Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems*

Gonzalo Alvarez[1] and Shujun Li[2]

[1] Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas, Serrano 144—28006 Madrid, Spain

[2] Department of Electronic and Information Engineering, Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong SAR, China

Abstract

In recent years, a large amount of work on chaos-based cryptosystems have been published. However many of the proposed schemes fail to explain or do not possess a number of features that are fundamentally important to all kind of cryptosystems. As a result, many proposed systems are difficult to implement in practice with a reasonable degree of security. Likewise, they are seldom accompanied by a thorough security analysis. Consequently, it is difficult for other researchers and end users to evaluate their security and performance. This work is intended to provide a common framework of basic guidelines that, if followed, every new cryptosystem would benefit from. The suggested guidelines address three main issues: implementation, key management, and security analysis, aiming at assisting designers of new cryptosystems to present their work in a more systematic and rigorous way to fulfill some basic cryptographic requirements. Meanwhile, several recommendations are made regarding some practical aspects of analog chaos-based secure communications, such as channel noise, limited bandwith, and attenuation.

1 Introduction

Modern telecommunication networks, and especially the Internet and mobile-phone networks, have tremendously extended the limits and possibilities of communications and information transmissions. Associated with this rapid development, there is a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography [Stinson, 1995; Menezes *et al.*, 1997].

Since 1990s, many researchers have noticed that there exists an interesting relationship between chaos and cryptography: many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems. Table 1 contains a partial list of these properties.

Table 1: Comparison between chaos and cryptography properties.

Chaotic property	Cryptographic property	Description
Ergodicity	Confusion	The output has the same distribution for any input
Sensitivity to initial conditions/control parameter	Diffusion with a small change in the plaintext/secret key	A small deviation in the input can cause a large change at the output
Mixing property	Diffusion with a small change in one plain-block of the whole plaintext	A small deviation in the local area can cause a large change in the whole space
Deterministic dynamics	Deterministic pseudo-randomness	A deterministic process can cause a random-like (pseudo-random) behavior
Structure complexity	Algorithm (attack) complexity	A simple process has a very high complexity

Interestingly, the tight relationship can even be found in the classic Shanon's paper on cryptography [1949]:

*This paper has been published in *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006.
The corresponding e-mail addresses of the authors: gonzalo@iec.csic.es (G. Alvarez), http://www.hooklee.com (S. Li).

"*Good mixing transformations are often formed by repeated products of two simple non-commuting 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.*"

¿From the above statement, it is clear that Shannon actually discussed a typical route to chaos via stretching and folding, which is well-known in today's chaos theory [Devaney, 1989]. Actually, it is a common way to employ one or more nonlinear maps to design a modern cipher, where the nonlinear maps can be considered as *discrete-time and discrete-value* versions of some chaotic systems. As a useful effort, recently the chaotic dynamics in AES have been studied [Ruggiero *et al.*, 2004; Kocarev *et al.*, 2004].

As a result of investigating the above relationship, a rich variety of chaos-based cryptosystems for end-to-end communications have been put forward [Hasler, 1998; Álvarez *et al.*, 1999b; Silva & Young, 2000; Kocarev, 2001; Li, 2003; Yang, 2004; Li, 2005a,b]. There exist two main approaches of designing chaos-based cryptosystems: analog and digital.

Most analog chaos-based cryptosystems are secure communication schemes designed for noisy channels, based on the technique of chaos synchronization [Pecora & Carroll, 1990]. Chaos synchronization is a technique developed since 1990s. Roughly speaking, it means that two chaotic systems can synchronize with each other under the driving of one or more scalar signals, which are generally sent from one system to another[1]. There are many different types of chaos synchronization, including complete synchronization, generalized synchronization, impulsive synchronization, phase synchronization, projective synchronization, lag synchronization, noise-induced synchronization, etc., due to different mathematical definitions of chaos synchronization [Boccaletti *et al.*, 2002].

In chaos-synchronization-based cryptosystems, the information can be transmitted by one or more chaotic signals in a number of ways, including (but not limited to) the following ones:

- chaotic masking [Kocarev *et al.*, 1992; Wu & Chua, 1993; Morgul & Feki, 1999; Cuomo *et al.*, 1993; Shahruz *et al.*, 2002; Memon, 2003], in which the analog message signal $m(t)$ is added to the output of the chaos generator, $x(t)$, within the transmitter;
- chaotic switching or chaos shift keying (CSK) [Dedieu *et al.*, 1993; Parlitz *et al.*, 1992], in which a binary message signal is used to choose the carrier signal from two or more different chaotic attractors;
- chaotic modulation [Halle *et al.*, 1993; Cuomo & Openheim, 1993; Chen *et al.*, 2003; Yang & Chua, 1996], in which the message modulates a parameter of the chaotic generator or, when spread spectrum techniques are used, to multiply the message signal by the chaotic carrier signal;
- chaos control methods [Hayes *et al.*, 1993, 1994; Lai *et al.*, 1999], in which small perturbations cause the symbolic dynamics of a chaotic system to track a prescribed symbol sequence;
- inverse system approach [Feldmann *et al.*, 1996; Zhou & Ling, 1997b], in which the receiver system is designed in an inverse manner to ensure the recovery of the encryption signal[2].

Regardless of the method used to transmit the message signal, the receiver has to synchronize with the transmitter's chaotic generator so as to regenerate the chaotic carrier signal $x(t)$ thereby recovering the message $m(t)$ via signal separation. For the state-of-the-art of analog chaos-based cryptosystems, refer to [Hasler, 1998; Álvarez *et al.*, 1999b; Silva & Young, 2000; Yang, 2004; Li, 2005a].

Digital chaos-based cryptosystems (also called digital chaotic ciphers), on the other hand, are designed for digital computers, where one or more chaotic maps are implemented in finite computing precision to encrypt the plain-message in a number of ways, such as the following ones:

- Stream ciphers based on chaos-based PRNG (pseudo-random number generators) [Wolfram, 1985; Matthews, 1989; Berstein & Lieberman, 1991; Zhou & Ling, 1997a; Li *et al.*, 2001; Lee *et al.*, 2003];
- Chaotic stream ciphers via inverse system approach (with ciphertext feedback) [Frey, 1993; Zhou & Ling, 1997b; Zhou & Feng, 2000; Lü *et al.*, 2004];
- Block ciphers based on chaotic round function or S-boxes [Kocarev *et al.*, 1998; Guo *et al.*, 1999; Jakimoski & Kocarev, 2001; Papadimitriou *et al.*, 2001; Tang *et al.*, 2005];
- Block ciphers based on forward/backward chaotic iterations [Habutsu *et al.*, 1991; Fridrich, 1998; Uís *et al.*, 1998; Masuda & Aihara, 2002];

[1] It is also possible that some signals are sent from one system to another (A to B), and others are sent backwards (B to A), which occurs in chaos synchronization of two bidirectional coupling chaotic systems. In addition, the driving signal may also be sent from a common external source to both chaotic systems, as in noise-induced chaos synchronization.

[2] Inverse system approach is actually a general way of designing chaos-based cryptosystems.

- Chaotic ciphers based on searching plain-bits in a chaotic pseudo-random sequence [Baptista, 1998; Álvarez *et al.*, 1999a; Wong *et al.*, 2001; Li *et al.*, 2004c; Huang & Guan, 2005; Xiao *et al.*, 2005].

These ciphers do not depend on chaos synchronization at all. Instead, they usually use one or more chaotic maps in which the initial conditions and the control parameters play the role of the secret key. For a comprehensive survey of digital chaos-based cryptosystems, see [Álvarez *et al.*, 1999b; Silva & Young, 2000; Kocarev, 2001; Li, 2003, 2005b].

Though a large number of chaos-based cryptosystems have been proposed, many of them were not designed in a secure way and have been found insecure. In fact, it has been noticed that a systematic approach to the design and security evaluation of chaos-based cryptosystems is lacking. Quoting [Bao, 2003]:

> "*The common annoying feature of the cryptosystems based on some mathematical models, e.g., those based on chaos systems, is that only the principle is given. They lack details, such as recommended key sizes and key generation steps, etc. Therefore it is not possible for others to implement the ciphers.*"

Hence, it is difficult to evaluate their security and performance in a systematic way, leaving a door widely open for attacks. To meet this need, this paper is intended to provide some basic guidelines on the description and analysis of new chaos-based cryptosystems, which would benefit both the designers and other interested researchers (especially cryptanalysts and end users who want to evaluate the security of the new cryptosystems).

The suggested guidelines address three main issues: implementation, key management, and security analysis, aiming at assisting designers to present their new cryptosystems in a more systematic and rigorous way to fulfill some basic cryptographic requirements. It is important to remark that the rules suggested in this paper are not new methods nor advances in cryptography. However, to the best of our knowledge, it is the first time that these topics are addressed systematically in the chaos literature from a cryptographical perspective. As such, and given that the vast majority of papers ignore these simple, basic, common-sense rules, they might be considered in the future by designers as a common framework to improve the overall performance, paying special attention to security, of new chaos-based cryptosystems.

The rest of the paper is organized as follows. Section 2 lists some minimum requirements about the practical aspects of chaotic ciphers implementation. In Sec. 3, the most important key-related issues are addressed. In Sec. 4, some recommendations are given for security analysis. In Sec. 5, some basic but decisive conditions about channel properties are discussed. Finally, Sec. 6 concludes the paper.

2 Implementation of Chaos-Based Cryptosystems

For many publications on chaos-based cryptosystems, only basic concepts are described whereas detailed implementation issues are neglected. However, generally speaking, implementation details are very important for cryptanalysts to evaluate the security of a cryptosystem. Also, the encryption speed and the implementation cost depend on such details. Therefore, the lack of implementation details generally makes it difficult to estimate the reliability and significance of the proposed cryptosystem through security analysis and performance evaluation.

2.1 Implementation of chaotic systems

As mentioned in Sec. 1, there are two basic approaches to the design of chaos-based cryptosystems: analog and digital. The first one is generally based on chaos synchronization, and the associated chaotic systems are implemented in analog form. The second one is independent of chaos synchronization and the chaotic systems are completely implemented in digital form.

For an analog implementation, the circuitry responsible for chaos generation (at least the explicit form of the differential equation system) should be given with enough details; while for a digital implementation, the following details should be provided: the finite computing precision, the adopted digital arithmetic (fixed-point or floating-point), the hardware/software configuration, etc.

Suggested Rule 1 *A thorough description of the implementation of the chaotic systems involved should be provided.*

When chaotic systems are completely or partially implemented in digital form, dynamical degradation will occur, i.e., the dynamical properties of digital chaotic systems may become non-ideal. The most well-known problem is the existence of many short-length chaotic orbits, which may weaken the desired statistical properties of digital chaotic ciphers, and then lower the security of the ciphers. This problem has been extensively studied in the last two decades, and it has been found that such dynamical degradation can really

cause security defects in some chaos-based cryptosystems [Li *et al.*, 2003b,a; Álvarez & Li, 2004a]. To overcome this problem, some methods should be used to improve the dynamical degradation of digital chaotic systems. An effective countermeasure is to timely perturb the underlying chaotic system with a small pseudo-random signal [Cermák, 1996; Sang *et al.*, 1998]. For more details on this issue, see [Li *et al.*, 2005g].

Suggested Rule 2 *For chaotic systems implemented in digital form, the negative effects of dynamical degradation should be taken into consideration with careful evaluation.*

2.2 Implementation of cryptosystems

In the cryptography community, there are two well-known sayings: "it is quite easy to design a secure but very slow cipher" and "it is quite easy to design a secure but very large cipher". If the security of a digital chaotic cipher is achieved without working efficiency, then its significance will be trivial and will not be accepted by both practitioners and cryptanalysts, because in the real world performance and implementation cost are important concerns besides security. The cost associated with the implementation and execution of the cipher should be studied and explained, covering aspects such as computational efficiency, program size and working memory requirements in software implementations on a variety of common platforms (32-bit CPUs, 64-bit CPUs, cheap 8-bit smart-card CPUs, etc.); and chip area in dedicated hardware implementations. Therefore, level of security, performance, and ease of implementation are the three main criteria to evaluate new cryptosystems.

