Chapter 8
Lessons learnt from the cryptanalysis of chaos-based ciphers*

Gonzalo Alvarez[1], José María Amigó[2], David Arroyo[3], Shujun Li[4]

8.1 Introduction

The idea of using chaotic transformations in cryptography is explicit in the foundational papers of Shannon on secrecy systems (e.g., [96]). Although the word "chaos" was not minted till the 1970s [71], Shannon clearly refers to this very concept when he proposes the construction of secure ciphers by means of measure-preserving, mixing maps which depend 'sensitively' on their parameters. The implementation of Shannon's intuitions had to wait till the development of Chaos Theory in the 1980s. Indeed, it was around 1990 when the first chaos-based ciphers were proposed (e.g., [78], [46]). Moreover, in 1990 chaos synchronization [91] entered the scene and shortly thereafter, the first applications to secure communications followed [56, 37]. The idea is remarkably simple: mask the message with a chaotic signal and use synchronization at the receiver to filter out the chaotic signal. The realization though had to overcome the desynchronization induced by the message itself. After this initial stage, the number of proposals which exploited the properties of chaotic maps for cryptographical purposes, grew in a spectacular way.

[1]Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas
Serrano 144, 28006 Madrid, Spain
[2]Centro de Investigación Operativa, Universidad Miguel Hernández
[3]Instituto de Acústica, Consejo Superior de Investigaciones Científicas
Serrano 144, 28006 Madrid, Spain
Avda. de la Universidad s/n. 03202 Elche (Alicante) Spain
[4]Fachbereich Informatik und Informationswissenschaft, Universität Konstanz
Universitätsstrasse 10, 78457 Konstanz, Germany

* This is the authors' preprint of a book chapter published in *Chaos-Based Cryptography: Theory, Algorithms and Applications*, edited by Ljupco Kocarev and Shiguo Lian, *Studies in Computational Intelligence*, vol. 354, pp. 257-295, Springer-Verlag GmbH, 2011. The original publication is available at `www.springerlink.com`.

As any topic developed in a rush tempo, chaos-based (or 'chaotic') cryptography has suffered, and to a minor extent it is still suffering from annoying shortcomings. Some of them even breach basic principles of cryptography but, alas, persist in the publications after the many years and the many warnings [6, 15, 17]. In this chapter we are going through the most common errors and bad practices that have been marring chaos-based cryptography. Formulated in a positive way, we shall highlight a number of principles and practices that should be prior to any serious proposal in this field. These general principles may be classified in four groups.

- Design aspects (e.g., specification of the key space, existence of weak keys, etc.)
- Dynamic-theoretical aspects (e.g., use of maps with robust chaos, etc.)
- Computational aspects (e.g., computational efficiency, study of numerical degradation, etc.)
- Security-related aspects (i.e., whether a cipher is resistant to known attacks, etc.)

Needless to say, resistance of a new cipher against known attacks is no guarantee of security, but it is obviously a necessary condition; the same applies to the various statistical tests for pseudo-randomness. The security of each cipher has to be discussed on a case-by-case basis and it depends very much on its specifics. Contrarily to the commonplace in chaotic cryptography that the more "messy" the encryption process, the more secure the resulting cipher, the security of a cipher should rely on general principles, well-tested architectures and efficient implementations. This is the aim of this work, i.e., to emphasize the main problems of recent chaos-based cryptosystems in order to establish a methodology to avoid them. Although it is not possible to conclude the unconditional security of an encryption system, we can asses its practical security by means of common tools and practices in the cryptanalysis of chaotic cryptography. Furthermore, this analysis can be used to define the requirements of chaotic cryptography from a theoretical point of view. In particular, we shall advocate below for a chaos-based cryptography on integer numbers or, more generally, finite fields as a general framework where chaos-based cryptography can merge with conventional cryptography while preserving its identity.

This paper is organized as follows. The first section deals with the main problems of chaos-based cryptography, which are the conclusion of our work in the field of the cryptanalysis of chaotic cryptosystems. As a result of the study of those problems, in the second section we introduce a set of rules to avoid them and to design *secure* chaotic cryptosystems (by means of the critical contexts drawn through the discussion in the first section). The coherence between chaos-based cryptography and conventional cryptography requires to go into a common theoretical background, which is the core of the last two sections. Once the fundamental limitations of naive chaotic cryptography have been recognized, one can take a practical approach and try

to make the most of it. After all, the properties of the numerical (actually, periodical) orbits of chaotic maps can be good enough in practice; as a matter of fact, this has been the general approach till now. This being the case, the last section concludes our paper by proposing the theoretical aspects of chaos-based cryptography. In particular, we go into the question of how chaos-based cryptography can be understood (and even defined) in the realm of finite-precision (hence, discrete) mathematics. We want to stress right away that a chaos-based (or rather 'chaos-inspired') cryptography on the integers, thus without numerical degradation, is possible and, of course, preferable to the use of real-number approximations. In fact, some examples of chaos-based ciphers on integer numbers are mentioned in Sec. 2 and 3 —this is the approach we recommend.

