ji}, because the graph is oriented, but if $c_{ij} = c_{ji} = 1$, then the connection between node i and node j is called as the **coupled** or **duplex** coupling. Without loss of generality one can set $c_{ii} = 0\ \forall i \in \{1, 2, \dots, N\}$, due to the above assumption that $\phi(\eta, h(\eta), L) \equiv 0\ \forall \eta, L$. Network (3.23) is called **(asymptotically) synchronized** if $\forall i, j \in \{1, 2, \dots, N\}, i \neq j$, it holds

$$\lim_{t\to\infty} (\eta^i(t) - \eta^j(t)) = 0. \tag{3.24}$$

A network, with $c_{ij} = 1\ \forall i, j \in \{1, 2, \dots, N\},\ i \neq j$, is called as the **full N-nodes DCN**. A network, where C is a cyclic matrix (i.e., each its row and column has precisely one nonzero entry), is called as the **cyclic DCN**. Finally, a network is called as a **disconnected** one, if there is renumbering of the nodes making C block diagonal, while the opposite case is called **connected**. One can easily see that all the previous notions have clear interpretation, e.g. a full network contains all possible connections, see e.g. the network h) in Fig. 3.7, while in a cyclic network each node has exactly one inbound and one outbound connection, so it creates an oriented cyclic chain of connections, see e.g. b) in Fig. 3.7, or network in Fig. 3.13. Finally, disconnected network would obviously consist of two independent subnetworks.

Obviously, a disconnected network can not be synchronized in general. Nevertheless, being connected is only necessary for a network to be synchronizable. This leads to the following definition.

Definition 3.6.1. *The DCN (3.23) is said to be* ***synchronizable*** *if there exists an integer $\mu \in \{1, 2, \dots, N\}$, such that for every $\sigma \in \{1, 2, \dots, N\}$ there exists a sequence of integers $\{\kappa_1, \dots, \kappa_l\}$ satisfying*

$$\kappa_1 = \mu,\ \kappa_l = \sigma, \quad c_{\kappa_1,\kappa_2} = \cdots = c_{\kappa_{l-1},\kappa_l} = 1.$$

If the above integer μ is unique, then the node with number μ is called as the ***master*** *of DCN (3.23). Synchronizable network is called as a* ***minimal***

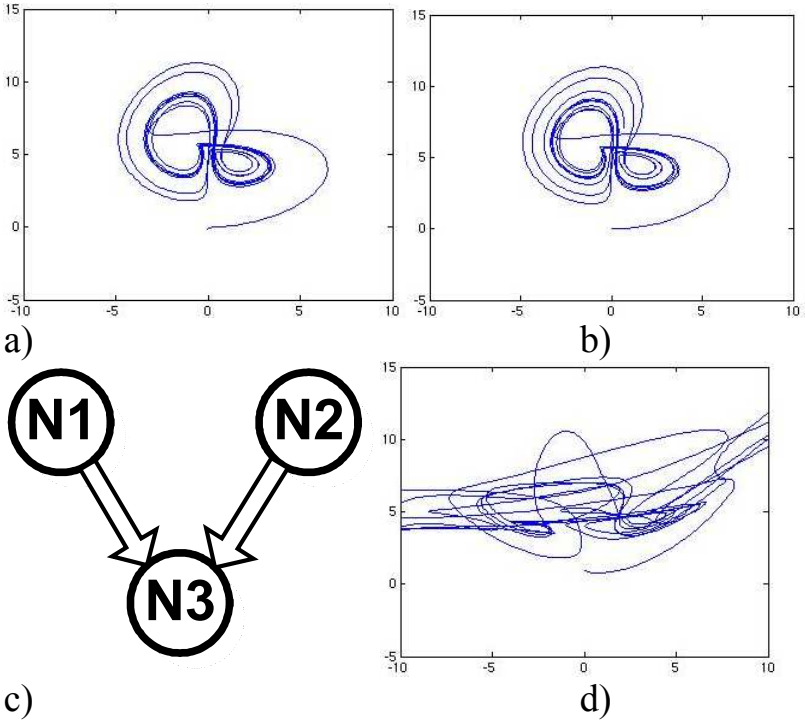


Figure 3.8: Lack of synchronizability of a dynamical three-node network, with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$; $c_{ij} = 1$ $(i \neq j)$; $l_1, l_2 = -35$ and $\tau = 0.5$. The node oscillators dynamics: a) node 1, b) node 2, d) node 3. Structure of the network - see c).

one, if removing any connection makes it not being synchronizable.

Note that the above synchronizability definition makes sense for networks being oriented graphs only. For un-oriented graphs, it is sufficient to replace it by the simple property of being connected. The following properties obviously hold:

1. **A minimal synchronizable network always has a master.**

2. **A cyclic network is always synchronizable, but never minimal**.

An example of a connected network, which is not synchronizable, is shown in Fig. 3.8. In Fig. 3.7, networks a) and c) are minimal ones having node 1

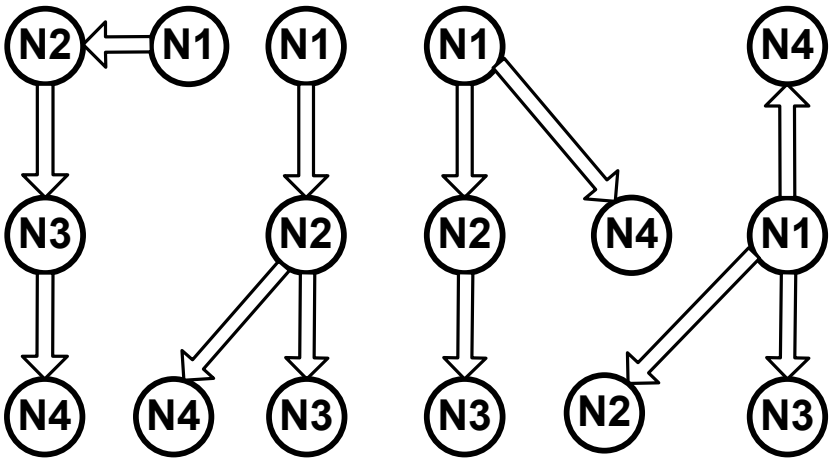


Figure 3.9: List of all four-node minimal synchronizable oriented networks.

as their master. Finally, Fig. 3.9 gives a full list of all four-nodes minimal synchronizable DCN.

3.6.1 Theoretical analysis of the synchronization in dynamical complex networks

In this section, a dynamical complex network (DCN) with nodes being the so-called generalized Lorenz system (GLS) is studied. GLS is a generalization of the classical Lorenz system containing it as a particular case. Full details about GLS may be found in Section 3.1, in particular, the so-called *generalized Lorenz canonical form*. The so-called observer canonical form of GLS were introduced there, see Theorems 3.1.2, 3.1.3.

Moreover, this observer canonical form of GLS provided a possibility to synchronize master-slave configuration of two GLS's using scalar signal η_1 only, call Theorem 3.6.2. The main theoretical result of this section is the following theorem that generalizes the mentioned result to the case of the symmetric (or duplex) synchronizing connection between two GLS's.