Cryptosystems are typically divided into two generic types: symmetric-key (also called private-key) and asymmetric-key (also called public-key). The first group of cryptosystems use the same secret key both for encryption and decryption and are very fast, thus appropriate for handling large amounts of data at high speed, such as video encryption. There is a further division between symmetric-key algorithms: block and stream ciphers. Block ciphers encrypt the original message by grouping the symbols in blocks of two or more elements, such that each block is encrypted/decrypted always in the same way. Block ciphers usually consist of an initial transformation, a cryptographic function f iterated r times (or "rounds"), and a final transformation. The secret key is expanded using some algorithm so as to have enough key material to use at every encryption round. Amongst the most widely used block ciphers are AES, Triple DES, IDEA, DES, RC5, etc. On the other hand, stream ciphers generate a pseudorandom stream of symbols using a deterministic public algorithm governed by a secret key. The message is mixed with this sequence, also known as "keystream", usually through a modulo 2 sum, resulting in the ciphertext. Amongst the most widely used stream ciphers are A5/1, A5/2, E0, RC4, SEAL, etc. The key length of symmetric ciphers usually ranges from 128 to 256 bits.

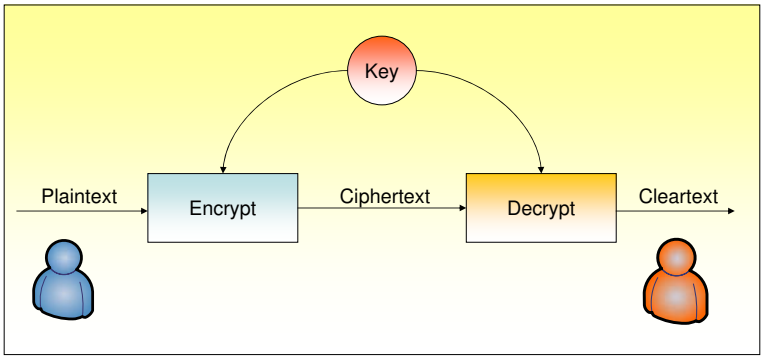

Figure 1: Block diagram of secret-key or symmetric ciphers.

When two different keys are used for the encryption and decryption processes, then the cryptosystem is assymetric. Usually, one key of the pair is publicly known whereas the other is kept private. These algorithms are much slower because in general they involve costly arithmetic operations with big integers, such as discrete logarithm or modulo exponentiation. As a consequence, they are used for tasks implying encryption of small amount of data, such as secret key agreement, digital signatures, authentication, etc. The most widely used public-key algorithm is RSA. The key length of public-key algorithms usually ranges from 1024 to 4096 bits. For a thorough and comprehensive introduction to classical cryptography, the reader is referred to [Stinson, 1995; Schneier, 1996; Menezes *et al.*, 1997].

Naturally, one can take those widely-used traditional ciphers, such as AES, DES, IDEA, RC5, RSA, etc., as good references to judge whether the implementation cost and the encryption speed of a new chaos-based cryptosystem is acceptable. Note that, as mentioned above, the encryption speed of public-key ciphers is generally much slower than the speed of secret-key ciphers, so one should compare a chaotic cipher with the

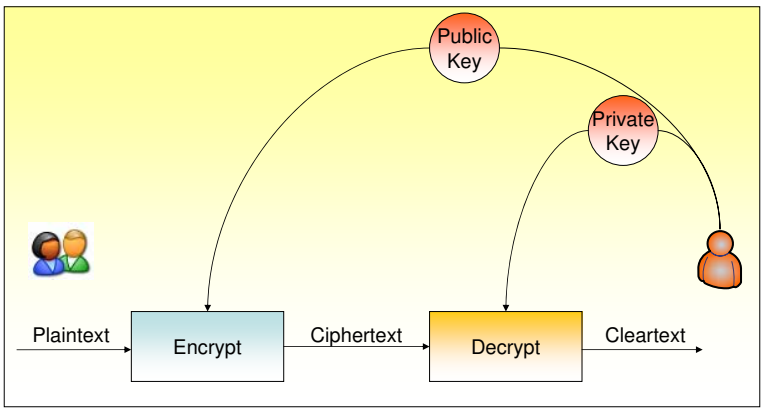

Figure 2: Block diagram of public-key or asymmetric ciphers.

same type of traditional ciphers. Since most chaotic cryptosystems are secret-key ciphers, we will mainly pay our attention to the encryption speed of secret-key chaotic ciphers. For example, for the digital chaotic cipher proposed in [Baptista, 1998], the encryption speed is only about 10 Kbps (bits/second) as shown in Table 1 of [Wong *et al.*, 2001], much lower than the speeds of all the above traditional ciphers, so one can say that the cipher is too slow to be used in real applications. Generally speaking, on a PC with a f_z Hz CPU, it is acceptable if the encryption speed is f_z/a bps, where $a \leq 100$. That is, the encryption speed is expected to be not slower than 10 Mbps on a 1 GHz CPU. As a reference, the encryption speed of a typical software implementation of AES ranges from 20 to 150 cycles/byte ($a = 2 \sim 20$), which corresponds to about 50 to 500 Mbps on a 1 GHz Pentium® processor [Gladman, 2003; Devine, 2004].

Besides the main frequency of the CPU, the encryption speed of a software implementation is tightly dependent on many other issues, such as the CPU structure, the memory size, the underlying OS platform, the developing language and all options of the compiler, and so on. Therefore, one should give the encryption speed of a new chaos-based cryptosystem with such details. In addition, it is well-known that the code optimization is very important to dramatically increase the speed of an algorithm, for example, using multiplications instead of division is useful to increase the speed for several times (for both fixed-point and floating-point arithmetics) [Fog, 2000]. Thus, it is somewhat meaningless to compare the encryption speeds of two ciphers without using the same developing environments and optimization techniques. As a typical example, we have studied the digital chaotic cipher proposed in [Lü *et al.*, 2004], and found the encryption speed is tightly dependent on the C codes: when different types of C statements are used to realize the final stage of the cipher (masking the plaintext with the pseudo-random key-stream), the encryption speed ranges between 250 Mbps to 750 Mbps on a 1.8 GHz Pentium® 4 CPU.

In [Li, 2003, §2.6], some basic suggestions are given for the design of fast and low-cost digital chaotic ciphers: avoiding using multiple iterations for each encryption step; avoiding using complicated floating-point arithmetic; choosing the simplest chaotic system from the implementation viewpoint (such as piecewise linear chaotic maps); adopting parallel mechanism in hardware implementations (such as using multiple chaotic systems for encryption simultaneously). Note that software parallel mechanism can also be achieved by carefully optimizing the codes, due to the support of parallel instructions in today's most CPUs.

Suggested Rule 3 *Without loss of security, the cryptosystem should be easy to implement with acceptable cost and speed.*

3 The Key

A fundamental issue of all kinds of cryptosystems is the key. Following Kerckhoffs' principle [Menezes *et al.*, 1997], the security of a cryptosystem should depend only on its key. No matter how strong and how well-designed the encryption algorithm might be, if the key is poorly chosen or the key space is too small, the cryptosystem will be easily broken. Unfortunately, after more than a decade of research, many chaotic secure communication schemes proposed to date fail to clearly, if at all, explain what the key is, how it should be chosen, and what the available key space is. Some designs did not even try to use any key (see for example [Memon, 2003; Acharya *et al.*, 2003; Bowong, 2004; Hua *et al.*, 2005]). Therefore, without a key, they might be viewed as some kind of coding systems, but never be regarded as a truly secure systems from the cryptographical point of view, because they are nevertheless easy to break.

3.1 Key definition

As just mentioned, a cryptosystem cannot exist without a key. In every cryptosystem, an important effort must be made to clearly define and characterize the key used for encryption and decryption.

Although common-sense, many chaos-based secure communication systems proposed in the literature thus far do not specify what the key is. It is assumed, sometimes implicitly, that the key is made from system parameters (and initial conditions for some ciphers) of the chaotic system. But even if so, it was usually not clearly specified what parameters are used as key, what their ranges are restricted to, and what their precisions or sensitivities will be throughout the communication processes.

Suggested Rule 4 *The key should be precisely defined.*

3.2 The key space

Once the key has been defined, it is equally important to characterize it, i.e., the key space must be studied in depth.

The size of the key space is the number of encryption/decryption key pairs that are available in the cryptosystem. Let us use k_i to denote a key and $\mathcal{K}$ to represent a finite set of possible keys, which is also called the key space and can be expressed as

$$\mathcal{K} = \{k_1, k_2, \ldots, k_r\}. \tag{1}$$

In classical cryptographic algorithms, which are mostly based on number theory, the key is usually a string of random bits generated by some automatic process. In such a process, if the key is n bits long, then every possible n-bit key must be equally likely, with probability 2^{-n}.

In most existing chaos-based schemes, though, the key space is nonlinear because all the keys are not equally strong. A key is considered *weak* or *degenerate* if it is relatively easy to break a ciphertext encrypted with this key in comparison with some other keys. There exist keys that give rise to non-uniformly distributed chaotic values. For instance, a bifurcation diagram like the one in Fig. 3 helps discover the intervals in which a given parameter originates periodic orbits. These values giving rise to periodic windows should be avoided since chaotic bands are preferred for encryption. As an example of the consequences of failing in doing so, check [Álvarez *et al.*, 2003b].

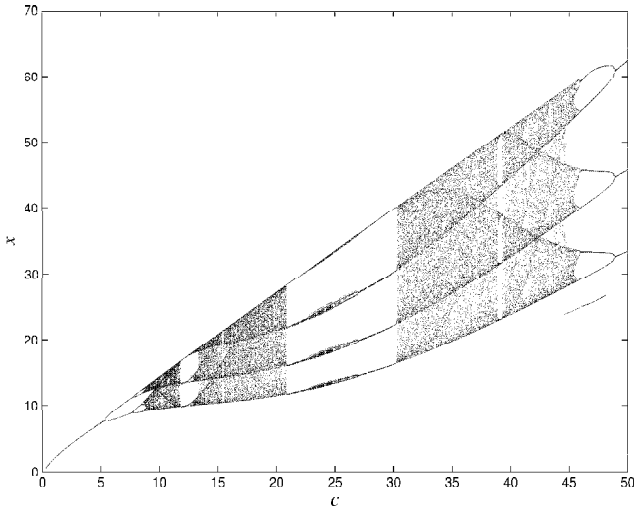

Figure 3: Bifurcation diagram of the Rössler attractor when $a = b = 0.1$ and c is varied.

When many parameters are used simultaneously as part of the key, the mutual interdependence complicates the task of deciding which ones give the best intervals. In any case, the designer of a proposed cryptosystem should conduct a study of the chaotic regions in the parameter space, from which valid keys (i.e., parameter values) that lead to chaotic behaviors can be chosen. Depending on the number m of parameters chosen as part of the key, this region will be an m-dimensional space.

A possible way to describe the key space might be in terms of positive Lyapunov exponents, assuming that an m-dimensional dynamical system is chaotic if its largest Lyapunov exponent is positive. The largest Lyapunov exponent can be computed for different combinations of chosen parameters. If it is positive, then the combination can be used as a valid key. In Fig. 4, the chaotic region for the Hénon attractor is plotted

following this criterion. This region corresponds to the key space. In this figure, parameters chosen from the lower white region give rise to periodic orbits, while parameters chosen from the upper white region give rise to unbounded orbits. As discussed above, these two regions should be avoided in order to design suitable keys. Only keys chosen from the black region are good. And even within this region, there exist periodic windows, unsuitable for robust keys. As an example of the importance of avoiding periodic windows in the key space, consider the cryptosystem proposed in [Pareek *et al.*, 2003], which was broken because values of the parameter within the logistic map's period-3 window were used as part of the key [Álvarez *et al.*, 2003b].