8.2 Main problems in chaos-based cryptography

The number of chaos-based ciphers proposed in the literature is too large for us to attempt here a review of them. The interested reader is referred to [17] for a brief but sufficient overview. Rather than discussing this or that implementation of chaos-based cryptography, we will only delve into the basic ideas that unify all of them.

Roughly speaking, there are two classes of chaotic cryptosystems. The first one is based on chaotic systems implemented in digital (i.e., discrete-time and discrete-space) domain. This type of chaos-based ciphers are usually known as digital chaos-based cryptosystems or digital chaotic ciphers. One typical type of digital chaotic ciphers amounts to numerically computing a great number of iterations of a discrete chaotic system, using the message and/or the key as initial data (see [46, 43] and references therein). This is basically also the strategy in [18], [102], where periodic approximations of chaotic automorphisms are used to define substitutions (so-called S-boxes) resistant to linear and differential cryptanalysis. The ciphers which exploit the ergodicity of chaotic maps, like the one originally proposed in [31] and its posterior improvements, may be thought in this class as well. There are also some ciphers built on top of chaos-based pseudo-random number generators (PRNGs) like those proposed in [70, 19].

The second class amounts to scrambling a message via a chaotic system evolving in continuous-space (but maybe discrete-time) domain. Analog cryptosystems based on chaos synchronization belong to this second class. Various cryptosystems of this class, corresponding to distinct ways of hiding a message, have drawn the attention of researchers over the years. The most important schemes following such a principle are additive masking, chaotic switching, parameter modulation, and message-embedding (a.k.a. direct modulation). Additive masking was first suggested in [56], [37] and [109]. Chaotic switching is also referred to as chaos shift keying (CSK). A description with

deep insights can be found in [61], even though the idea of CSK was proposed a couple of years before [38]. Essentially, chaotic switching is a special type of chaotic parameter modulation: binary modulation. As a generalization of chaotic switching, the parameter involved in a parameter modulation system can be both discrete [89, 38] or continuous [42, 51], rather than only 0 or 1 in chaotic switching. The message-embedding technique is given different names in the literature: embedding [72, 82], non autonomous modulation [112] or direct chaotic modulation [47]. A slight different method based on message-embedding is the hybrid message-embedding. It was first proposed in [113] but the terminology " hybrid" was actually introduced in [88]. Most analog chaos-based cryptosystems are based on a single communication channel between the sender and the receiver, which is used to transmit the driving signal and the encrypted message to achieve synchronization between the slave and master systems. Some researchers also proposed to use two communication channels to enhance security, where one channel is used for synchronization and the other is for encryption [83, 54]. In Fig. 8.1, we show the basic structures of the three analog chaos-based cryptosystems: chaotic masking, chaotic switching and chaotic modulation.

In any of the families of chaos-based cryptosystems the core of the design process is the selection of a *good* chaotic system for an encryption algorithm [55]. From a general point of view it is not possible to define chaotic cryptosystems satisfying the *chaotic-system-free property* [64]. This being the case, the selection of a certain encryption scheme demands the identification of a group of chaotic systems with a certain set of dynamical properties. Furthermore, the *hardware* implementation of the chaotic encryption algorithm must guarantee its security, but also its efficiency. According to our experience in the field of the cryptanalysis of chaos-based cryptosystems, the most critical problems in chaotic cryptography arise from three elements: the selection of a chaotic system, the choice of an encryption architecture, and the implementation of the encryption. Next those problems are listed and discussed, according to our previous works in [67, 24, 21].

8.2.1 Problems with the selection of the chaotic system

Problem 1. Definition of the key leading to non-chaotic behavior. In some chaos-based cryptosystems the control parameters (or part of it) of the underlying chaotic systems are determined by the secret key. If the link between the secret key and the control parameters is not established carefully, then it is possible that the underlying chaotic system evolves in an non-chaotic way, which further erodes the confusion and diffusion properties required by the resulting cryptosystem.

The chaotic systems used as base of cryptosystems are defined in a parametric way such that their dynamics depend on one or several control param-