Theorem 3.6.2. *Consider a DCN consisting of two GLS in the canonical form (3.4)−(3.5) with the states $\eta, \hat{\eta}$, outputs $\eta_1, \hat{\eta}_1$ and its uniformly*

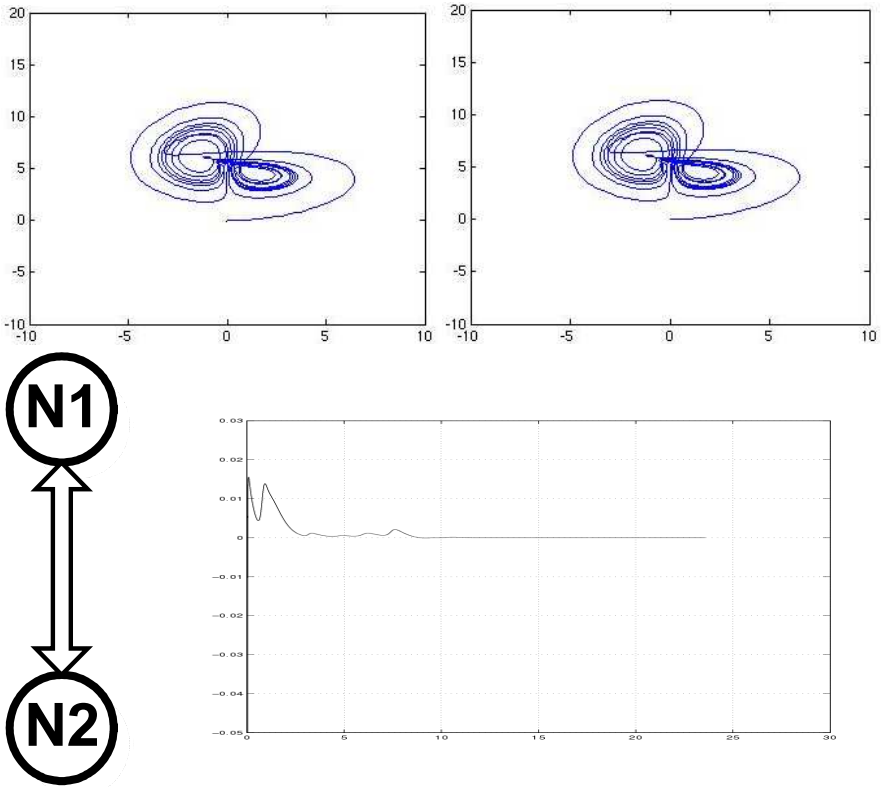


Figure 3.10: Synchronization of a two-node network, with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$, $c_{ij} = 1$ $(i \neq j)$, $l_1, l_2 = -40$ and $\tau = 0.5$. Initial condition $0 \leq [\eta_1^i, \eta_2^i, \eta_3^i]^\top \leq 1$. From left to right: the node oscillators; bottom: structures of a two-node network, synchronization error of a two-node network.

bounded trajectory $\eta(t)$, $t \geq t_0$, *coupled as follows:*

$$\frac{d\hat{\eta}}{dt} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \hat{\eta} + \begin{bmatrix} \lambda_1 + \lambda_2 - l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \eta_1 + \\ + c_{12} \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\eta_1\hat{\eta}_3 - (1/2)(\tau+1)(\eta_1)^3 \\ K_1(\tau)(\eta_1)^2 \end{bmatrix}, \qquad (3.25)$$

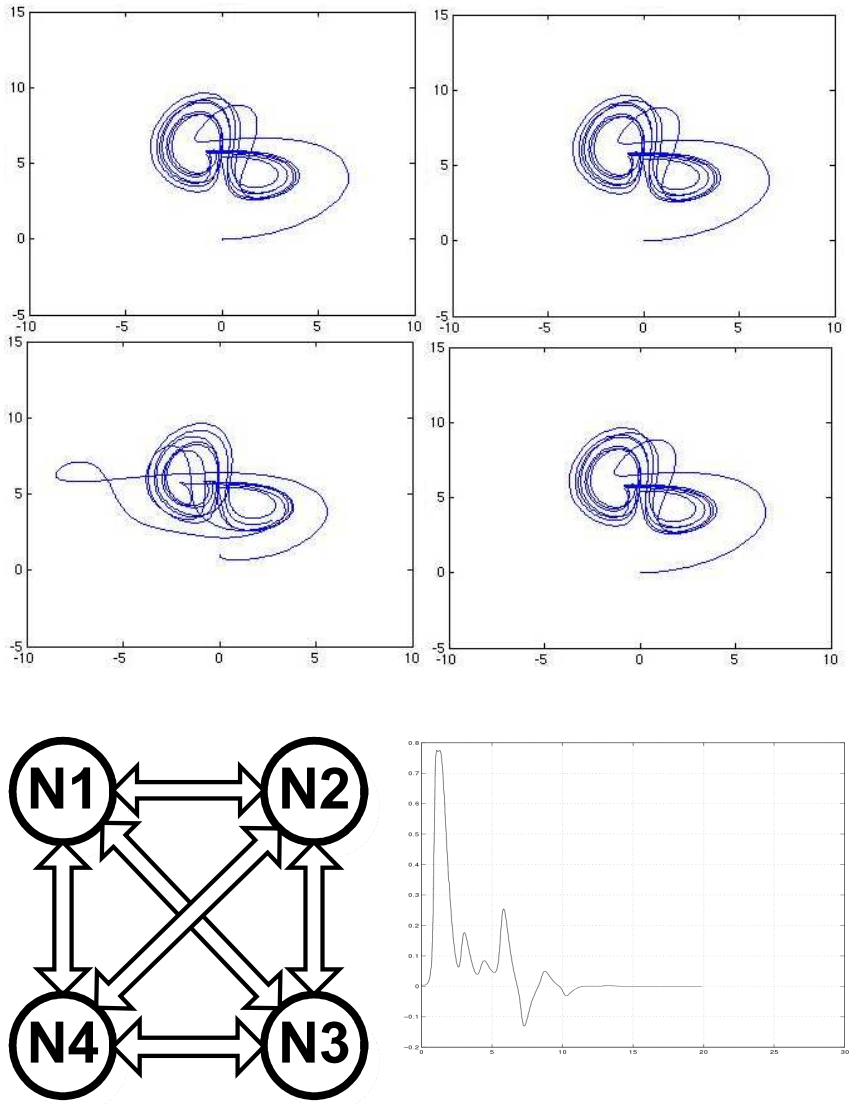


Figure 3.11: Synchronization of a network with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$; $c_{ij} = 1$ $(i \neq j)$; $l_1, l_2 = -40$ and $\tau = 0.5$. From left to right: the node oscillators; bottom: structures of a four-node network, synchronization error of a four-node network.

$$\frac{d\eta}{dt} = \begin{bmatrix} l_1 & 1 & 0 \\ l_2 & 0 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix} \eta + \begin{bmatrix} \lambda_1 + \lambda_2 - l_1 \\ -\lambda_1\lambda_2 - l_2 \\ 0 \end{bmatrix} \hat{\eta_1} + \\ + c_{21} \begin{bmatrix} 0 \\ -(\lambda_1 - \lambda_2)\hat{\eta_1}\eta_3 - (1/2)(\tau+1)(\hat{\eta_1})^3 \\ K_1(\tau)(\hat{\eta_1})^2 \end{bmatrix}, \tag{3.26}$$

where $l_{1,2} < 0$ are gains to be designed. Then,

1. *for $c_{12} = 0,\ c_{21} = 1$ or $c_{21} = 0,\ c_{12} = 1$, and for all gains $l_{1,2} < 0$, one has $\lim_{t\to\infty}(\eta(t) - \hat{\eta}(t)) = 0$ globally and exponentially;*