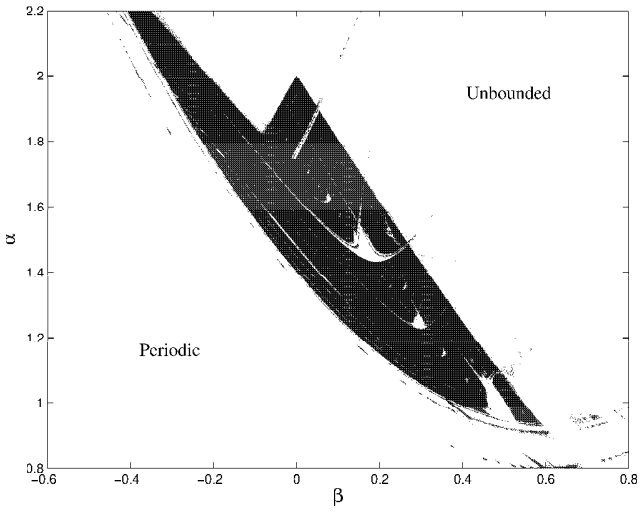

Figure 4: Chaotic region for the Hénon attractor.

However, this type of irregular and often fractal chaotic regions shared by most of existing "secure communication systems" is inadequate for cryptographical designs because there is no easy way to define and specify its boundary. It is preferred to have a continuous region in which all parameter values can retain complete chaoticity. A simple map satisfying this expectation is the skew tent map shown in Fig. 5:

$$F(x) = \begin{cases} x/p, & x \in [0, p], \\ (1-x)/(1-p), & x \in (p, 1], \end{cases} \tag{2}$$

where $p \in (0, 1)$ is the control parameter. For any control parameter $p \in (0, 1)$, the above piecewise linear map has a positive Lyapunov exponent and thus is always chaotic. In fact, for any piecewise linear chaotic map $F : X \to X$, if each linear segment is mapped onto the set X, the map will be chaotic and have many desired dynamical properties, such as a uniform invariant density and an exponentially-decreasing auto-correlation function [Baranovsky & Daems, 1995; Li *et al.*, 2005g]. Based on this result, as long as the control parameter does not change the onto property of each linear segment, the obtained chaotic map will be good to use in chaos-based cryptosystems.

Suggested Rule 5 *The key space $\mathcal{K}$, from which valid keys are to be chosen, should be precisely specified and avoid non-chaotic regions.*

It is sometimes taken for granted that the security of an encryption scheme is related to the size of the key space. A necessary, but not sufficient, condition for an encryption scheme to be secure is that the key space is large enough so as to frustrate brute-force attacks (see Sec. 4.4). If the chaotic region does not meet this requirement, then it should be sufficiently enlarged. However, a possible solution is not as simple as discretizing the region with a finer grid, because this could lead to *equivalent* keys, i.e., a number of different keys can all be used to decrypt a given ciphertext. When one key is very close to the real one, it could decrypt part or all of the ciphertext. To avoid such a risk, the safeguard between adjacent keys should be defined. In other words, the chaotic region should be discretized with a proper resolution, where "proper" means that any two adjacent keys are not equivalent. In the chaotic regime, the sensitivity to parameters will guarantee that two orbits starting from the same initial point but with slightly different parameters will exponentially diverge. However, the need for synchronization sometimes allows for a significant parameter mismatch, which allows some specific attacks (such as General Synchronization based attacks, see Sec. 4.2.3 for more details).

¿From the cryptographical point of view, a secret parameter should be sensitive enough to guarantee the so-called avalanche property: even when the smallest change occurs in the parameter, the ciphertext will change dramatically. Ideally, it is expected that about half of all ciphertext bits will be changed, i.e., assuming

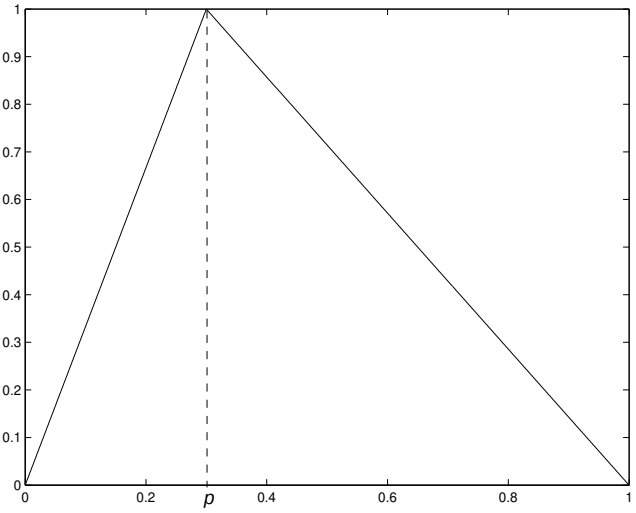

Figure 5: Skew tent map with a control parameter p.

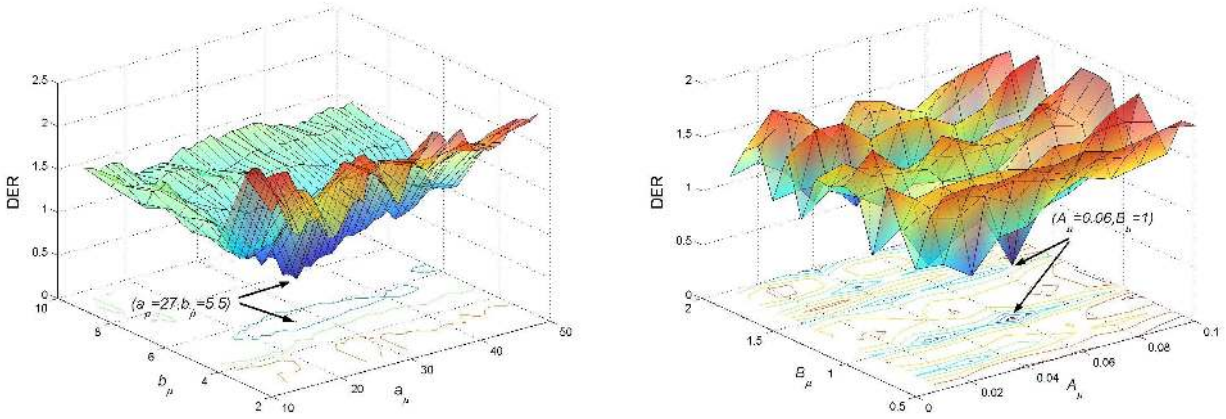

Figure 6: Two BER plots of a chaos-based cryptosystem, with two fixed secret parameters and two changeable ones. In the plots, DER means decryption-error-rate, which is a variant of BER. See Sec. C of [Li *et al.*, 2005f] for more details.

that the bit-length of a ciphertext is L, the mathematical expectation of the number of changed bits is $L/2$. For example, a natural idea to do so is to iterate the employed chaotic map for several times [Zhou & Ling, 1997b], but it will do harm to the encryption speed.

Suggested Rule 6 *The useful chaotic region, i.e., the key space $\mathcal{K}$, should be discretized in such a way that the avalanche effect is guaranteed: two ciphertexts encrypted by two slightly different keys $k_1, k_2 \in \mathcal{K}$ should be completely different.*

In some chaotic cryptosystems where more than one parameter is used as part of the key, it is possible to fix one of them and then try to estimate the others using a bit-error-rate (BER) attack, also known as error function attack (EFA) [Wang *et al.*, 2004; Álvarez *et al.*, 2004e]. This is an undesirable setting. Ideally, when the key is made from a number of parameters, the recovered signal affected by an illegal attempt of decryption should never reveal useful information to the attacker, as one parameter is slowly varied. The BER or EFA plot should be flat except at the exact key value. In other words, except when all sub-parameters are correct (i.e., the secret key exact value is guessed), the recovered signal should always appear the same as the ciphertext signal, from both statistical and semantic points of view. This implies that the total key space should be a product, but not a summation, of all the parameters involved. As a negative example, Figure 6 shows two BER plots of a chaos-based cryptosystem proposed in [Minai & Pandian, 1998], which has been broken by Li *et al.* [2005f].

Suggested Rule 7 *Partial knowledge of the key should never reveal partial information about the plaintext nor the unknown part of the key.*

3.3 Key generation

Once the key has been defined and the key space has been properly characterized, the process of choosing good keys should be explained in detail. If some nontrivial (ideally large) parameter ranges are given and the parameter values can be randomly chosen from within these ranges, then it is clear that there is no possibility of generating weak or degenerate keys.

Sometimes, a useful chaotic region has a very irregular shape. This shape could be enclosed in a simple and regular one, such as an n-dimensional sphere or a cube, and the key could be chosen randomly within this regular-shape region and then be checked if it is indeed located within the useful chaotic region.

Suggested Rule 8 *The algorithm or process of generating valid keys from the key space $\mathcal{K}$ should be precisely specified.*

4 Security Analysis

Here comes the core of cryptanalysis, provided that security is the foremost concern in a cryptosystem, although usually the most difficult to assess. After a new cryptosystem has been designed, it should always be evaluated by some basic security analysis. Although this analysis cannot comprise all possible attacks against the new cipher, it should cover at least some best-known attacks, to check if it can pass these typical tests. This analysis helps to spot and correct defects and flaws before the new scheme is published.

First of all, to resist common attacks, the designed cryptosystem should have the following two basic cryptographic properties: confusion and diffusion. The first property is intended to make the relationship between the key and the ciphertext as complex as possible, thus frustrating attempts to study the ciphertext looking for redundancies and statistical patterns. The second property refers to rearranging or spreading out the bits in the message so that the influence of individual plaintext or key bits is spread out over as much of the ciphertext as possible. Obviously, the suggested Rule 6 mentioned above corresponds to the diffusion property of the key. Here, some rules corresponding to the two properties are needed. To achieve the confusion property, statistical properties of the ciphertext, such as distribution, correlation and differential probability, should be independent of the exact value of the key and of the plaintext. Many proposed chaos-based cryptosystems are easily broken because of the lack of the confusion property [Álvarez *et al.*, 2000, 2004c,e].

As Fridrich pointed out in [Fridrich, 1998], amongst many other desirable properties, from a security viewpoint a good cryptosystem (based on symmetric or asymmetric encryption) should:

1. Be sensitive with respect to keys: flipping one bit in a key creates completely different ciphertext when applied to the same plaintext.
2. Be sensitive with respect to plaintext: flipping one bit in the plaintext creates completely different ciphertext.
3. Map plaintext to random ciphertext: there should not be any patterns in the ciphertext.

The first two items correspond to the diffusion property, and the last one to the confusion property. Similarly, we have the following two rules.

Suggested Rule 9 *For two keys (or two plaintexts) with the slightest difference, no distinguishable difference between the corresponding ciphertexts can be found by any known statistical analysis.*

Suggested Rule 10 *The ciphertext should be statistically undistinguishable from the output of a truly random function, and should be statistically the same for all keys.*

In the following, we discuss different types of attacks that should be considered in the design of a new chaos-based cryptosystem. It should be bear in mind that passing one or more of these tests does not guarantee that the cryptosystem will be secure, but nevertheless it is a first step towards a secure cryptosystem that cannot be overlooked.

4.1 Cryptographical attacks

As mentioned in Sec. 3, when performing cryptanalysis on an encryption algorithm, a general assumption is that the cryptanalyst knows exactly the design of the algorithm and how the cryptosystem works, i.e., he knows everything about the cryptosystem except the secret key. This is a reasonable assumption, since an encryption algorithm has to be sold to multiple users in the market or is easy to be stolen. As a consequence,

reverse engineering is always possible for both software and hardware implementations to reveal all details on how a cipher works. History has shown that maintaining the secrecy of the cryptosystem is very difficult indeed.

The basic concepts related to cryptography and cryptanalysis, such as plaintext, ciphertext, keyspace, etc, and their relationships, can be described in a formal way by using the following mathematical notation [Stinson, 1995, p. 1], illustrated in Fig. 7. A cryptosystem is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \{e_k : k \in \mathcal{K}\}, \{d_k : k \in \mathcal{K}\})$, where the following conditions are satisfied.

1. $\mathcal{P}$ is a finite set of possible plaintexts.
2. $\mathcal{C}$ is a finite set of possible ciphertexts.
3. $\mathcal{K}$, the key space, is a finite set of possible keys.
4. For each $k \in \mathcal{K}$, there is an encryption rule $e_k \in \mathcal{E}$ and a corresponding decryption rule $d_k \in \mathcal{D}$. Each $e_k : \mathcal{P} \to \mathcal{C}$ and $d_k : \mathcal{C} \to \mathcal{P}$ are functions such that $d_k(e_k(x)) = x$ for every plaintext $x \in \mathcal{P}$. $\mathcal{E}$ and $\mathcal{D}$ represent the sets of all possible encryption and decryption rules respectively.