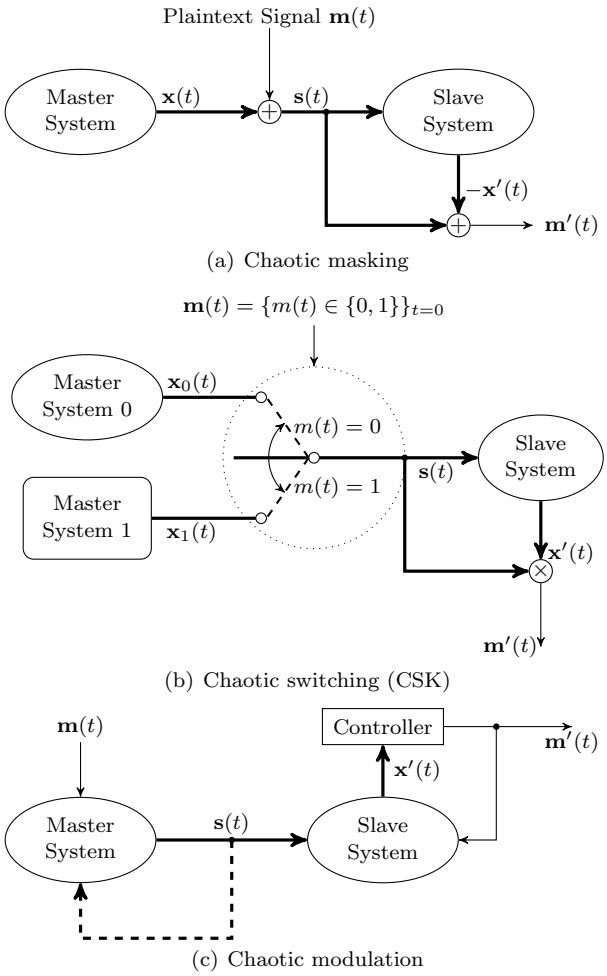

Fig. 8.1 Basic structures of the three analog cryptosystems based on chaos synchronization.

eters. Moreover, those chaotic systems are dynamical systems which show a chaotic behavior for certain values of the associated control parameters. Therefore, the design of a cryptosystem based on any of those dynamical systems must be done by guaranteeing the use of the set of values of the control parameters leading to chaos. Otherwise, the underlying dynamical system associated with the cryptosystem will not be chaotic anymore, which implies a reduction of the level of entropy in the ciphertext (i.e., the output of the cryptosystem) and also a decreasing of the influence on the ciphertext of a change in the plaintext (i.e., the input of the cryptosystem). This problem is specially relevant when the design of the cryptosystem is based on a

dynamical system with chaotic behavior only for a set of disjoint parts of the whole space of the control parameters. This is the case of the logistic map and the Hénon map, which have been used in [93, 73, 106] and in [34] respectively without a thorough analysis of their dynamics, as we have pinpointed in [29, 27, 25, 26]. As a conclusion, it is highly advisable to use dynamical systems with chaotic behavior for all the values of the control parameter(s). That is, *robust chaotic systems* [30] should be used instead of non-robust ones.

Problem 2. Nonuniform probability distribution function. In some chaos-based encryption architectures the confusion and/or diffusion properties depend on the probability distribution function of the orbits derived from the underlying chaotic systems. If that distribution is not uniform and dependent on the values of control parameters, then the quality of the diffusion process is reduced.

The iteration of a chaotic map can be used to generate pseudo-random sequences to encrypt the plaintext. The encryption procedure could be performed in different ways, but all of them demand the equiprobability of all the states contained in the pseudo-random sequences. If this requirement is not satisfied, then the conditional entropy of the ciphertext with respect to the plaintext may not be large enough so that some information will be leaked about relationships between the output and the input of the target cryptosystem (see the entropy attack in [11], and the cryptanalysis in [10]). This effect is specially significant for image encryption, as pointed out recently in [63]. As a remedy, chaotic maps with a uniform probability distribution function should be selected as base of this kind of cryptosystems, being the family of piecewise linear chaotic maps [68] a good option.

Problem 3. Return map reconstruction. The ciphertext of some cryptosystems makes it possible to reconstruct a return map of the underlying chaotic system. If such a return map is meaningful, then an attacker may be able to infer the values of the control parameters that govern the evolution of the chaotic system.

The most direct way to estimate the control parameters from a chaotic orbit is to plot x_{n+1} versus x_n, which is actually the chaotic map itself. If this representation shows a simple function between x_{n+1} and x_n, then it could be possible to infer the control parameter. In [97] a chosen-ciphertext attack is used to build a discretized version of the logistic map which further leads to the estimation of the control parameter. One solution against this kind of attack is to shuffle/truncate the chaotic orbit before using it for encryption, which randomizes the plot of the return map.

The reconstruction of the return map is specially meaningful in the context of analog chaos-based cryptography. Encryption techniques based on chaotic masking or chaotic switching can be circumvented by constructing some return maps of the master system of an analog chaotic cryptosystem [92], as it has been shown in [65, 66].

Problem 4. Low sensitivity to secret key. The most common problem (and one of the most serious ones) about analog chaos-based cryptosystems is the low sensitivity to the secret key. The low sensitivity is a necessary requirement for real implementations of any analog chaos-based cryptosystem because it is impossible to ensure exact matching of the master and slave systems. Unavoidable noise and manufactural component deviation involved in chaotic circuits are the two main factors causing this security problem [107, 116].

Problem 5. Erosion of computational efficiency due to the structural complexity of the underlying chaotic systems. The structural complexity of a chaotic system is a critical element when evaluating its suitability for cryptographic applications. With this bottom line in [21, Sec. 1.3.3] we emphasized that structural complexity can be minimized by selecting chaotic systems defined in discrete time. Indeed, in discrete time chaos can be achieved for phase space of Dimension 1, whereas it has to be at least of Dimension 3 when considering continuous time.