2. *for $c_{12} = 1,\ c_{21} = 1$, and for every bounded region of initial conditions of system (3.25)–(3.26), there exist sufficiently large gains $l_{1,2} < 0$ such that $\lim_{t\to\infty}(\eta(t) - \hat{\eta}(t)) = 0$.*

Proof. The first claim is a straightforward consequence of a result in [12], where global synchronization of the master-slave configuration of two GLS was proved. To prove the second claim, denoting $e = (e_1, e_2, e_3)^\top = \eta - \widehat{\eta}$, and deducing (3.26) from (3.25), one obtains

$$\dot{e} = \widetilde{A}e + \begin{bmatrix} 0 \\ \alpha e_1 + \beta_1 e_1^2 + \beta_2 e_1^3 + \gamma e_3 \\ -K_1(\tau)\left(2\eta_1(t)e_1 + e_1^2\right) \end{bmatrix} \tag{3.27}$$

$$\alpha(t) := \frac{3(\tau+1)\eta_1^2(t)}{2} + (\lambda_1 - \lambda_2)\eta_3(t),\ \beta_2 := \frac{\tau+1}{2},$$

$$\beta_1(t) := \frac{3(\tau+1)\eta_1(t)}{2},\ \gamma(t) := (\lambda_1 - \lambda_2)\eta_1,$$

$$\widetilde{A} = \mathrm{diag}\{\overline{A}(l_1, l_2), \lambda_3\},\ \widehat{A} = \begin{bmatrix} 2l_1 - (\lambda_1 + \lambda_2) & 1 \\ 2l_2 + \lambda_1\lambda_2 & 0 \end{bmatrix}.$$

Notice that $\widehat{A}(\theta)$ is Hurwitz $\forall\ \theta > 0$, where

$$\widehat{A}(\theta) := \overline{A}(l_1(\theta), l_2(\theta)) = \begin{bmatrix} \theta & 1 \\ \theta^2 & 0 \end{bmatrix},$$

$$l_1(\theta) = \frac{\theta + \lambda_1 + \lambda_2}{2},\ l_2(\theta) = \frac{\theta^2 - \lambda_1\lambda_2}{2}. \tag{3.28}$$

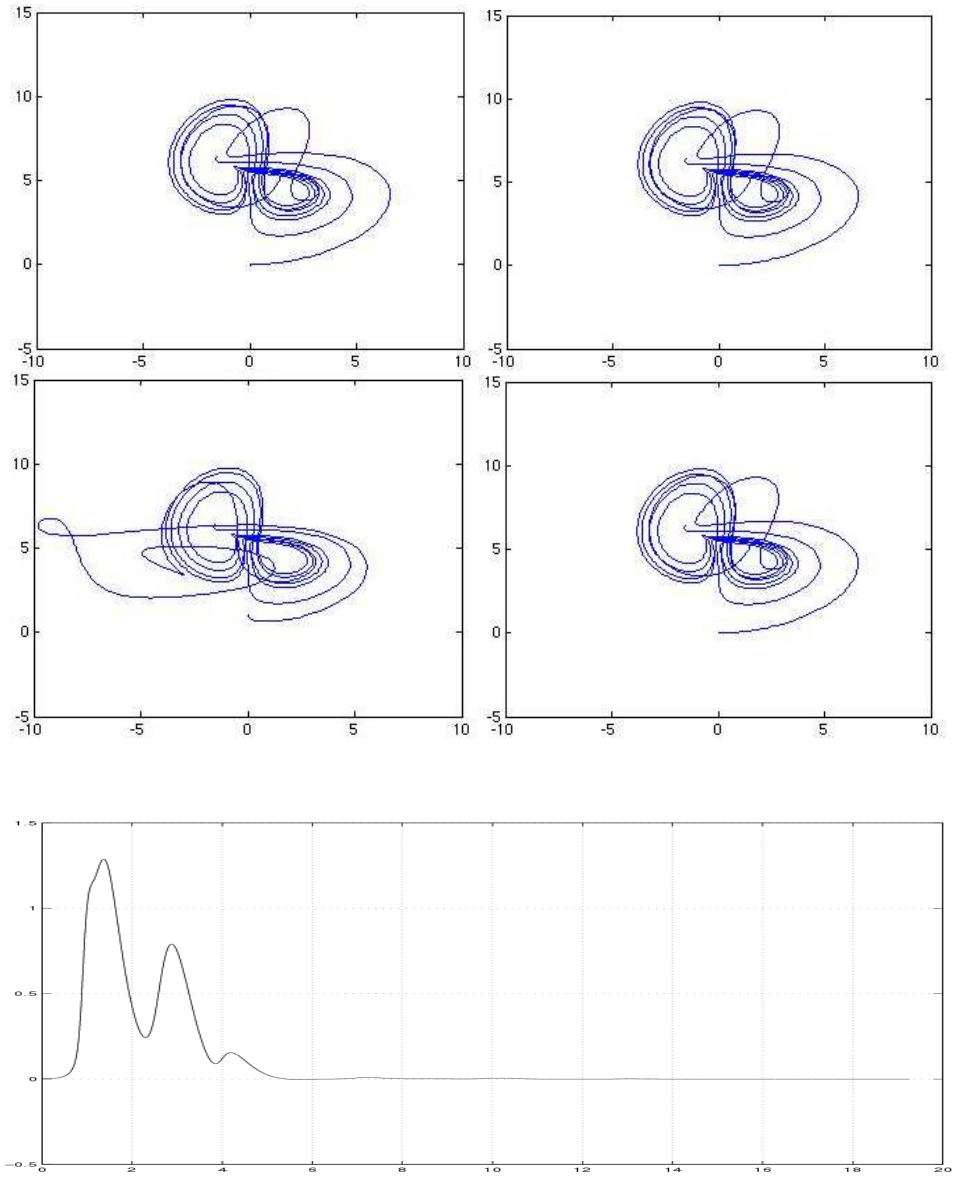


Figure 3.12: Synchronization of a network with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$; $c_{ij} = 1$ $(i \neq j)$; $l_1, l_2 = -35$ and $\tau = 0.5$. From left to right: the node oscillators; bottom: synchronization error between first node and second node of a four-node network. Other error dynamics are analogous.