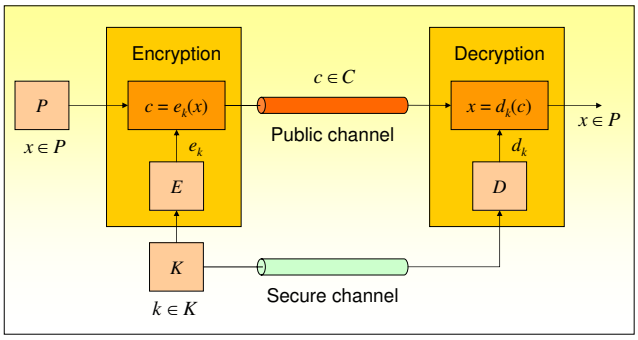

Figure 7: Cryptographic elements in a symmetric cryptosystem.

According to [Stinson, 1995, p. 25], when dealing with cryptanalysis, there are different levels of attacks on cryptosystems. These are enumerated as follows, ordered from the hardest type of attack to the easiest.

1. Ciphertext-only: The opponent possesses one or more ciphertexts, $y_1, \cdots, y_n \in \mathcal{C}$.
2. Known-plaintext: The opponent possesses one or more plaintexts, $x_1, \cdots, x_n \in \mathcal{P}$, and the corresponding ciphertexts, $y_1, \cdots, y_n \in \mathcal{C}$.
3. Chosen-plaintext: The opponent has obtained temporary access to the encryption machinery, hence he can choose some plaintexts, $x_1, \cdots, x_n \in \mathcal{P}$, and get the corresponding ciphertexts, $y_1, \cdots, y_n \in \mathcal{C}$.
4. Chosen-ciphertext: The opponent has obtained temporary access to the decryption machinery, hence he can choose some ciphertexts, $y_1, \cdots, y_n \in \mathcal{C}$, and get the corresponding plaintexts, $x_1, \cdots, x_n \in \mathcal{P}$.

In each of these four attacks, the objective is to determine the key, $k \in \mathcal{K}$, or one of its equivalent forms, that was used in encryption/decryption[3]. The last two attacks, which might seem unreasonable at first sight, are very common when the cryptographic algorithm, whose key is fixed by the manufacturer and unknown to the attacker, is embedded in a device which the attacker can freely manipulate. Daily life examples of such devices are electronic purse cards, GSM phone SIM (Subscriber Identity Module) cards, POST (Point Of Sale Terminals) machines, or web application session token encryption. Many examples of how to break a chaotic cryptosystem with known-plaintext and chosen-plaintext attacks can be found in, e.g., [Biham, 1991; Stojanovski *et al.*, 1996; Álvarez *et al.*, 2000, 2003a,b,c,d; Hu *et al.*, 2003; Liu *et al.*, 2004; Li *et al.*, 2004b, 2005a,b,c,e,f]. Known-plaintext attacks also play a significant role in the error function attack [Wang *et al.*, 2004].

Suggested Rule 11 *It should be checked whether the designed cryptosystem can be broken by the relatively simple known-plaintext and chosen-plaintext attacks, and even chosen-ciphertext attacks.*

In addition to the four general attacks described above, there are some other more specialized attacks based on them. For instance, for the case of block ciphers, resistance to differential and linear cryptanalysis should be proved or checked very carefully when presenting a new cryptosystem.

[3]For public-key cryptosystems, only the private key is concerned.

4.1.1 Differential cryptanalysis

Differential cryptanalysis was introduced by Biham and Shamir [1993, p. 11]. It is a chosen-plaintext attack aimed at finding the secret key in an iterated cipher. It analyzes the effect of particular differences in plaintext pairs on the differences of the resultant ciphertext pairs. These differences can be used to assign probabilities to the possible keys and to locate the most probable key. Usually, the difference is chosen as a fixed XORed (exclusive-or) value of the two plaintexts. The goal of differential cryptanalysis is to reduce the number of tests when compared to a brute-force attack (see Sec. 4.4).

Let $x, x^* \in \mathcal{P}, x \neq x^*$, such that $\Delta x = x \oplus x^*$, i.e., Δx is the difference of the pair of plaintexts x and x^*. Let $y = e_k(x) = f(x)$ and $y^* = e_k(x^*) = f(x^*)$. Their difference is $\Delta y = y \oplus y^*$. The differential approximation probability of a given map f (DP_f) is defined as (see [Jakimoski & Kocarev, 2001]):

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in \mathcal{P} | f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n} \right),$$

where 2^n is the cardinality of $\mathcal{P}$. Thus, DP_f acts as a measure of the diffusion (or sensitive dependence on initial condition). The smaller the value of DP_f, the better its cryptographic properties, i.e., its resistance to differential cryptanalysis. A recent example of computing DP_f for a chaos-based block cipher can be found in [Szczepanski *et al.*, 2005].

A variation of differential cryptanalysis applied to image encryption can be found for instance in [Chen *et al.*, 2004; Mao *et al.*, 2004].

4.1.2 Linear cryptanalysis

Linear cryptanalysis was first introduced by Matsui [1994]. It is a known-plaintext attack, whose purpose is to construct a linear approximate expression of the block cipher under study. A linear expression for one iteration is an equation for a certain modulo two sum of the round input bits and the round output bits as a sum of round key bits. This expression can have only two possible values: 0 and 1. Each of these expressions is satisfied with a probability $p \neq 1/2.$, where the magnitude of $|p - 1/2|$ represents its effectiveness. In [Harpes *et al.*, 1995] Matsui's idea was generalized by replacing his linear expressions by I/O sums. Likewise, instead of using the magnitude $|p - 1/2|$ as a measure of effectiveness, "imbalances" were used, which are similarly defined but with an extra factor of two so that the imbalance will lie between 0 and 1 inclusive, i.e., $|2p - 1|$.

Let $x, y \in \mathcal{P}$, such that $y = e_k(x) = f(x)$. The nonlinearity of the encryption function f is measured using the linear approximation probability (LP_f), defined as (see [Jakimoski & Kocarev, 2001]):

$$LP_f = \max_{a,b \neq 0} \left(\frac{\#\{x \in \mathcal{P} | x \bullet a = f(x) \bullet b\} - 2^{n-1}}{2^{n-1}} \right)^2,$$

where a and b are two bit masks, and $\bullet$ denotes the parity of bit-wise product. Immunity of f to linear cryptanalysis requires that LP_f is as small as possible. Again, a recent example of computing LP_f for a chaos-based block cipher can be found in [Szczepanski *et al.*, 2005].

Suggested Rule 12 *Resistance to differential and linear cryptanalysis should be proved or checked very carefully in digital block ciphers.*

4.2 Chaos-specific attacks

Different methods have been proposed to attack chaos-based cryptosystems, for both analog and digital settings, to different degrees of success. Since the attacking methods of digital chaotic ciphers are not easy for classification[4], here we only discuss the analog case. There are three possibilities for cryptanalysis [Beth *et al.*, 1994]:

1. Extracting the message signal $m(t)$ directly from the transmitted ciphertext signal $c(t)$.
2. Extracting the chaotic carrier signal $x(t)$ to recover the message signal $m(t)$ by removing $x(t)$ from the transmitted ciphertext signal $c(t)$.
3. Estimating the secret parameters from the transmitted ciphertext signal $c(t)$ to completely break the whole cryptosystem.

[4]The attacks to different digital chaotic ciphers are generally rather different, due to their completely different encryption structures. See [Álvarez *et al.*, 2000, 2003a,b,c, 2004e; Li *et al.*, 2003b,c, 2004a,b] for some examples, and [Li, 2005b] for a comprehensive survey.

4.2.1 Message signal extraction

In chaotic masking schemes, extracting the message signal 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: autocorrelation and cross-correlation analysis, power spectral analysis and filtering technique (both linear and nonlinear) [Yang *et al.*, 1998a; Álvarez & Li, 2004b; Álvarez *et al.*, 2004a, 2005b, 2004c,d,f], return-map analysis [Pérez & Cerdeira, 1995; Yang *et al.*, 1998c], etc.

In chaotic switching (i.e., CSK) and chaotic modulation schemes, the direct extraction of the message signal is also possible, where no special constrains are required for $m(t)$. This can be accomplished using return maps [Pérez & Cerdeira, 1995; Zhou & Chen, 1997; Yang *et al.*, 1998c], correlation analysis [Zhou & Chen, 1997], generalized synchronization technique [Yang *et al.*, 1998b; Álvarez *et al.*, 2005b, 2004c], power energy analysis [Álvarez *et al.*, 2004c] or short-time period (also called short-time zero-crossing rate – STZCR) [Yang, 1995; Álvarez & Li, 2004c].

The power spectral or filtering analysis exploits a limitation of chaotic signals used to mask the information signal. The basic fundamental requirement of the pseudorandom noise used in cryptography is that its spectrum should be infinitely broad, flat, and of much higher power density than the signal to be concealed. In other words, the plaintext power spectrum should be effectively buried into the pseudorandom noise power spectrum. However, most secure applications proposed in the literature do not satisfy this condition. On the contrary, the spectrum of the signal generated by chaotic oscillators commonly used such as Rossler, Lorenz, Chua, Duffing, etc., is of narrow band, decaying very fast with increasing frequency, and shows a power density much lower than the plaintext at the plaintext frequencies used. Hence, it can not cope with a filtering attack intended to separate the masking signal and the plaintext, such as the one illustrated in Fig. 8. This attack is very powerful because it does not require any *a priori* knowledge of the system structure or configuration.

The return-map method was initially devised by [Pérez & Cerdeira, 1995] and further developed by [Zhou & Chen, 1997; Yang *et al.*, 1998c; Li *et al.*, 2005d,e,f]. Given one of the variables in the chaotic system, one or more proper return maps can be constructed allowing for a partial reconstruction of the dynamics. By analyzing the evolution of the signal on the attracting sets of those maps, the message can be extracted under certain conditions. Two typical examples of return map attacks are shown in Fig. 9. These attacks can be performed without the knowledge of the precise structure of the chaotic system in use. This method can decrypt ciphertexts encrypted using chaotic switching, chaotic masking, chaotic modulation. However, it does not work for phase synchronization based cryptosystems.

The generalized synchronization attack, first introduced in [Yang *et al.*, 1998b], assumes that the attacker knows the type of attractor used for the transmission and reception, but ignores the precise value of the parameters, which usually are considered to be the secret key of the cryptosystem. Using the concept of generalized synchronization (GS) defined in [Rulkov *et al.*, 1995], the attacker's receiver uses a set of parameters which is completely different to the secret key and thus will never achieve synchronization. Nevertheless, by measuring the synchronization error over time, it is possible to detect the switching between the two attractors in the transmitter as a variation in the square error. See Fig. 10 for a typical example on how such switching events can be detected. This one is a very powerful technique when complete synchronization is used. It does not work for some other types of synchronization though.

4.2.2 Chaotic carrier signal extraction

In chaotic masking and some chaotic modulation schemes, the chaotic carrier signal $x(t)$ may be extracted using nonlinear dynamic (NLD) forecasting techniques proposed by Short et al. in [1996; 1994; 1997; 1998; 2001]. Once the chaotic carrier signal is extracted, the message signal can be then obtained by removing the carrier signal from the transmitted ciphertext signal. This attacking method is the first one proposed in the literature and also the best well-known one in chaotic cryptography. The disadvantages of this attacking method include: 1) it cannot recover the message signal exactly; 2) it cannot work well for many chaotic modulation schemes.

4.2.3 Parameter estimation

As analyzed in [Zhou & Ling, 1997b; Wang *et al.*, 2004], many secure chaos-based communication schemes are not sufficiently sensitive to parameter mismatch, which makes it possible to use approximate parameter values for decryption. Note that this offends Rule 6 listed in this paper, and means the reduction of the key space. Similar cryptanalysis results have also been developed for some specific chaos-based cryptosystems [Álvarez *et al.*, 2004e,b; Li *et al.*, 2005f; Álvarez *et al.*, 2005b].