8.2.2 Problems with the encryption architecture

Problem 6. Part of the key should not leak the rest of the key. In some cryptosystems the secret key is composed of different subkeys. If the knowledge of some subkeys allows the recovery of the rest of the key, then a *partial key recovery attack* can be performed. Therefore, the design of a cryptosystem must guarantee that the different subkeys composing the secret key are uncorrelated.

In the context of a secure and robust encryption system it is assumed that partial knowledge of the key does not reveal information about the rest of the key and, as a result, the cryptosystem performance is not harmed [6, Rule 7]. This rule is not satisfied in the scenarios drawn by [31, 34, 20], partial knowledge of the key can be used to obtain the rest of the key [11, 26, 95].

Case study 8.2.1 ([26]) *Cryptanalysis of the cryptosystem proposed in [34]*

In [34] the Hénon map is used as the *heart* of a chaos-based cryptosystem, which entails a security problem that we have highlighted in [26]. The analytical definition of the Hénon map is:

$$x_{k+1} = \begin{bmatrix} u_{k+1} \\ v_{k+1} \end{bmatrix} = \begin{bmatrix} 1 - \delta \cdot u_k^2 + v_k \\ \beta \cdot v_k \end{bmatrix}, \tag{8.1}$$

with $\delta, \beta \in \mathbb{R}$. In the cryptosystem defined in [34] the plaintext is divided into blocks $\{p_k\}_{k=0}^{N-1}$, where each block has M bits. The encryption of the plain-blocks is carried out for $k = 0, \ldots, N-1$ in turn. For the k-th plain-block p_k,

the corresponding cipher-block is x_{k+1}, which is calculated through Eq. (8.1) by setting

$$\delta = \psi\left(p_k\right) \cdot \mu_1\left(v_k\right), \tag{8.2}$$
$$\beta = \mu_2\left(v_k\right), \tag{8.3}$$

where $\psi(x)$ is a bijective function assuring that δ is a valid parameter of Eq. (8.1) and $\mu_i(x)$, $i \in \{1, 2\}$. Based on the general form of the proposed cryptosystem, the authors of [34] present a concrete configuration: $M = 48$, $\psi(x)$, $\mu_1(x)$ and $\mu_2(x)$ are set in Eqs. (8.4), (8.5), (8.6) respectively.

$$\psi\left(x\right) = 1.77 \cdot 10^{-2} + 1.39 \cdot 10^{-15} \cdot x, \tag{8.4}$$

$$\mu_1(x) = \begin{cases} 1.27 + \frac{x}{10.2}, & \text{if } |x| \leq 0.1 + \frac{x}{1.3} \\ 1.28 + \frac{x}{10.2}, & \text{if } 0.1 + \frac{x}{1.3} < |x| \leq 0.2 + \frac{x}{1.3} \\ 1.29 + \frac{x}{10.2}, & \text{if } 0.2 + \frac{x}{1.3} < |x| \leq 0.3 + \frac{x}{1.3} \\ 1.30 + \frac{x}{10.2}, & \text{otherwise} \end{cases} \tag{8.5}$$

$$\mu_2(x) = \begin{cases} 0.29 + \frac{x}{10}, & \text{if } |x| \leq 0.1 + \frac{x}{1.1} \\ 0.30 + \frac{x}{10}, & \text{if } 0.1 + \frac{x}{1.1} < |x| \leq 0.2 + \frac{x}{1.1} \\ 0.31 + \frac{x}{10}, & \text{if } 0.2 + \frac{x}{1.1} < |x| \leq 0.3 + \frac{x}{1.1} \\ 0.32 + \frac{x}{10}, & \text{otherwise} \end{cases} \tag{8.6}$$

Next we show how a known-plaintext attack can be employed to reconstruct Eq. (8.5), Eq. (8.6), and v_0 (initial condition of the underlying Hénon map defined in Eq. (8.1)) when Eq. (8.4) is known. Given two plaintexts $\{p_{1,k}\}_{k=0}^{N-1}$, $\{p_{2,k}\}_{k=0}^{N-1}$, then

$$u_{1,1} = 1 - \psi(p_{1,0}) \cdot \mu_1(v_0) \cdot u_0^2 + v_0, \tag{8.7}$$
$$u_{2,1} = 1 - \psi(p_{2,0}) \cdot \mu_1(v_0) \cdot u_0^2 + v_0, \tag{8.8}$$

and

$$u_{1,k+1} = 1 - \psi(p_{1,k}) \cdot \mu_1(v_k) \cdot u_{1,k}^2 + v_k, \tag{8.9}$$
$$u_{2,k+1} = 1 - \psi(p_{2,k}) \cdot \mu_1(v_k) \cdot u_{2,k}^2 + v_k, \tag{8.10}$$
$$v_k = \mu_2(v_{k-1}) \cdot u_{k-1}, \tag{8.11}$$

where $k \geq 1$. Subtracting Eq. (8.9) from Eq. (8.10):

$$\widetilde{\mu}_1(v_k) = \frac{u_{2,k+1} - u_{1,k+1}}{\psi(p_{1,k}) \cdot u_{1,k}^2 - \psi(p_{2,k}) \cdot u_{2,k}^2}. \tag{8.12}$$