In particular, there exists a matrix S such that

$$S\widehat{A}(1) + \widehat{A}(1)^\top S = -I_2, \quad S > 0,\ S^\top = S,$$

and, moreover, S is a constant matrix independent of θ. Further, consider Lyapunov's function candidate

$$V(e) = [e_1, \theta^{-1}e_2]S[e_1, \theta^{-1}e_2]^\top + \frac{(\theta^{-1}e_3)^2}{2},$$

and compute its full derivative along trajectories of the system (3.27)-(3.28) to obtain:

$$\begin{aligned}\dot{V} = -\theta\left(\epsilon_1^2 + \epsilon_2^2\right) + \lambda_3\epsilon_3^2 + K_1\epsilon_3\left(2\eta_1(t)\epsilon_1 + \epsilon_1^2\right) + \\ + 2\left[\epsilon_1, \epsilon_2\right]S\left[0, \alpha\epsilon_1 + \beta_1\epsilon_1^2 + \beta_2\epsilon_1^3 + \gamma\epsilon_3\right]^\top,\end{aligned}$$

where

$$\epsilon_1 := e_1,\ \epsilon_2 := \theta^{-1}e_2,\ \epsilon_3 := \theta^{-1}e_3.$$

Notice that $\alpha, \beta_{1,2}, \gamma$ are dependent only on system parameters and $\eta(t)$, which is bounded by assumption of the theorem. Therefore, there exist a constant R_2 and a smooth function $R_1(\cdot)$ such that

$$\dot{V} \leq -\theta\left(\epsilon_1^2 + \epsilon_2^2\right) + \lambda_3\epsilon_3^2 + |R_1(\epsilon_1)\epsilon_1(\epsilon_1 + \epsilon_3) + |R_2\epsilon_2(\epsilon_1 + \epsilon_2 + \epsilon_3)|.$$

Notice that $R_{1,2}$ do not depend on θ. As a consequence, selecting

$$\theta = \theta(e_1) := \max\{|R_1(e_1(t))|, |R_2|\} + R,$$

where $R > 0$ is a suitable constant big enough, guarantees that $\dot{V} \leq -R_3\|\epsilon\|^2,\ R_3 > 0$. By definition of $V(e)$ there exist real constants $c_2 > c_1 > 0$ such that

$$c_1\left[e_1^2 + [\theta^{-1}e_2]^2\right] + [\theta^{-1}e_3]^2/2 \leq \|V(e)\| \leq c_2\left[e_1^2 + [\theta^{-1}e_2]^2\right] + [\theta^{-1}e_3]^2/2.$$

As a consequence, it holds obviously that $\forall s > 0$,

$$\|e\| \leq s \Rightarrow \|V(e)\| \leq c_2 s,\ \|V(e)\| \leq s \Rightarrow |e_1| \leq \frac{s}{c_1}.$$

Now, semi-global exponential synchronization is achieved in the following way: consider any $s > 0$, then taking gains (3.28) with

$$\theta = \max_{|e_1| \leq s(c_2/c_1)} \theta(e_1)$$

guarantees exponential convergence on the region of initial errors $\|e(0)\| \leq s$. Indeed, such a selection of gains guarantees that $\dot{V} \leq -R_3\|\epsilon\|^2,\ R_3 > 0$ for all $\|e(t)\| \leq s$, as the above inequalities will assure that $\|V(e(t))\| \leq c_2 s$ which, in turn, guarantees $|e_1| \leq s(c_2/c_1)$. As a consequence, $V(e)$ decreases along trajectories, which guarantees that inequality $\|V(e(t))\| \leq c_2 s$ holds and consequently $|e_1(t)| \leq s(c_2/c_1)$. In other words, for any $e(t)$ with $\|e(0)\| \leq s$, it holds that for all $t \geq 0$, $\dot{V} \leq -R_3\|\epsilon\|^2,\ R_3 > 0$, and therefore $e(t)$ goes to zero exponentially as $t \to \infty$. ■

Now, consider a DCN consisting of N nodes, each of them being a GLS, defined as

$$\begin{bmatrix} \dot{\eta}_1^i \\ \dot{\eta}_2^i \\ \dot{\eta}_3^i \end{bmatrix} = \begin{bmatrix} (\lambda_1+\lambda_2)\eta_1^i + \eta_2^i \\ \hline -\eta_1^i(\lambda_1\lambda_2 + (\lambda_1+\lambda_2)\eta_3^i + \\ (\tau+1)(\eta_1^i)^2/2) \\ \hline \lambda_3\eta_3^i + K_1(\tau)(\eta_1^i)^2 \end{bmatrix} + \\ + \sum_{j=1}^{N} c_{ji} \begin{bmatrix} (\lambda_1+\lambda_2-l_1)(\eta_1^j - \eta_1^i) \\ \left\{ \begin{array}{c} (-\lambda_1\lambda_2 - l_2)(\eta_1^j - \eta_1^i) - \\ (\lambda_1-\lambda_2)(\eta_1^j - \eta_1^i)\eta_3^i - \\ (1/2)(\tau+1)(\eta_1^j)^3 - (\eta_1^i)^3 \end{array} \right\} \\ K_1(\tau)((\eta_1^j)^2 - (\eta_1^i)^2) \end{bmatrix}, \tag{3.29}$$

with the possible non-symmetric 0-1 coupling matrix

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1(N-1)} & c_{1N} \\ c_{21} & c_{22} & c_{23} & \cdots & c_{2N} \\ c_{31} & c_{32} & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & c_{(N-1)(N-1)} & c_{(N-1)N} \\ c_{N1} & c_{N2} & \cdots & c_{N(N-1)} & c_{NN} \end{bmatrix}.$$

As a matter of fact, Theorem 3.6.2 verifies that synchronization of the 2-node DCN (3.29), at least semi-globally, does not depend on the topology of its connections, as long as the corresponding DCN remains synchronizable. For DCN with N nodes, the following result is a straightforward

consequence of claim 1 of Theorem 3.6.2.