Low sensitivity of chaos-based cryptosystems to parameter mismatch implies another fact: one can approximately estimate the secret parameter to break the cryptosystem. There are some different methods of realizing parameter identification: direct solving parameters from the ciphertext signal [Vaidya & Angadi, 2003; Liu

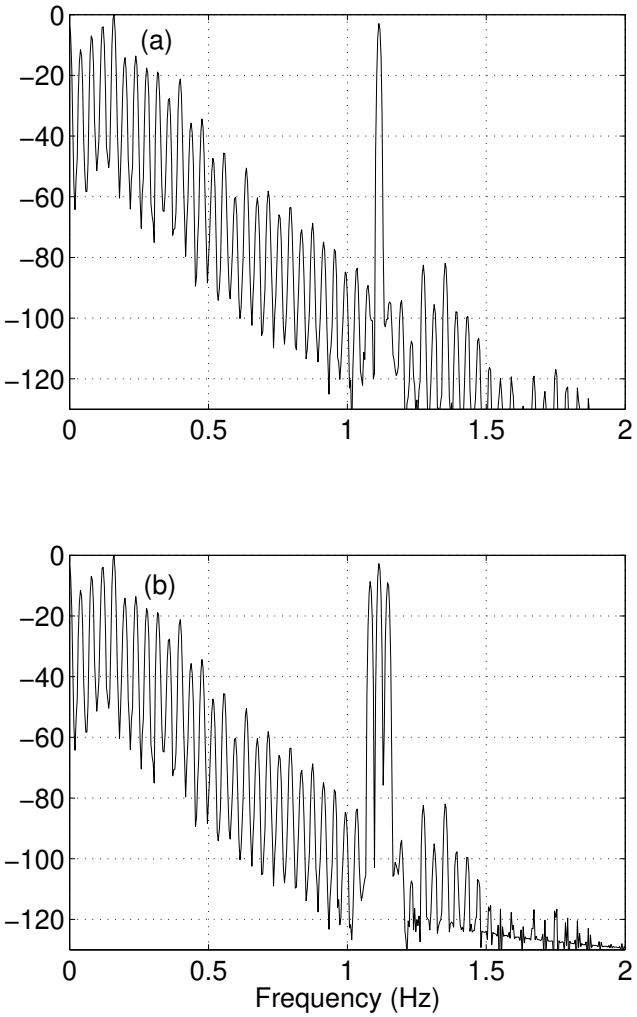

Figure 8: Logarithmic power spectra, as a function of frequency, of two sinusoidal plaintexts masked by the Duffing oscillator (see [Álvarez *et al.*, 2005a]). Plaintext signal components clearly emerge over the background noise created by the chaotic oscillator. By high-pass filtering the ciphertext to eliminate the chaotic masking component, the plaintext information can be retrieved with high fidelity.

et al., 2004], estimating parameters via generalized synchronization [Tao *et al.*, 2003; Tao & Du, 2003], adaptive control/synchronization techniques [Dedieu & Ogorzałek, 1997; Zhou & Lai, 1999; Huang, 2004], correlation analysis [Geddes *et al.*, 1999], or return maps [Li *et al.*, 2005d]. The risk of parameter identification is not so well-known in chaotic cryptography as Short's NLD-forecasting attack and return-map attacks, but it should receive special attention due to its power to completely break many chaos-based cryptosystems. A recent example of this kind of attack can also be found in [Álvarez *et al.*, 2005b] and is illustrated in Fig. 11. It shows that the error grows monotonically with the mismatch between the transmitter and receiver parameters $\{|\sigma^* - \sigma|,\ |\mu^* - \mu|\}$, and that the minimum error corresponds to the receiver system parameters values $\{\sigma^*,\ \mu^*\}$ exactly matching the transmitter system parameters values $\{\sigma,\ \mu\}$. The parameter value recovery procedure consists of the straightforward search for the minimum recovery error. Figure 12 shows another example recently reported in [Li *et al.*, 2005d]. In the broken cryptosystem, one secret parameter can be calculated with an iterative algorithm, employing the fact that return maps reconstructed from different parameters have different shapes.

Suggested Rule 13 *It should be checked whether the cryptosystem can be broken by all known chaos-specific attacks.*

4.3 Application-specific attacks

There are special attacks for specific applications. For example, for digital images (videos), unlike normal one-dimensional data, strong correlation always exists between different pixels (transform coefficients). Such correlation information can be utilized to develop some effective correlation-based attacks, if the information is

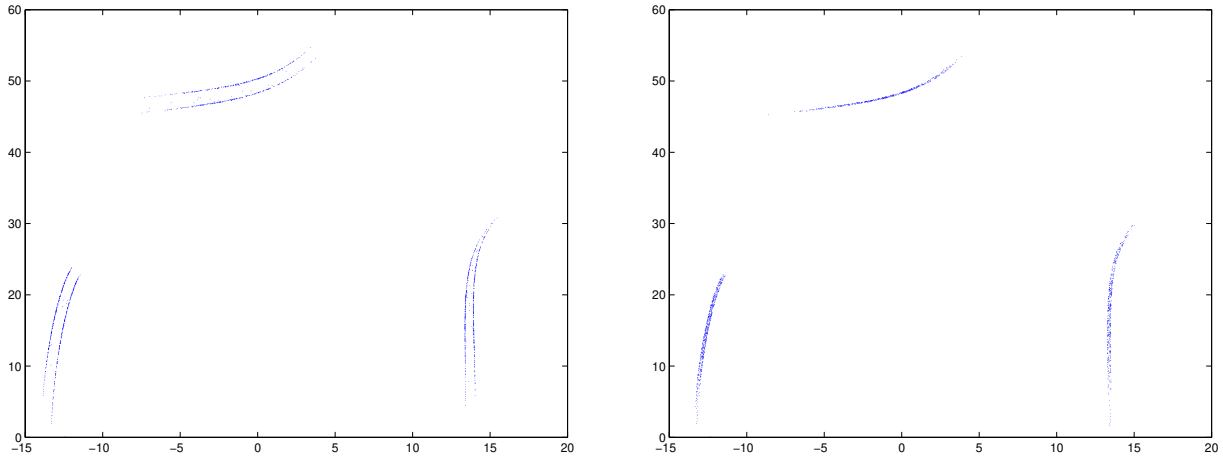

Figure 9: Two return maps of two chaos-based cryptosystems based on the Lorenz system: a) return map of a typical chaotic switching cryptosystem; b) return map of a typical chaotic masking cryptosystem. For chaotic switching, the current plain-bit is extracted by observing in which branch the current return-map point lies. For chaotic masking, the plain-signal can be partially reconstructed from the fluctuation of the return-map points around the midline of each branch.

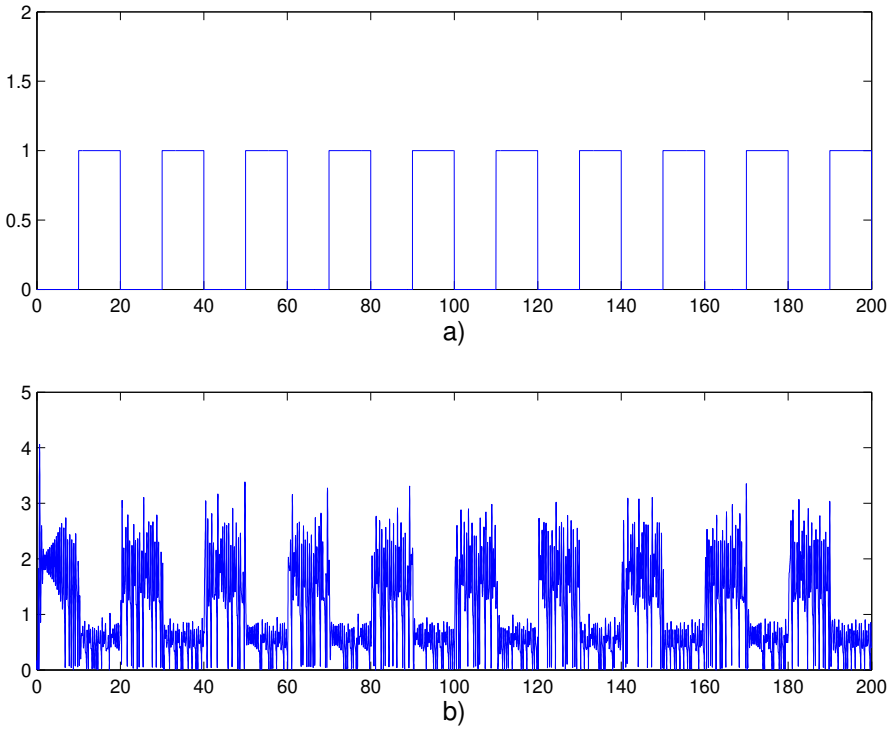

Figure 10: GS attack of a typical chaotic switching cryptosystem based on the Lorenz system: a) the plain-signal $m(t)$, b) the error signal $|x_2(t) - x_1(t)|$, where $x_1(t)$, $x_2(t)$ denote the first variable of the sender and the attacker system, respectively. The two parameters used in the sender system for switching are $b_0 = 4.0$, $b_1 = 4.4$, and the parameter used in the attacker system is $b' = 4.6$.

not successfully canceled in cipher-images/cipher-videos. In Fig. 13, it is shown that how such correlation works for a chaos-based image encryption scheme, as reported in [Li *et al.*, 2005a], where only partial information of the secret key is broken but almost all visual information of the plain-image has been successfully recovered. Similar results can also be found in [Li & Zheng, 2002; Li *et al.*, 2004e].

In addition, in some applications, cryptosystems need to be specially optimized to make the encryption more efficient. However, sometimes there exists a tradeoff between efficiency and security, and the increase of efficiency causes decrease of security. For example, encrypting partial data of digital videos is very useful to promote the encryption speed and make the cryptosystem practical, but it is possible to reconstruct partial

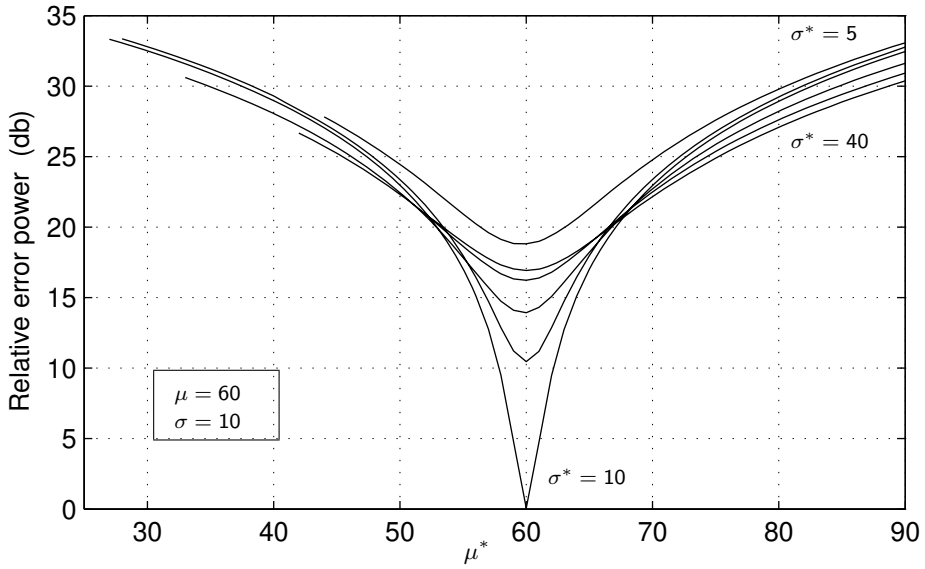

Figure 11: An example of parameter estimation by minimizing the mean of the error power ε^2, for $\sigma^* = \{5, 7.5, 10, 20, 30, 40\}$ as a function of μ^*, where σ^* and μ^* are test values of two secret parameters in a chaos-based cryptosystem.