From Eq. (8.11):

$$\widetilde{\mu}_2(v_{k-1}) = \frac{u_{1,k+1} - 1 + \psi(p_{1,k}) \cdot \widetilde{\mu}_1(v_k) \cdot u_{1,k}^2}{u_{k-1}}. \tag{8.13}$$

If the quantization error is ignored, we have $\widetilde{\mu}_1(v_k) = \mu_1(v_k)$ and $\widetilde{\mu}_2(v_{k-1}) = \mu_2(v_{k-1})$. As a consequence, it is possible to reconstruct $\mu_1(v_k)$ and $\mu_2(v_k)$ repeating this procedure for $k = 1, \ldots, N$. In order to prove the proposed known-plaintext attack, 10000 points for $\mu_1(v_k)$ and $\mu_2(v_k)$ were calculated for $u_0 = 0.4,\ v_0 = 0.9402036$ and $u_0 = 0.4,\ v_0 = -0.5123493$. In Fig. 8.2 it is shown how it was possible to get an estimation of $\mu_1(v_k)$, $\mu_2(v_k)$ shape. This is due to the fact that the first component of the Hénon map employed in the encryption process is sent through the communication channel without applying any masking transformation.

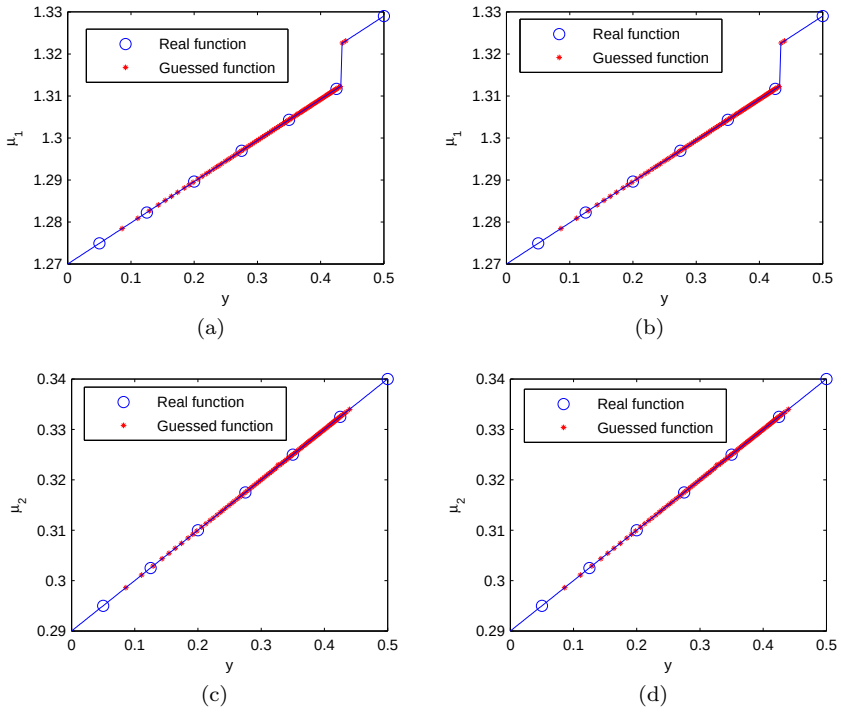

Fig. 8.2 Recovered and original functions for the PRSK mechanism when they are designed as in [34] (a) $\mu_1(v)$ for $v_0 = 0.9402036$; (b) $\mu_1(v)$ and $v_0 = -0.5123493$; (c) $\mu_2(v)$ for $v_0 = 0.9402036$; and (d) $\mu_2(v)$ and $v_0 = -0.5123493$.

Problem 7. Key estimation from the ciphertext. A bad definition of the ciphertext derived from a chaos-based cryptosystem could allow the es-

timation of the initial condition(s) and/or the control parameter(s) of the underlying chaotic system. This problem is present in some chaos-based cryptosystems whose ciphertext is given by fragments of orbits, sampled versions of the orbits, or discretized versions of the orbits of the underlying chaotic systems. Moreover, parameter estimation is a critical problem of cryptosystems based on chaotic parameter modulation, since adaptive synchronization techniques can be used to get an approximation of the control parameters of the underlying chaotic systems by minimizing the synchronization errors.

An m-dimensional discrete-time chaotic map is defined by the rule of evolution

$$x_{n+1} = f_\lambda(x_n),$$

and, as a result, the ciphertext cannot be the orbits of the map since it may allow the estimation of λ from $m + 1$ or a bit more consecutive units of ciphertext. This is the case of the cryptosystem proposed in [73], and which we have cryptanalyzed in [27].