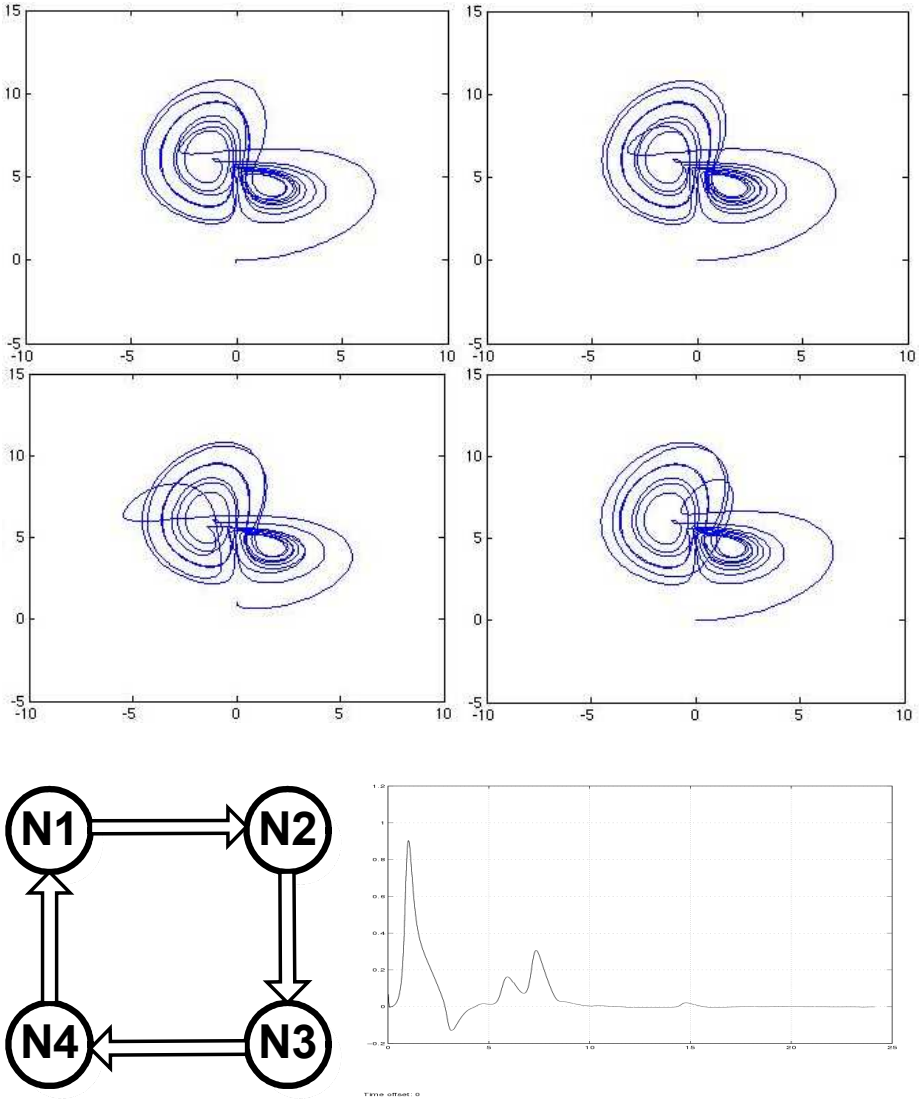


Figure 3.13: Synchronization of a network with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$; $c_{ij} = 1$ $(i \neq j)$; $l_1, l_2 = -40$ and $\tau = 0.5$. From left to right: the node oscillators; bottom: structures of a four-nodes network (cycle topology), synchronization error of a four-node network.

Theorem 3.6.3. *Consider DCN (3.29) which is synchronizable and minimal. Then, it is globally exponentially synchronized.*

3.6.2 Numerical analysis of the synchronization in dynamical complex networks

As indicated by Theorem 3.6.2 for non-minimal synchronizable DCN's, only semi-global synchronization is possible in general. This theorem, nevertheless, considers all cases of a two-node network only. In this section, it is shown experimentally that this property holds even for networks with a larger number of nodes. More specifically, consider several four-node DCN of GLS of the form (3.29). The first example is presented by Fig. 3.8, which is not synchronizable in the sense of Definition 3.6.1. Simulations confirm that the network is indeed not synchronized. In Fig. 3.10, Theorem 3.6.2 is illustrated. One can see that two nodes with a duplex connection (i.e., neither is master or slave) are synchronized; but for initial synchronization errors up to 1, quite strong gains are needed. In Fig. 3.13, a fully connected DCN with four nodes is synchronized, i.e., information is transmitted from any node to all other nodes. Again, strong synchronizing gains are needed. Fig. 3.12 shows the complicated error convergence when gains are taken weaker; further weakening the gains will eventually destroy the synchronization. Some "structural perturbation" of the full four-nodes network are shown on the remaining figures. Fig. 3.13 shows the special case of a cyclic network, indicating that synchronization persists with the same parameters as in the case of Fig. 3.11. Actually, many more experiments have been carried out, showing that such a nice robust structural property always holds, where the only clear limit is that the network should not lose its synchronizability (see Definition 3.6.1). Regarding semi-global versus global performance, an interesting observation is that for particular initial conditions and gains, a synchronizable network is always either synchronized or diverging to infinity. This was actually predicted during the proof of Theorem 3.6.2.

3.7 Conclusion

In this chapter several possibilities to use generalized Lorenz chaotic systems in communication and encryption have been investigated. Among them, chaotic masking via message embedded precise synchronization and modified chaos shift keying scheme have been proposed to improve security and minimize the redundance of the information content. In particular, it was shown that ACSK digital communication method has the potential of introducing a high degree of security at a low receiver complexity. At the same time, it requires reasonable amount of data to encrypt a single bit, thereby making revolutionary possibility of practical and realistic use of continuous time chaotic system for digital data encryption. Further, network synchronization of GLS has been studied as well for possible future application in secure network communication. Important conclusions here is that generally one can only guarantee semi-global network synchronization while minimal synchronizable configuration is always globally exponentially synchronized. At the same time, both synchronizability and its minimality are merely properties of the network topology. In other words, synchronization may be determined from some graph-theoretic properties of the network, once we know how to synchronize the simple master-slave configuration of two nodes, which therefore is of fundamental importance in the present investigations.

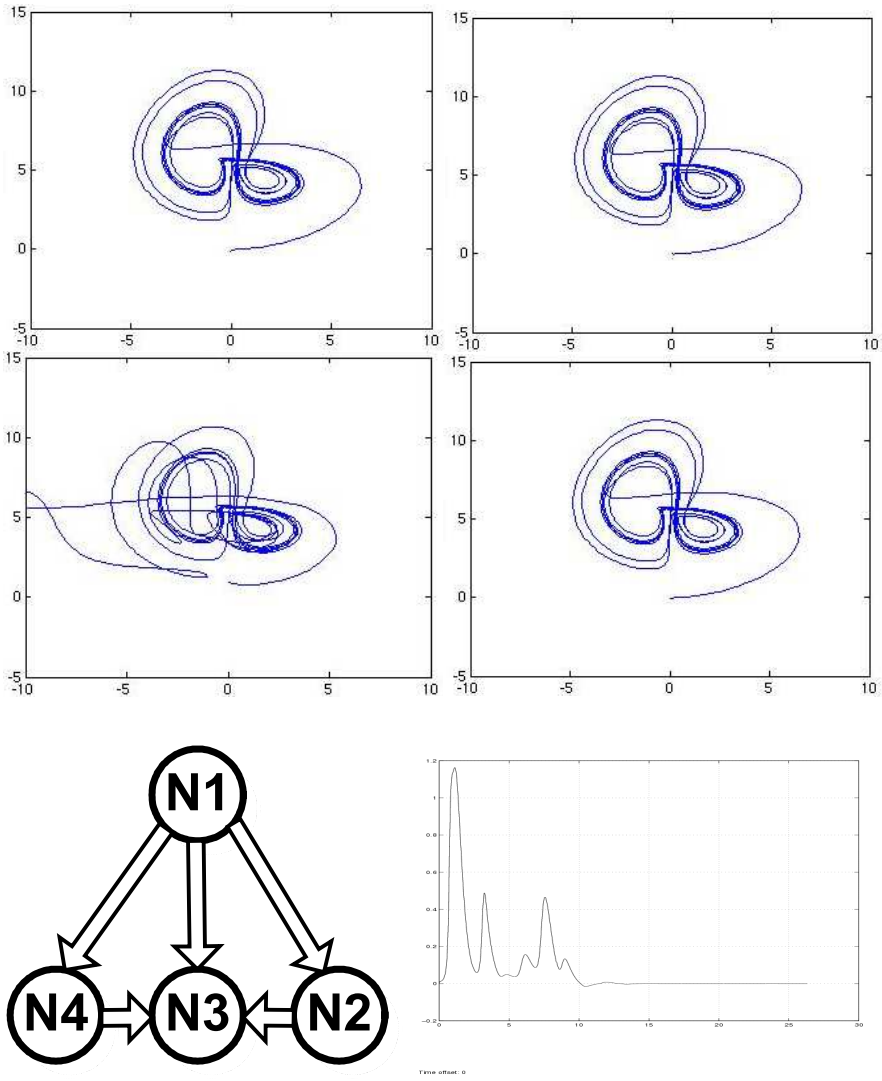


Figure 3.14: Synchronization of a network with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$; $c_{ij} = 1$ $(i \neq j)$; $l_1, l_2 = -40$ and $\tau = 0.5$. From left to right: the node oscillators; bottom: structures of a four-node network, synchronization error of a four-node network.