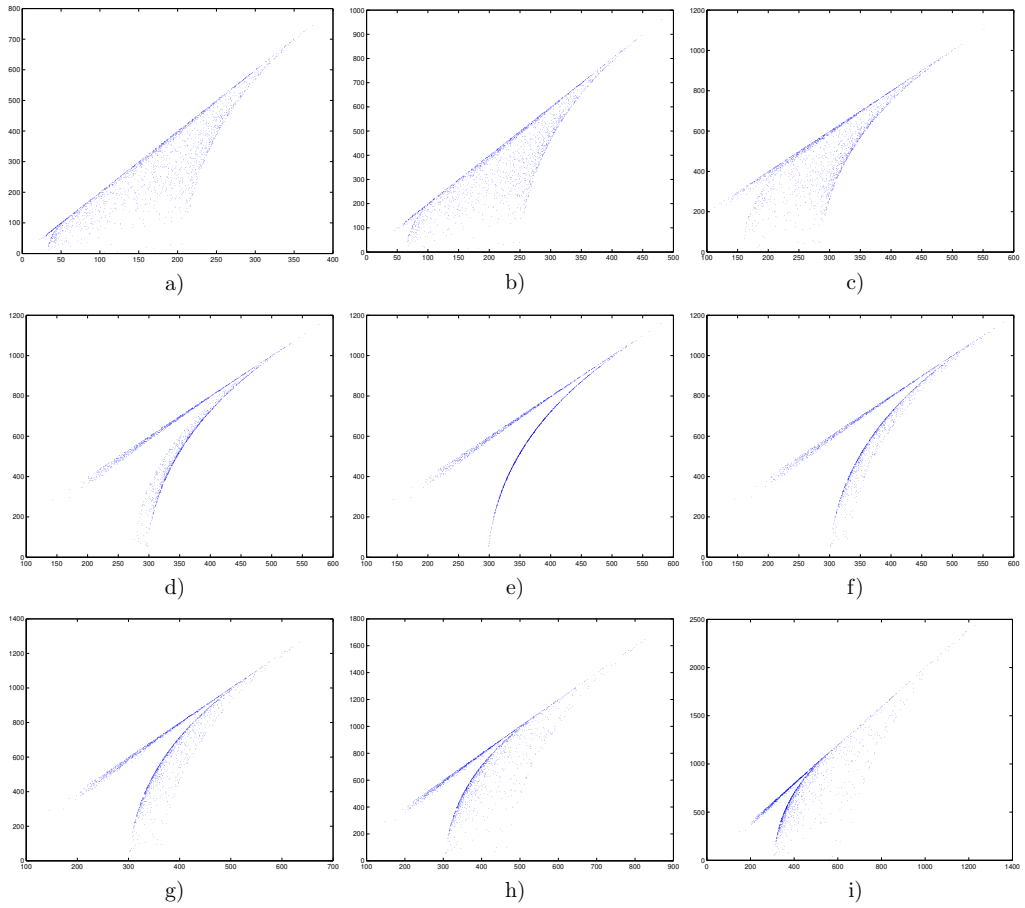

Figure 12: An example of estimating a secret parameter from return maps [Li *et al.*, 2005d]. The nine return maps are reconstructed from nine different attacker parameters: $M + 0.9$, $M + 0.4$, $M + 0.1$, $M + 0.01$, M, $M - 0.01$, $M - 0.02$, $M - 0.04$, $M - 0.06$, where M is the secret parameter used in the sender system. Considering the fact that different return maps have different shapes, an iterative algorithm can be developed to determine the secret parameter with a desired precision.

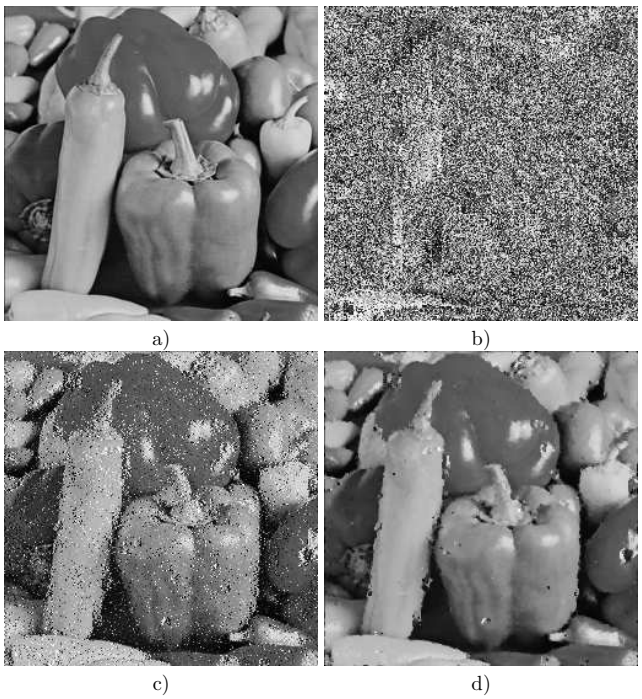

Figure 13: An attack to a chaos-based image encryption method [Li *et al.*, 2005a]: a) the plain-image, b) the cipher-image, c) the image recovered by the attack, d) the enhanced image of c).

visual information about the plain-videos from the partial non-encrypted data. Therefore, if there exists a tradeoff between efficiency and security, explicit criteria should be provided to show how to balance the two considerations. For more discussions on chaos-based image and video encryption, see [Li *et al.*, 2004d].

Suggested Rule 14 *It should be checked whether the cryptosystem can be broken by all known application-specific attacks.*

4.4 Brute-force attacks

A brute-force attack is a method of breaking a cipher by exhaustively searching all possible keys. The quicker the brute-force attack, the weaker the cipher. The feasibility of a brute-force attack on a cipher depends on the key space size κ of the cipher and on the amount of computational power available to the attacker. Given today's computer speed, it is generally agreed that a key space of size $\kappa < 2^{100}$ is not sufficiently secure.

Suggested Rule 15 *To provide a sufficient security against brute-force attacks, the key space size should be* $\kappa > 2^{100}$.

It should be noted that this requirement might be very difficult to meet because the key space might not allow for such a big number of different strong keys. For instance, Fig. 4 was created by using computation with resolution of 10^{-3}, so there are 1400×3000 different points. To get a number of keys with $\kappa > 2^{100} \simeq 10^{30}$, the resolution must be 10^{-15}. However, with that resolution, thousands of keys would become equivalent, unless there is a strong sensitivity to parameter mismatch.

The major problem of analog secure communication techniques is robustness. Under adverse but realistic communications conditions, such as transmission through a real channel in a noisy environment (see Sec. 5), filtering in the channel or attenuation of the driving signal, desynchronization will result in most cases, thus rendering the system useless. Therefore, a tradeoff between synchronization robustness and security must be reached: if the system is very sensible, it will be more secure but synchronization might not be achieved; on the other hand, if the tolerances are larger, then a brute-force attack will be easier.

Furthermore, as a consequence of the unavoidable errors on the values of the circuit components, the synchronization process can be heavily influenced. Provided that the parameter adjustment at transmitter and receiver constitutes the system key, the tolerances in circuit components reduces the key space and makes easier a brute-force attack.

In addition, as mentioned above in the suggested Rule 2, when chaotic systems are implemented digitally, the dynamical degradation may lead to weak keys and further reduce the key space. For digital cryptosystems,

the known negative influence of the digitalization effect of chaotic systems should be taken into account to estimate the size of key space. For example, in Zhou et al.'s chaotic ciphers proposed in [Zhou & Ling, 1997b], many weak keys have been found and an enhanced brute-force attack has been proposed (see [Li *et al.*, 2003a,b] or [Li, 2003, Chap. 4] for details).

4.5 Statistical testing

Most chaotic cryptosystems in essence behave as stream ciphers: the nonlinear equations governing the evolution of the system are used to generate a keystream $\mathbf{z} = z_1 z_2 \ldots$ by using the system parameters, initial conditions, etc., as the key, k. If $\mathbf{p} = p_1 p_2 \ldots$ is the plaintext string, the keystream $\mathbf{z}$ is used to encrypt the plaintext string according to the rule:

$$\mathbf{c} = c_1 c_2 \ldots = e_{z_1}(p_1) e_{z_2}(p_2) \ldots$$

Decrypting the cipher text string $\mathbf{c}$ at the receiver can be accomplished by computing the keystream $\mathbf{z}$ given the knowledge of the key k and undoing the operations e_{z_i}.

A simple example is the Vernam cipher [Stinson, 1995, p. 50], also known as *one-time pad*, a stream cipher defined on the binary alphabet, which can be proved to be theoretically unbreakable. The binary plaintext $\mathbf{p} = p_1 p_2 \ldots$ is encrypted with a binary keystream $\mathbf{z} = z_1 z_2 \ldots$, producing a binary ciphertext $\mathbf{c} = c_1 c_2 \ldots$ according to the rule:

$$c_i = p_i \oplus z_i = (p_i + z_i) \mod 2.$$

It is crucial to the security of the keystream cipher that the keystream should be as long as the message, unpredictable, and never reused, thus preventing two different messages encrypted with the same portion of the keystream being intercepted or generated by an attacker.

Some requirements must be obeyed to ensure that a chaotic pseudo-random generator can generate the secret keystream sequence without repetition nor predictability. These requirements include:

1. Parameter sensitivity: small variation in one of the system parameters is enough to make two trajectories, starting at the same initial point, separate at exponential rate.

2. Initial condition sensitivity: two trajectories starting at two different, though arbitrarily close, initial points separate from each other exponentially.

3. Ergodicity: almost every trajectory tends to an invariant distribution that is independent of the initial conditions, and almost every trajectory will eventually visit any arbitrary interval of arbitrary size.

Due to these restricting conditions, the chaotic transmitter system will only be reproducible at reception if the exact values of initial conditions and parameters are known. Thus, these values can be considered as keys of the chaos-based cryptosystem.

There are two basic statistical requirements for any PRNG. First, the pseudo-random sequence should pass all known statistical tests for randomness. Second, the period of the pseudo-random sequence should be as large as possible.

According to [Menezes *et al.*, 1997, Sec. 5.4], although it cannot be proven mathematically that a generator is indeed a PRNG, there exist many tests that help to detect weaknesses in the generator. Passing the tests merely provides probabilistic evidence that the generator produces sequences which have certain characteristics of random sequences. When evaluating a PRNG for cryptographic purposes, the National Institute of Standards & Technology (NIST) proposes a battery of statistical tests that must be performed [NIST, 2000]: frequency, block frequency, serial, cumulative sums, runs, long runs, Marsaglia's rank, spectral, nonoverlapping template matchings, overlapping template matchings, Maurer's universal statistical, approximate entropy, random excursions, Ziv-Lempel complexity, and linear complexity. Most of these tests are covered in greater detail in [Menezes *et al.*, 1997; Knuth, 1997; Karian & Dudewicz, 1999].

Suggested Rule 16 *When a keystream cipher is used, the security study should include the statistical test results conducted on the pseudo-random number generator.*

5 Issues Related to the Transmission Channel

Many analog secure communication systems proposed thus far were tested only using Matlab or some other simulation programs, but not through a real channel under real transmission conditions. It should be noted that a real channel is subjected to significant noise, has a limited bandwidth, and undergoes attenuation effect. When designing a new secure communication scheme, in addition to the concerned security analysis, the

channel characteristics should also be taken into account, thus preventing the system from failing when tested in a noisy, bandwidth-limited, and attenuated channel. Usually, no description of the intended application or type of signals is made: whether the system will be used in telephony, radio, TV, etc. Different media require different transmission channels and are imposed different limitations.

For instance, according to the USA's Federal Communications Commission's Part 68 rules, practical telephone lines have signal/noise ratio between 30 and 45 dB. Noise comes in many forms such as electrical interference from fluorescent fixtures, hiss from the many amplifier stages in the voice path, speech correlated noise can be introduced from non-linear speech digitizing and compression methods, and crosstalk from other conversations.

In a telephone network, the bandwidth's low end is rolled off at 180 Hz to stay away from the 50-60 Hz region, due to the possible interference from power lines. The high end cut off is very critical. Due to the fact that voice on the telephone network is digitized at 8 kHz sampling rate, any signal above 4 kHz will be aliased back as noise in the voice band; hence voice lines roll off at about -25 dB at 4 kHz.