Furthermore, if the invariant set of the chaotic map has a size dependent on the control parameters, even sampled versions of the orbits may allow the estimation of the control parameters through a ciphertext-only attack [10]. We have analyzed this situation in [29] for the cryptosystem proposed in [93]. In addition, the theory of symbolic dynamics may also reveal the weakness of a cryptosystem if the ciphertext allows getting the symbolic sequences of the underlying chaotic system. In [25] we have shown through a chosen-ciphertext attack how to derive the symbolic sequence of the logistic map driving the encryption procedure defined in [106]. Once we have the symbolic sequence, we can infer the values of the control parameter and initial condition of the underlying logistic map according to the theory of applied symbolic dynamics described in [3]. Nevertheless, a constant size for the invariant set of a chaotic map is a necessary but not sufficient condition to avoid the estimation of the control parameter from the corresponding orbits. In this respect, and according to [22], chaotic orbits should be analyzed also by means of their associated order patterns. Finally, another critical context is depicted when measures of statistical distance can be applied to distinguish between keystreams, as we have shown in [23].

For most analog chaos-based secure communication systems, the ciphertext is not very sensitive to the secret key, which is caused by a simple relationship between synchronization error and key mismatch: the larger the key mismatch is, the larger the synchronization error will be, and vice versa. This means that an iterative algorithm can be used to determine the value of the secret parameters, which corresponds to the concept of adaptive synchronization. A lot of work has been reported about adaptive synchronization when the master systems' parameters are unknown to the receiver/attacker. Some of the work can directly be used or easily extended to break analog chaos-based secure communication systems [39, 103, 104]. In addition to methods based on adaptive synchronization, there are also other ways one can use to

estimate the secret parameters (i.e., the key) of chaos-based cryptosystems. For instance, due to the nature of Lorenz and Chua Chaotic Systems, the secret parameters can be determined from the driving signal and its derivatives (mainly differentials of different orders) [32, 105, 74]. For some specific schemes, it is also possible to derive part of the secret parameters by analyzing the return maps of the master systems [65]. When chosen-ciphertext attacks are possible, i.e., when the attacker can access the decryption machine for some time, the attacker may set the driving signal to a fixed constant C in order to get the values of all secret parameters [50].

Case study 8.2.2 ([27]) *Cryptanalysis of the cryptosystem described in [73]*

In [73] the encryption procedure is carried out by decomposing the input plaintext signal into two different subbands and masking each of them with a pseudo-random number sequence generated by iterating the chaotic logistic map. The decomposition of the input plaintext signal x_n is driven by

$$t_n = K \sum_{\forall j} x_j h_{2n-j}, \tag{8.14}$$

$$t'_n = K' \sum_{\forall j} x_j h'_{2n-j}. \tag{8.15}$$

Then, the masking stage generates the ciphertext signal (v_n, v'_n) according to the following equations:

$$v_n = t_n + \alpha(t'_n), \tag{8.16}$$

$$v'_n = t'_n - \alpha'(v_n), \tag{8.17}$$

where $\alpha(u) = u + s_n$ ($\alpha'(u) = u + s'_n$) and s_n (s'_n) is the state variable of the logistic map.

The secret key of the cryptosystem is composed of the initial conditions and the control parameters of the two logistic maps involved, i.e., s_0, s'_1, λ and λ'.

In a known-plaintext attack the cryptanalyst possesses a plaintext signal $\{x_n\}$ and its corresponding encrypted subband signals $\{v_n\}$ and $\{v'_n\}$. Because $\{h_n\}$, $\{h'_n\}$, K and K' are public, we can get $\{t_n\}$ and $\{t'_n\}$ from $\{x_n\}$. Then we can get the values of $\{s_n\}$ and $\{s'_n\}$ as follows:

$$s_n = v_n - t_n - t'_n, \tag{8.18}$$

$$s'_n = t'_n - v_n - v'_n. \tag{8.19}$$

For $n = 0$, the values of the subkeys s_0 and s'_0 have been obtained. Furthermore, we can obtain the control parameters by just doing the following operations:

$$\lambda = \frac{s_{n+1}}{s_n(1-s_n)},$$
$$\lambda' = \frac{s'_{n+1}}{s'_n(1-s'_n)}.$$

Problem 8. Direct extraction of plaintext. In the context of analog chaos-based cryptography, in some cases it is feasible to infer the plaintext message signals from the driving signals without estimating the secret key or the carrier signals. Techniques such as power-spectral filtering (or power energy analysis) and return map analysis have been used for this purpose.