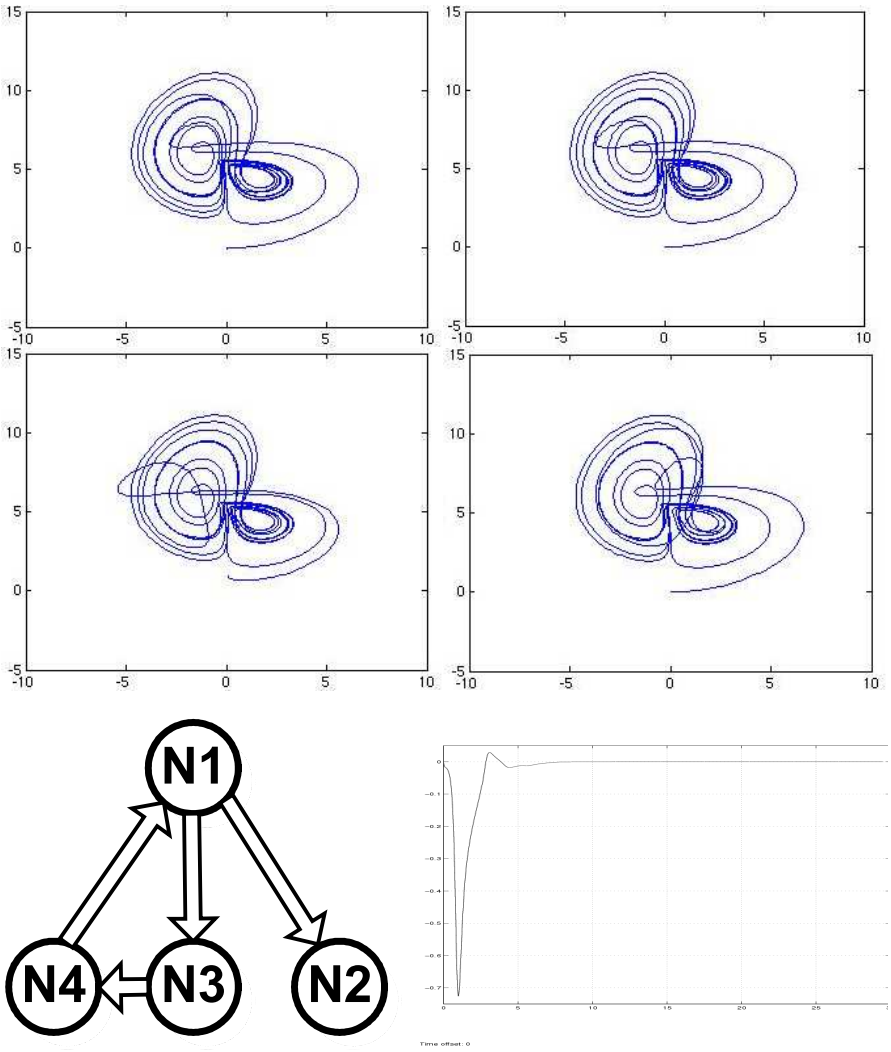


Figure 3.15: Synchronization of a network with $\lambda_1 = 8$, $\lambda_2 = -16$, $\lambda_3 = -1$; $c_{ij} = 1$ $(i \neq j)$; $l_1, l_2 = -40$ and $\tau = 0.5$. From left to right: the node oscillators; bottom: structures of a four-node network, synchronization error of a four-node network.

Chapter 4

Conclusions

4.1 Summary

This thesis was devoted to the study of the novel methods of communication and encryption using chaotic system in order to improve the existing communication schemes. Some new theoretical properties of chaotic system synchronization was developed, as these methods depend crucially on chaos synchronization phenomena. In particular, new theoretical properties of the so-called generalized Lorenz system has been described. These properties was used to design and systematically analyze the new communication and encryption scheme, called the anti-synchronization chaos shift keying (ACSK) implemented via the generalized Lorenz system. Further, analysis of dynamical properties of generalized Lorenz system enabled study of its synchronization within dynamical complex networks for possible communication. More specifically, different chaotic communication techniques that can be implemented with and without synchronization have been studied in the present thesis. Encryption methods based on the properties of chaos are reviewed. The main contribution of the thesis is the novel modulation scheme called the anti-synchronization chaos shift keying. ACSK digital communication method has potential of introducing a high degree of security at a low receiver complexity. At the same time, it requires reasonable amount of data to encrypt a single bit, thereby making revolutionary possibility of practical and realistic use of continuous

time chaotic system for digital data encryption. The thesis implements the ACSK scheme by using the so-called generalized Lorenz system (GLS) family. GLS has been introduced and studied relatively recently, [20; 81; 10], nevertheless, its using to ACSK implementation, and further theoretical analysis was performed in this thesis.

The ideas about the communication using generalized Lorenz system via their synchronization are generalized to study the synchronization of complex networks of chaotic systems. Namely, interesting theoretical proof of the exponential synchronization of two generalized Lorenz systems with bi-directional connection has been presented and more complicated networks structure studied numerically. Basic observation here is that the increasing complexity of connections can destabilize the network, stability is maintained by high synchronizing gains and locally only, with decreasing size of stability region.

4.2 Future research outlooks

On the basis of this thesis several perspective investigations can be performed in the future:

1. The detailed theoretical study of the generalize Lorenz system properties and its application for a data transmission system building based on the properties of chaotic dynamics were conducted in this thesis. The first goal we set in the future, is to bring the theoretical results of research to the practical implementation, namely, the development of the user friendly encoding/decoding data software based on the tested anti-synchronization chaos shift keying method.

2. Further development of often chaos-based encryption approaches using the generalized Lorenz system and its favorable properties. Among them, the inverse system approach resulting in block cipher and pseudorandom bit generator resulting into the stream cipher.

3. Message-embedded synchronization of networks of nodes being generalized Lorenz system with different messages sent between nodes.

This would enable to construct networks communicating securely using chaos masking scheme with message embedded synchronization.

Bibliography

[1] Abarbanel, H. D. I., Rulkov, N. F., and Sushchik, M. M. Generalized synchronization of chaos: The auxiliary system approach. *Physical Review E 53*, 5 (1996), 4528–4535.

[2] Álvarez, G., and Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos 16*, 8 (2006), 2129–2151.

[3] Álvarez, G., Montoya, F., Romera, M., and Pastor, G. Breaking parameter modulated chaotic secure communication system. *Chaos, Solitons and Fractals 21*, 4 (2004), 783–787.

[4] Álvarez, G., Montoya, P., Pastor, G., and Romera, M. Chaotic cryptosystems. In *Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on* (1999), pp. 332–338.