Finally, modern telephone companies compensate the attenuation due to the junction switches and trunk link; but the attenuation of the subscriber loop depends on its length and can not be effectively controlled. Usually the subscriber loop attenuation range from 0 and 8 dB at each end (0 dB to 16 dB taking into account both ends).

All these examples taken from public switched telephone networks serve the purpose of illustrating how the channel constraints cannot be neglected when designing a communication system. If they are simulated and no real implementation is made, channel characteristics should be added to the simulation. The following rule might be a reference:

Suggested Rule 17 *A designed secure communication system should work in a real channel environment with* ≈ -40 *dB signal/noise ratio, with a certain limited bandwidth, and with attenuation between* 0 *dB and* 16 *dB.*

6 Conclusions

A set of rules have been suggested as design and validation guidelines for chaos-based cryptosystems. These guidelines are by no means comprehensive and do not intend to constrain the freedom and creativity of the designer. However, if these suggested rules are followed, a reasonable degree of security and most acceptable features of cryptography can be guaranteed. More importantly, on this common ground, a new chaos-based cryptosystem can be easily studied by the cryptography community. It is the authors' hope that a better dialogue between the chaos and cryptography communities will be gradually established, which will be mutually beneficial.

Acknowledgements

This research was partially supported by Ministerio de Educación y Ciencia of Spain, Proyecto SEG2004-02418. The authors thank Prof. Dr. Guanrong Chen and Dr. Fausto Montoya for their help in reviewing manuscripts of this paper, and thank Dr. Shihong Wang for sending the C codes of the CML-based cipher [Lü *et al.*, 2004] for testing the encryption speed.

References

Acharya, R., Subbanna, P., Kumarc, S. & Choo, L. [2003] "Transmission and storage of medical images with patient information," *Comput. Biol. Med.* **33**, 303–310.

Álvarez, E., Fernández, A., García, P., Jiménez, J. & Marcano, A. [1999a] "New approach to chaotic encryption," *Phys. Lett. A* **263**, 373–375.

Álvarez, G., Hernández, L., Montoya, F. & Muñoz, J. [2004a] "Cryptanalysis of a novel cryptosystem based on chaotic oscillators and feedback inversion," *J. Sound Vibrat.* **275**, 423–430.

Álvarez, G., Hernandez, L., Muñoz, J., Montoya, F. & Li, S. [2005a] "Security analysis of communication system based on the synchronization of different order chaotic systems," arXiv:nlin.CD/0506056.

Álvarez, G. & Li, S. [2004a] "Breaking cryptography with chaos at the physical level," arXiv:nlin.CD/0403029.

Álvarez, G. & Li, S. [2004b] "Breaking network security based on synchronized chaos," *Comp. Comm.* **27**, 1679–1681.

Álvarez, G. & Li, S. [2004c] "Estimating short-time period to break different types of chaotic modulation based secure communications," arXiv:nlin.CD/0406039.

Álvarez, G., Li, S., Montoya, F., Pastor, G. & Romera, M. [2005b] "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," *Chaos Solitons Fractals* **24**, 775–783.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [1999b] "Chaotic cryptosystems," in L. D. Sanson, ed., *Proc. 33rd Annual 1999 International Carnahan Conference on Security Technology*, 332–338 (IEEE).

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2000] "Cryptanalysis of a chaotic encryption system," *Phys. Lett. A* **276**, 191–196.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2003a] "Cryptanalysis of a chaotic secure communication system," *Phys. Lett. A* **306**, 200–205.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2003b] "Cryptanalysis of a discrete chaotic cryptosystem using external key," *Phys. Lett. A* **319**, 334–339.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2003c] "Cryptanalysis of an ergodic chaotic cipher," *Phys. Lett. A* **311**, 172–179.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2003d] "Keystream cryptanalysis of a chaotic cryptographic method," *Comp. Phys. Comm.* **156**, 205–207.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004b] "Breaking a secure communication scheme based on the phase synchronization of chaotic systems," *Chaos* **14**, 274–278.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004c] "Breaking parameter modulated chaotic secure communication system," *Chaos Solitons Fractals* **21**, 783–787.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004d] "Breaking two secure communication systems based on chaotic masking," *IEEE Trans. Circuits Syst. II* **51**, 505–506.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004e] "Cryptanalyzing a discrete-time chaos synchronization secure communication system," *Chaos Solitons Fractals* **21**, 689–694.

Álvarez, G., Montoya, F., Romera, M. & Pastor, G. [2004f] "Cryptanalyzing an improved security modulated chaotic encryption scheme using ciphertext absolute value," *Chaos Solitons Fractals* **23**, 1749–1756.

Bao, F. [2003] "Cryptanalysis of a new cellular automata cryptosystem," in *Information Security and Privacy, 8th Australasian Conference, ACISP 2003, Wollongong, Australia, July 9-11, 2003, Proceedings*, *Lecture Notes in Computer Science*, vol. 2727, 416–427 (Springer-Verlag).

Baptista, M. S. [1998] "Cryptography with chaos," *Phys. Lett. A* **240**, 50–54.

Baranovsky, A. & Daems, D. [1995] "Design of one-dimensional chaotic maps with prescribed statistical properties," *Int. J. Bifurc. Chaos* **5**, 1585–1598.

Berstein, G. M. & Lieberman, M. A. [1991] "Method and apparatus for generating secure random numbers using chaos," US Patent No. 5007087.

Beth, T., Lazic, D. E. & Mathias, A. [1994] "Cryptanalysis of cryptosystems based on remote chaos replication," in Y. G. Desmedt, ed., *Advances in Cryptology – CRYPTO'94*, *Lecture Notes in Computer Science*, vol. 839, 318–331 (Springer-Verlag).

Biham, E. [1991] "Cryptanalysis of the chaotic-map cryptosystem suggested at EuroCrypt'91," in *Advances in Cryptology – EUROCRYPT'91*, *Lecture Notes in Computer Science*, vol. 547, 532–534 (Spinger-Verlag, Berlin).

Biham, E. & Shamir, A. [1993] *Differential Cryptanalysis of the Data Encryption Standard* (Springer-Verlag).

Boccaletti, S., Kurths, J., Osipov, G., Valladares, D. & Zhou, C. [2002] "The synchronization of chaotic systems," *Phys. Rep.* **366**, 1–101.

Bowong, S. [2004] "Stability analysis for the sinchronization of chaotic systems with different order: application to secure communication," *Phys. Lett. A* **326**, 102–113.

Cermák, J. [1996] "Digital generators of chaos," *Phys. Lett. A* **214**, 151–160.

Chen, G., Mao, Y. & Chui, C. [2004] "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos Solitons Fractals* **21**, 749–761.

Chen, J. Y., Wong, K. W., Cheng, L. M. & Shuai, J. W. [2003] "A secure communication scheme based on the phase synchronization of chaotic systems," *Chaos* **13**, 508–514.

Cuomo, K. M. & Openheim, A. V. [1993] "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.* **71**, 65–68.

Cuomo, K. M., Openheim, A. V. & Strogatz, S. H. [1993] "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II* **40**, 626–633.

Dedieu, H., Kennedy, M. P. & Hasler, M. [1993] "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing," *IEEE Trans. Circuits Syst. II* **40**, 634–641.

Dedieu, H. & Ogorzałek, M. J. [1997] "Identifiability and identification of chaotic systems based on adaptive synchronization," *IEEE Trans. Circuits Syst. I* **44**, 948–962.

Devaney, R. L. [1989] *An Introduction to Chaotic Dynamical Systems* (Addison-Wesley, Redwood City, California, USA).

Devine, C. [2004] "AES encryption benchmark," Online document, `http://www.cr0.net:8040/code/crypto/aesbench`.

Feldmann, U., Hasler, M. & Schwarz, W. [1996] "Communication by chaotic signals: The inverse system approach," *Int. J. Circuit Theory Appl.* **24**, 551–579.

Fog, A. [2000] "How to optimize for the Pentium family of microprocessors," Online document, `http://www.codingnow.com/2000/download/pentopt.htm`.

Frey, D. R. [1993] "Chaotic digital encoding: An approach to secure communication," *IEEE Trans. Circuits Syst. II* **40**, 660–666.

Fridrich, J. [1998] "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurc. Chaos* **8**, 1259–1284.

Geddes, J. B., Short, K. M. & Black, K. [1999] "Extraction of signals from chaotic laster data," *Phys. Rev. Lett.* **83**, 5389–5392.

Gladman, B. [2003] "Implementations of AES (Rijndael) in C/C++ and assembler," Online document, `http://fp.gladman.plus.com/cryptography_technology/rijndael/index.htm`.

Guo, D., Cheng, L. M. & Cheng, L. L. [1999] "A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks," *Applied Intelligence* **10**, 71–84.

Habutsu, T., Nishio, Y., Sasase, I. & Mori, S. [1991] "A secret key cryptosystem by iterating a chaotic map," in *Advances in Cryptology – EUROCRYPT'91*, *Lecture Notes in Computer Science*, vol. 547, 127–140 (Spinger-Verlag).

Halle, K. S., Wu, C. W., Itoh, M. & Chua, L. O. [1993] "Spread spectrum communication through modulation of chaos in Chua's circuit," *Int. J. Bifurc. Chaos* **3**, 469–477.

Harpes, C., Kramer, G. & Massey, J. [1995] "A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma," in J.-J. Q. L.C. Guillou, ed., *Advances in Cryptology – EUROCRYPT'95 Lecture Notes in Computer Science*, vol. 921, 24–38 (Springer-Verlag).

Hasler, M. [1998] "Synchronization of chaotic systems and transmission of information," *Int. J. Bifurc. Chaos* **8**, 647–659.

Hayes, S., Grebogi, C. & Ott, E. [1993] "Communicating with chaos," *Phys. Rev. Lett.* **70**, 3031–3034.

Hayes, S., Grebogi, C., Ott, E. & Mark, A. [1994] "Experimental control of chaos for communication," *Phys. Rev. Lett.* **73**, 1781–1784.

Hu, G., Feng, Z. & Meng, R. [2003] "Chosen ciphertext attack on chaos communication based on chaotic synchronization," *IEEE Trans. Circuits Syst. I* **50**, 275–279.

Hua, C., Yang, B., Ouyang, G. & Guan, X. [2005] "A new chaotic secure communication scheme," *Phys. Lett. A* **342**, 305–308.

Huang, D. [2004] "Synchronization-based estimation of all parameters of chaotic systems from time series," *Phys. Rev. E* **69**, 067201.

Huang, F. & Guan, Z.-H. [2005] "Cryptosystem using chaotic keys," *Chaos Solitons Fractals* **23**, 851–855.

Jakimoski, G. & Kocarev, L. [2001] "Chaos and cryptography: Block encryption ciphers based on chaotic maps," *IEEE Trans. Circuits Syst. I* **48**, 163–169.

Karian, Z. A. & Dudewicz, E. J. [1999] *Modern Statistical, Systems, and GPSS Simulation*, 2 edn. (CRC Press).

Knuth, D. [1997] *The Art of Computer Programming*, vol. 2, *Seminumerical Algorithms* (Addison-Wesley).

Kocarev, L. [2001] "Chaos-based cryptography: A brief overview," *IEEE Circuits and Systems Magazine* **1**, 6–21.

Kocarev, L., Amato, P., Ruggiero, D. & Pedaci, I. [2004] "Discrete Lyapunov exponent for Rijndael block cipher," in *Proc. 2004 International Symposium on Nonlinear Theory and its Applications* (NOLTA 2004), 609–612.

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

Kocarev, L., Jakimoski, G., Stojanovski, T. & Parlitz, U. [1998] "From chaotic maps to encryption schemes," in *Proc. IEEE Int. Symposium Circuits and Systems* (ISCAS'98), vol. 4, 514–517 (IEEE).

Lai, Y.-C., Bollt, E. & Grebogi, C. [1999] "Communicating with chaos using two-dimensional symbolic dynamics," *Phys. Lett. A* **255**, 75–81.

Lee, P.-H., Pei, S.-C. & Chen, Y.-Y. [2003] "Generating chaotic stream ciphers using chaotic systems," *Chinese J. Phys.* **41**, 559–581.

Li, C., Li, S., Chen, G., Chen, G. & Hu, L. [2005a] "Cryptanalysis of a new signal security system for multimedia data transmission," *EURASIP J. Appl. Signal Process.* **2005**, 1277–1288.