Regarding power-spectral filtering, even when the power spectra of some chaotic systems seem to be good, significant spectrum peaks can be found in the spectra by removing the symmetries of the chaotic attractors [62, 86, 85]. For instance, the spectrum of $x(t)$ in the Lorenz System is relatively good, but that of $|x(t)|$ has a significant peak. When the plaintext message signal is hidden in the driving signal, the narrow-band spectrum means that the driving signal may be directly filtered to recover the message signal [114, 8]. On the other hand, for some parameter modulation systems the power energy of the driving signal varies according to the value of the transmitted signal. This makes it possible to obtain a smoother version of the message signal by observing the average power energy of the driving signal in a sliding time-window [12]. Exact recovery of the plain message signal is possible for chaotic switching systems, because each bit has to be held for a considerably long time to ensure that chaos synchronization is established.

In addition to power filtering, cryptanalysts have figured out some other techniques that can be used to extract the plaintext directly from the ciphertext, which include generalized synchronization, short-time period analysis and switching event detection. For chaotic switching systems and some parameter modulation systems, there is a simple relationship between the synchronization error and the value of the transmitted signal. This link can be interpreted as a way to extract the plaintext message signal directly [8, 115]. With respect to the study of short-time period, if the spectrum of the driving signal (or some modification of it) involved has a significant peak, generally there exists a simple relationship between the peak frequency and the values of the control parameters. In this case, one can try to extract the short-time period as a measurement of the peak frequency modulated by the plaintext message signal. According to the change of the extracted short-time periods, the plaintext message signal can be extracted exactly (for chaotic switching systems) or approximately (for some parameter modulation systems) [111, 4]. Finally, for chaotic switching and parameter modulation systems the dynamics of the master systems will change significantly when the value of the modulating signal (i.e., the plaintext message signal) changes. By detecting and tracking these switching events, it may be possible to recover the modulating signal [101].

Case study 8.2.3 ([4]) *Short-time period analysis based cryptanalysis of a cryptosystem proposed in [40]*

In [40], the author proposes a symmetric secure communication system based on parameter modulation of a chaotic oscillator acting as a transmitter. The receiver is a chaotic system synchronized by means of an adaptive observer. Two sample implementations are given: one with the Lorenz attractor and another with Chua's attractor. In this case study the latter will be broken, to illustrate how our method works with a different double-scroll attractor. It works equally well for Lorenz attractor, though.

Chua's circuit dynamics can be described by the following equations:

$$\begin{aligned} \dot{x}_1 &= \alpha(-x_1 + x_2) - f_1(x_1), \\ \dot{x}_2 &= x_1 - x_2 + x_3, \\ \dot{x}_3 &= -\beta x_2. \end{aligned} \tag{8.20}$$

where $f_1(x) = bx + 0.5(a-b)(|x+1| - |x-1|)$. In the example the system is implemented with the following parameter values, $(\alpha, \beta, a, b) = (10, 18, -4/3, -3/4)$. The encryption process is defined by modulating the parameter β with the binary encoded plaintext, so that it is $\beta + 1.25$ if the plaintext bit is "1" and $\beta - 1.25$ if the plaintext bit is "0". The duration of the plaintext bits must be much larger than the convergence time of the adaption law. The uncertain system can be rewritten in a compact form as:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -10 & 10 & 0 \\ 1 & -1 & 1 \\ 0 & \beta & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{pmatrix} f_1(x_1) \\ 0 \\ 0 \end{pmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} x_2\theta, \tag{8.21}$$

$$y = C \cdot x = x_3, \tag{8.22}$$

$$C = [0\ 0\ 1], \tag{8.23}$$

$$\theta = \Delta\beta = \pm 1.25. \tag{8.24}$$

To launch an attack based on short-time period analysis, we first transform $x_3(t)$ to $|x_3(t)|$, which has a significant peak in the frequency domain and thus a short-time periodicity linked to the plaintext bits. The short-time period of $|x_3(t)|$ can be measured as the distance between adjacent cross-zero points (or from the dominant frequency peak in the short-time FFT domain). The resultant signal is denoted by $p(t)$. Then, $p(t)$ is filtered by removing singular peaks and DC component to get $p^*(t)$. Next, an averaging filter is used to get a smoother signal $fp^*(t)$. Finally, this smoother signal is binarized to recover the plaintext signal. The signals involved in the process are shown in Fig. 8.3.

Problem 9. Efficiency of the cryptosystem depending on the value of the key. If the encryption and decryption times depend on the key or a subkey, then a timing attack can be performed to estimate the (sub)key.