[5] Baker, G. L., and Gollub, J. P. *Chaotic Dynamics: An Introduction*. Cambridge University Press, 1996.

[6] Baptista, M. Cryptography with chaos. *Physics Letters A 240*, 1-2 (1998), 50–54.

[7] Bianco, M. E., Bar, D., and Reed, D. Encryption system based on chaos theory, September 1991.

[8] Carroll, T. L., and Pecora, L. M. Using multiple attractor chaotic systems for communication. *Chaos 9*, 2 (1999), 445–451.

[9] Čelikovský, S. Observer Form of the Hyperbolic-Type Generalized Lorenz System and its Use for Chaos Synchronization. *Kybernetika 40*, 6 (2004), 649–664.

[10] Čelikovský, S., and Chen, G. On a generalized Lorenz canonical form of chaotic systems. *Int. J. of Bifur. Chaos 12* (2002), 1789–1812.

[11] Čelikovský, S., and Chen, G. On the generalized Lorenz canonical form. *Chaos Solitons and Fractals 26*, 5 (2005), 1271–1276.

[12] Čelikovský, S., and Chen, G. Secure synchronization of a class of chaotic systems from a nonlinear observer approach. *IEEE Transactions on Automatic Control 50*, 1 (2005), 76–82.

[13] Čelikovský, S., and Lynnyk, V. Observer-based Chaos Synchronization And Its Application to Multi-Valued Alphabet Chaos Shift Keying Secure Encryption. In *Proceedings of the 6th Asian Control Conference 2006* (2006), pp. 52–57.

[14] Čelikovský, S., and Lynnyk, V. Anti-synchronization chaos shift keying method: Error derivative detection improvment. In *Proceedings of the 2nd IFAC Conference on Analysis and Control of Chaotic Systems.* (London, GB, June 2009), pp. 1–6.

[15] Čelikovský, S., and Lynnyk, V. Efficient chaos shift keying method based on the second error derivative anti-synchronization detection. In *Proceedings of the 7th IEEE International Conference on Control and Automation.* (Christchurch, New Zealand, 2009), pp. 530–535.

[16] Čelikovský, S., and Lynnyk, V. Security analysis of anti-synchronization chaos shift keying method via power and return map analysis. In *Proceedings of the Third International Conference on Dynamics, Vibration and Control* (Hangzhou, China, May 2010). To appear.

[17] Čelikovský, S., Lynnyk, V., and Chen, G. Robust structural synchronization in dynamical complex networks. In *Proceedings 7th IFAC Symposium on Nonlinear Control Systems* (Pretoria, SA, 2007), pp. 289–294.

[18] Čelikovský, S., Lynnyk, V., and Šebek, M. Anti-synchronization chaos shift keying method based on generalized Lorenz system. In *Proceedings of the 1st IFAC Conference on Analysis and Control of Chaotic Systems.* (Reims, France, 2006), pp. 333–338.

[19] Čelikovský, S., Lynnyk, V., and Šebek, M. Observer-based chaos sychronization in the generalized chaotic Lorenz systems and its application to secure encryption. In *Proceedings of the 45th IEEE Conference on Decision and Contol* (San Diego, USA, 2006), pp. 3783–3788.

[20] Čelikovský, S., and Vaněček, A. Bilinear systems and chaos. *Kybernetika 30*, 4 (1994), 403–424.

[21] Chen, G., and Li, Z. Global synchronization and asymptotic stability of complex dynamical networks. *IEEE Trans. on Circ. Sys.–II 53* (2006), 28–33.

[22] Cuomo, K. M., and Oppenheim, A. V. Circuit Implementation of Synchronized Chaos with Application to Communications. *Physical Review Letters 71*, 1 (1993), 65–68.

[23] Cuomo, K. M., Oppenheim, A. V., and Strogatz, S. H. Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on circuits and systems-II 40* (1993), 626–633.

[24] Dedieu, H., Kennedy, M. P., and Hasler, M. Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuit. *IEEE Transactions on Circuits and System Part 2 40* (1993), 634–642.

[25] Erdos, P., and Renyi, A. On the evolution of random graphs. *Publ. Math. Inst. Hung. Acad. Sci 5* (1960), 17–61.

[26] Feki, M. An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solution and Fractals 18*, 1 (2003), 141–148.

[27] Feldmann, U., Schwarz, W., and Hasler, M. Communication by chatic signals: the inverse system approach. In *Proceedings of the IEEE Int. Symp. on Circ. Sys.* (Seatle, WA, 1995), pp. 680–683.

[28] Frey, D. Chaotic digital encoding: An approach to secure communication. *IEEE Transactions on circuits and systems-II 40* (1993), 660–666.

[29] Galias, Z., and Gian-Mario, M. Quadrature chaos-shift keying: Theory and performance analysis. *IEEE, Transactions on Circuits and Systems- I:Fundamental Theory and Applications 48*, 12 (2001), 1510–1518.

[30] Gallagher, J., and Goldstein, J. Sensitive dependence cryptography, 1991.

[31] Gőtz, M., Kelber, K., and Schwarz, W. Discrete-time chaotic encryption systems. i. statistical design approach. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on 44*, 10 (Oct 1997), 963–970.

[32] Gleick, J. *Chaos: Making a New Science*. Penguin (Non-Classics), 1988.

[33] Guckenheimer, J., and Holmes, P. *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields (Applied Mathematical Sciences Vol. 42)*. Springer, 2002.

[34] Habutsu, T., Nishio, Y., Sasase, I., and Mori, S. A secret key cryptosystem by iterating a chaotic map. In *Proceedings EUROCRYPT'91* (1991), vol. 547, pp. 127–140.

[35] Hayes, S., Grebogi, C., and Ott, E. Communicating with chaos. *Physical Review Letters 70* (1993), 3031–3034.

[36] Kennedy, M. P., and Kolumbán, G. Digital communications using chaos. *Signal Process. 80*, 7 (2000), 1307–1320.

[37] Kerckhoffs, A. La cryptographie militaire. *Journal des sciences militaires 11* (1883), 161–191.

[38] Kocarev, L. Chaos-based Cryptography: A Brief Overview. *IEEE Circuits and Systems Magazine 1*, 3 (2001), 6–21.

[39] Kocarev, L., Halle, K. S., S., E. K., and O., C. L. Experimental demonstration of secure communications via chaotic synchronization. *Int. J. of Bifur. Chaos 2* (1992), 709–713.

[40] Kocarev, L., Jakimovski, G., Stojanovski, T., and Parlitz, U. From chaotic maps to encryption schemes. In *Proceedings of the IEEE Intarnational Symposium Circuits and Systems (ISCAS'98)* (1998), vol. 4, pp. 514–517.

[41] Kocarev, L., and Parlitz, U. General approach for chaotic synchronization with applications to communication. *Physical Review Letters 74* (1995), 5028–5031.

[42] Kolmogorov, A. New metric invariant of transitive dynamical systems and endomorphisms of lebesgue spaces. *Doklady of Russian Academy of Sciences 119*, 5 (1958), 861–864.

[43] Kolumbán, G., Kennedy, M., Ják'o, Z., and Kis, G. Chaotic communications with correlator receivers: theory and performance limits. *Proceedings of the IEEE 90*, 5 (2002), 711–732.