Li, C., Li, S., Zhang, D. & Chen, G. [2004a] "Cryptanalysis of a chaotic neural network based multimedia encryption scheme," in *Advances in Multimedia Information Processing – PCM 2004 Proceedings, Part III*, *Lecture Notes in Computer Science*, vol. 3333, 418–425 (Springer-Verlag).

Li, C., Li, S., Zhang, D. & Chen, G. [2005b] "Chosen-plaintext cryptanalysis of a clipped-neural-network-based chaotic cipher," in *Advances in Neural Networks – ISNN 2005: Second International Symposium on Neural Networks, Chongqing, China, May 30 - June 1, 2005, Proceedings, Part II*, *Lecture Notes in Computer Science*, vol. 3497, 630–636 (Springer-Verlag).

Li, C., Li, X., Li, S. & Chen, G. [2005c] "Cryptanalysis of a multistage encryption system," in *Proc. IEEE Int. Symposium Circuits and Systems* (ISCAS 2005), 880–883.

Li, S. [2003] *Analyese and New Designs of Digital Chaotic Ciphers*, PhD thesis, School of Electronics and Information Engieering, Xi'an Jiaotong University, Xi'an, China, available online at `http://www.hooklee.com/pub.html`.

Li, S. [2005a] "Chaotic cryptography (1): Analog chaos-based secure communications," invited lecture, Department of Physics, Beijing Normal University, Beijing, China, slides are available online at `http://www.hooklee.com/Talks/CC1.pdf`.

Li, S. [2005b] "Chaotic cryptography (2): Digital chaotic ciphers," invited lecture, Department of Physics, Beijing Normal University, Beijing, China, slides are available online at `http://www.hooklee.com/Talks/CC2.pdf`.

Li, S., Álvarez, G. & Chen, G. [2005d] "Breaking a chaos-based secure communication scheme designed by an improved modulation method," *Chaos Solitons Fractals* **25**, 109–120.

Li, S., Álvarez, G. & Chen, G. [2005e] "Return-map cryptanalysis revisited," *Int. J. Bifurc. Chaos* **16**, 1557–1568, 2006.

Li, S., Álvarez, G., Chen, G. & Mou, X. [2005f] "Breaking a chaos-noise-based secure communication scheme," *Chaos* **15**, article 013703.

Li, S., Chen, G. & Mou, X. [2005g] "On the dynamical degradation of digital piecewise linear chaotic maps," *Int. J. Bifurc. Chaos* **15**, 3119–3151.

Li, S., Chen, G. & Mou, X. [2004b] "On the security of the Yi-Tan-Siew chaotic cipher," *IEEE Trans. Circuits Syst. II* **51**, 665–669.

Li, S., Chen, G., Wong, K.-W., Mou, X. & Cai, Y. [2004c] "Baptista-type chaotic cryptosystems: Problems and countermeasures," *Physics Letters A* **332**, 368–375.

Li, S., Chen, G. & Zheng, X. [2004d] "Chaos-based encryption for digital images and videos," in B. Furht & D. Kirovski, eds., *Multimedia Security Handbook*, chap. 4, 133–167 (CRC Press, LLC), preprint is available at `http://www.hooklee.com/pub.html`.

Li, S., Li, C., Chen, G. & Mou, X. [2004e] "Cryptanalysis of the RCES/RSES image encryption scheme," Cryptology ePrint Archive: Report 2004/376, available online at `http://eprint.iacr.org/2004/376`.

Li, S., Mou, X. & Cai, Y. [2001] "Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography," in *Progress in Cryptology – INDOCRYPT 2001*, *Lecture Notes in Computer Science*, vol. 2247, 316–329 (Springer-Verlag).

Li, S., Mou, X., Cai, Y., Ji, Z. & Zhang, J. [2003a] "On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision," *Comp. Phys. Comm.* **153**, 52–58.

Li, S., Mou, X., Ji, Z. & Zhang, J. [2003b] "Cryptanalysis of a class of chaotic stream ciphers," *J. Electronics & Information Technology* **25**, 473–478 (in Chinese).

Li, S., Mou, X., Yang, B. L., Ji, Z. & Zhang, J. [2003c] "Problems with a probabilistic encryption scheme based on chaotic systems," *Int. J. Bifurc. Chaos* **13**, 3063–3077.

Li, S. & Zheng, X. [2002] "On the security of an image encryption method," in *Proceedings of 2002 IEEE International Conference on Image Processing* (ICIP 2002), vol. 2, 925–928.

Liu, L., Wu, X. & Hu, H. [2004] "Estimating system parameters of Chua's circuit from synchronizing signal," *Phys. Lett. A* **324**, 36–41.

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

Mao, Y., Chen, G. & Lian, S. [2004] "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurc. Chaos* **14**, 3613–3624.

Masuda, N. & Aihara, K. [2002] "Cryptosystems with discretized chaotic maps," *IEEE Trans. Circuits Syst. I* **49**, 28–40.

Matsui, M. [1994] "Linear cryptanalysis method for DES cipher," in T. Helleseth, ed., *Advances in Cryptology – EUROCRYPT'93*, *Lecture Notes in Computer Science*, vol. 765, 386–397 (Springer-Verlag).

Matthews, R. A. J. [1989] "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia* **XIII**, 29–42.

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

Menezes, A. J., van Oorschot, P. C. & Vanstone, S. A. [1997] *Handbook of Applied Cryptography* (CRC Press).

Minai, A. A. & Pandian, T. D. [1998] "Communicating with noise: How chaos and noise combine to generate secure encryption keys," *Chaos* **8**, 621–628.

Morgul, O. & Feki, M. [1999] "A chaotic masking scheme by using synchronized chaotic systems," *Phys. Lett. A* **251**, 169–176.

NIST [2000] "Random number generation and testing," Online document, `http://csrc.nist.gov/rng/`.

Papadimitriou, S., Bountis, T., Mavaroudi, S. & Bezerianos, A. [2001] "A probabilistic symmetric encryption scheme for very fast secure communications based on chaotic systems of difference equations," *Int. J. Bifurc. Chaos* **11**, 3107–3115.

Pareek, N. K., Patidar, V. & Sud, K. K. [2003] "Discrete chaotic cryptography using external key," *Phys. Lett. A* **309**, 75–82.

Parker, A. T. & Short, K. M. [2001] "Reconstructing the keystream from a chaotic encryption scheme," *IEEE Trans. Circuits Syst. I* **48**, 624–630.

Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S. & Shang, A. [1992] "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurc. Chaos* **2**, 973–977.

Pecora, L. M. & Carroll, T. L. [1990] "Synchronization in chaotic systems," *Phys. Lett. A* **64**, 821–824.

Pérez, G. & Cerdeira, H. A. [1995] "Extracting messages masked by chaos," *Phys. Rev. Lett.* **74**, 1970–1973.

Ruggiero, D., Pedaci, I., Amato, P. & Kocarev, L. [2004] "Analysis of the chaotic dynamic of Rijndael block cipher," in *Proc. RISP Int. Workshop on Nonlinear Circuit and Signal Processing* (NCSP'04), 77–80.

Rulkov, N. F., Sushckik, M. M., Tsimring, L. S. & Abarbanel, H. D. I. [1995] "Generalized syncronization of chaos in directionally coupled chaotic systems," *Phys. Rev. E* **51**, 980–994.

Sang, T., Wang, R. & Yan, Y. [1998] "Perturbance-based algorithm to expand cycle length of chaotic key stream," *Electron. Lett.* **34**, 873–874.

Schneier, B. [1996] *Applied Cryptography – Protocols, algorithms, and souce code in C* second edn. (John Wiley & Sons, Inc., New York, USA).

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

Shanon, C. [1949] "Communication theory of secrecy systems," *Bell Sys. Tech. J.* **28**, 656–715.

Short, K. M. [1994] "Steps toward unmasking secure communications," *Int. J. Bifurc. Chaos* **4**, 959–977.

Short, K. M. [1996] "Unmasking a modulated chaotic communications scheme," *Int. J. Bifurc. Chaos* **6**, 367–375.

Short, K. M. [1997] "Signal extraction from chaotic communications," *Int. J. Bifurc. Chaos* **7**, 1579–1597.

Short, K. M. & Parker, A. T. [1998] "Unmasking a hyperchaotic communication scheme," *Phys. Rev. E* **58**, 1159–1162.

Silva, C. P. & Young, A. M. [2000] "Introduction to chaos-based communications and signal processing," in *Proc. IEEE Aerospace Conference*, 279–299.

Stinson, D. R. [1995] *Cryptography: Theory and Practice* (CRC Press).

Stojanovski, T., Kocarev, L. & Parlitz, U. [1996] "A simple method to reveal the parameters of the lorenz system," *Int. J. Bifurc. Chaos* **6**, 2645–2652.

Szczepanski, J., Amigo, J., Michalek, T. & Kocarev, L. [2005] "Cryptographically secure substitutions based on the approximation of mixing maps," *IEEE Trans. Circuits Syst. I* **52**, 443–453.

Tang, G., Liao, X. & Chen, Y. [2005] "A novel method for designing S-boxes based on chaotic maps," *Chaos Solitons Fractals* **23**, 413–419.

Tao, C. & Du, G. [2003] "A new approach to breaking down chaotic secure communication," *Int. J. Bifurc. Chaos* **13**, 2689–2698.

Tao, C., Du, G. & Zhang, Y. [2003] "Decoding digital information from the cascaded heterogeneous chaotic systems," *Int. J. Bifurc. Chaos* **13**, 1599–1608.

Uís, J., Ugalde, E. & Salazar, G. [1998] "A cryptosystem based on cellular automata," *Chaos* **8**, 819–822.

Vaidya, P. G. & Angadi, S. [2003] "Decoding chaotic cryptography without access to the superkey," *Chaos Solitons Fractals* **17**, 379–386.

Wang, X., Zhan, M., Lai, C.-H. & Gang, H. [2004] "Error function attack of chaos synchronization based encryption schemes," *Chaos* **14**, 128–137.

Wolfram, S. [1985] "Cryptography with cellular automata," in *Advances in Cryptology – CRYPTO'85*, *Lecture Notes in Computer Science*, vol. 218, 429–432 (Spinger-Verlag).

Wong, W.-K., Lee, L.-P. & Wong, K.-W. [2001] "A modified chaotic cryptographic method," *Comp. Phys. Comm.* **138**, 234–236.

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

Xiao, D., Liao, X. & Wong, K. [2005] "An efficient entire chaos-based scheme for deniable authentication," *Chaos Solitons Fractals* **23**, 1327–1331.

Yang, T. [1995] "Recovery of digital signals from chaotic switching," *Int. J. Circuit Theory Appl.* **23**, 611–615.

Yang, T. [2004] "A survey of chaotic secure communication systems," *Int. J. Comp. Cognition* **2**, 81–130.

Yang, T. & Chua, L. O. [1996] "Secure communication via chaotic parameter modulation," *IEEE Trans. Circuits Syst. I* **43**, 817–819.

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

Yang, T., Yang, L. B. & Yang, C. M. [1998b] "Breaking chaotic switching using generalized synchronization: Examples," *IEEE Trans. Circuits Syst. I* **45**, 1062–1067.

Yang, T., Yang, L. B. & Yang, C. M. [1998c] "Cryptanalyzing chaotic secure communications using return maps," *Phys. Lett. A* **245**, 495–510.

Zhou, C. & Lai, C.-H. [1999] "Decoding information by following parameter modulation with parameter adaptive control," *Phys. Rev. E* **59**, 6629–6636.

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

Zhou, H. & Ling, X. [1997a] "Generating chaotic secure sequences with desired statistical properties and high security," *Int. J. Bifurc. Chaos* **7**, 205–213.

Zhou, H. & Ling, X. [1997b] "Problems with the chaotic inverse system encryption approach," *IEEE Trans. Circuits Syst. I* **44**, 268–271.

Zhou, L.-H. & Feng, Z.-J. [2000] "A new idea of using one-dimensional PWL map in digital secure communications–dual-resolution approach," *IEEE Trans. Circuits Syst. II* **47**, 1107–1111.