[44] Kolumbán, G., Kennedy, M. P., and Chua, L. O. The Role of Synchronization in Digital Communications Using Chaos-part II: Chaotic Modulation and Chaotic Synchronization. *IEEE Transactions on Circuits and Systems-I:Fundamental Theory and Applications 45*, 11 (1998), 1129–1140.

[45] Kolumbán, G., Kennedy, M. P., and Kis, G. Multilevel differential chaos shift keying. In *Proceedings of the Intarnational Workshop on Nonlinear Dynamics of Electronics Systems* (1997), pp. 191–196.

[46] Kolumbán, G., Kennedy, M. P., and Kis, G. Performance improvement of chaotic communications systems. In *Proceedings of the European Conference on Circuit Theory and Design* (1997), pp. 284–289.

[47] Kolumbán, G., Kis, G., Kennedy, M. P., and Jákó, Z. Fm-dcsk: a new and robast solution to chaos communications. In *Proceedings of the Intarnational Symposium on Nonlinear Theory and Its Applications* (1997), pp. 117–120.

[48] Kolumbán, G., Vizvari, G., Schwarz, W., and Abel, A. Differential chaos shift keying : a robust coding for chaos communication. In *Proceedings of the International Workshop on Nonlinear Dynamics of Electronics Systems* (1996), pp. 92–97.

[49] Lau, F., and Tse, C. *Chaos-based digital communication systems*. Springer, 2003.

[50] Li, S. *Analyses and New Designs of Digital Chaotic Ciphers*. PhD thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China, June 2003.

[51] Li, S., Chen, G., and Álvarez, G. Return-map cryptoanalysis revisited. *International Journal of Bifurcation and Chaos 16*, 5 (2006), 1157–1168.

[52] Lian, K.-Y., and Liu, P. Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on 47*, 9 (Sep 2000), 1418–1424.

[53] Lorenz, E. N. Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences 20*, 2 (March 1963), 130–141.

[54] Lu, J., and Chen, G. A time-varying complex dynamical network model and its controlled synchronization criterion. *IEEE Trans. on Auto. Contr. 50* (2005), 841–846.

[55] Lu, J., Yu, X., and Chen, G. Chaos synchronization of general complex dynamical networks. *Physica A 334* (2004), 281–302.

[56] Lynnyk, V., and Čelikovský, S. Observer-based chaos anti-synchronization and its application in secure encryption. In *Proceedings of 16th International Conference of Process Control 2007* (Štrbské Pleso, 2007), pp. 155:1–6.

[57] Lynnyk, V., and Čelikovský, S. On the anti-synchronization detection for the generalized Lorenz system and its application to secure encryption. *Kybernetika 46*, 1 (2010), 1–18.

[58] Matthews, R. On the derivation of a "chaotic" encryption algorithm. *Cryptologia XIII* (1989), 29–42.

[59] Menezes, A. J., Vanstone, S. A., and Oorschot, P. C. V. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1996.

[60] Milonni, P. W., Shih, M.-L., and Ackerhalt, J. R. *Chaos in Laser-Matter Interactions (World Scientific Lecture Notes in Physics)*. World Scientific Publishing Company, 1987.

[61] Oseledec, V. A multiplicative ergodic theorem: Characteristic lyapunov exponents of dynamical systems. *Trudy MMO 19*, 197 (1968), 179–210. in Rusian.

[62] Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S., and Shang, A. Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos 2* (1992), 973–977.

[63] Parlitz, U., Kocarev, L., Stojanovski, T., and Preckel, H. Encoding messages using chaotic synchronization. *Physical Review E 53* (1996), 4351–4361.

[64] Pecora, L. M., and Carroll, T. L. Synchronization in chaotic systems. *Phys. Rev. Lett. 64*, 8 (Feb 1990), 821–824.

[65] Peitgen, H.-O., Jűrgens, H., and Saupe, D. *Chaos and Fractals: New Frontiers of Science*. Springer, 2004.

[66] Perez, G., and Cerdeira, H. Extracting messages masked by chaos. *Physical Review Letters 74*, 11 (1995), 1970–1973.

[67] Pikovsky, A., Rosenblum, M., and Kurths, J. Phase synchronization of chaotic oscillators. *Physical Review Letters 76*, 11 (1996), 1804–1807.

[68] Pyragas, K. Properties of generalized synchronization of chaos. *Nonlinear Analysis: Modelling and Control*, 3 (1998), 1–29.

[69] Reka, A., and Barabási. Statistical mechanics of complex networks. *Rev. Mod. Phys. 74* (June 2002), 47–97.

[70] Rosenblum, M. G., Pikovsky, A., and Kurths, J. *Synchronization – A universal concept in nonlinear sciences*. Cambridge University Press, Cambridge, 2001.

[71] Rossler, O. E. An equation for continuous chaos. *Physics Letters A 57*, 5 (1976), 397–398.

[72] Ruelle, D. Strange attractor. *The Mathematical Intelligencer 2*, 1 (1980), 126137.

[73] Rulkov, N., Sushchik, M., Tsimring, L., and Abarbanel, H. Generalized synchronization of chaos in directionally coupled chaotic systems. *Phys. Rev. E 51*, 2 (Feb 1995), 980–994.

[74] Schuster, H. G., and Just, W. *Deterministic Chaos: An Introduction*. Wiley-VCH Verlag, 1995.

[75] Shannon, C. E. A mathematical theory of communication. *Bell System Technical Journal 27*, 4 (1948), 379–423.

[76] Shannon, C. E. Communication theory of secrecy systems. *Bell System Technical Journal 28*, 4 (1949), 656–715.

[77] Stewart, I. *Does God Play Dice?: The Mathematics of Chaos*. Blackwell Publishers, September 1990.

[78] Strogatz, S. H. Exploring complex networks. *Nature 410*, 6825 (March 2001), 268–276.

[79] Tenny, R., Tsimring, L. S., Abarbanel, H. D. I., and Larson, L. E. Security of chaos-based communication and encryption. In *Digital Communications Using Chaos and Nonlinear Dynamics (Institute for Nonlinear Science)*. Springer, 2006, pp. 191–229.

[80] United States. Data encryption standard / u. s. department of commerce, national bureau of standards, 1977.

[81] Vaněček, A., and Čelikovský, S. *Control systems: from linear analysis to synthesis of chaos*. Prentice-Hall, London, 1996.

[82] Volkovskii, A. R., and Rulkov, N. F. Synchronouns chaotic response of a nonlinear ocsillating system as a principle for the detection of the information component of chaos. *Tech. Phys. Lett. 19* (1993), 97–99.

[83] Wikipedia. Stream cipher — Wikipedia, the free encyclopedia, 2008.

[84] Yang, T. *Chaotic communication systems*. Nova Science, Huntington, N.Y, 2001.

[85] Yang, T., Yang, L., and Yang, C. Breaking chaotic switching using generalized synchronization: Examples. *IEEE Transactions on Circuits and systems- I: Fundamental theory and applications 45*, 10 (1998), 1062–1067.

[86] Yang, T., Yang, L., and Yang, C. Cryptanalyzing chaotic secure communications using return maps. *Physics Letters A 245*, 6 (1998), 495–510.