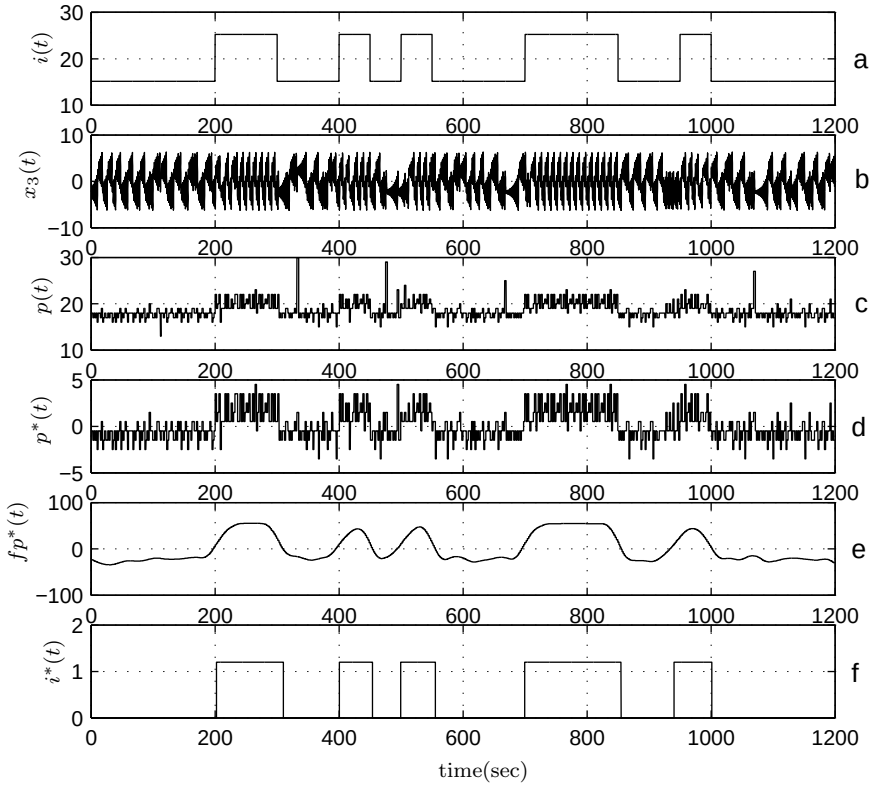

Fig. 8.3 Breaking a cryptosystem based on Chua's circuit: a) original binary information signal, $i(t)$; b) the transmitted state variable signal or ciphertext, $x_3(t)$; c) the short-time period signal, $p(t)$; d) the clipped signal, $p^*(t)$, after removing singular peaks and DC component; e) the low-pass filtered signal, $fp^*(t)$, revealing the modulation signal; f) recovered message signal, $i^*(t)$, after adequate detection.

Some encryption architectures perform the transformation of the plaintext into the ciphertext through several encryption rounds. Additionally, in each encryption round a chaotic map is iterated n times. Since the encryption and decryption times have to be constant and independent of the value of the key, it is not a good practice to select the number of encryption rounds and n as part of the key. Otherwise, a timing attack [60, 33] based on the analysis of the encryption and decryption time can be used for the partial estimation of the secret key, which is a serious security flaw.

Case study 8.2.4 ([29]) *Timing attack on a cryptosystem proposed in [93]*

Let us exemplified a timing attack by recalling the cryptosystem proposed in [93]. In every encryption round of the cryptosystem under consideration, the logistic map is iterated n times, where n is a subkey. This means that, for

a certain number of encryption rounds (j) and a certain value of the control parameter λ, the encryption speed decreases as n increases. Similarly, because the encryption/decryption procedure is composed of j repeated cycles, the encryption speed will also become slower if the value of j increases. To be more precise, for a given plain-image, we can expect the existence of the following bi-linear relationship between the encryption/decryption time (EDT) and the values of n and j:

$$EDT(n, j) \approx (c \times n + d_0) \times j + d_1, \tag{8.25}$$

where c corresponds to the common operations consumed on each chaotic iteration, d_0 to the operations performed in each cycle excluding those about chaotic iterations, and d_1 to those operations performed on the initialization process and the postprocessing after all the j cycles are completed. In addition, because λ is just the control parameter of the chaotic map, it is expected that EDT will be independent of its value.

With the aim of verifying this hypothesis, some experiments have been made under the following scenario. An image with random pixel values of size 256×256 was encrypted for different values of λ, n and j. The encryption time corresponding to each key is shown in Fig. 8.4, from which one can see that Eq. (8.25) is verified.

The above experimental results ensure the feasibility of a timing attack to a subkey of the cryptosystem under study: by observing the encryption time, it is possible to estimate the value of n if j is known and vice versa. Without loss of generality, assuming an attacker Eve knows the value of n, but not that of j, let us demonstrate how the timing attack can be performed in practice. In this case, the relationship between EDT and the value of j can be simplified as $EDT(n, j) = c_n \times j + d_n$, where $c_n = c \times n$ and $d_n = d_0 \times j + d_1$. Then, if Eve gets a temporary access to the encryption (or decryption) machine, she can carry out a real timing attack in the following steps:

1. She observes the whole process of encryption (or decryption) to get the encryption (or decryption) time t_j and also the size of the ciphertext (i.e., the size of the plaintext).
2. By choosing two keys with different values of j, she encrypts[2] a plaintext (or decrypts a ciphertext) of the same size and gets t_1 and t_2.
3. She derives the values of c_n and d_n by substituting t_1 and t_2 into $EDT(n, j) = c_n \times j + d_n$.
4. She estimates the value of j to be $\hat{j} = \text{round}((t_j - d_n)/c_n)$.
5. She verifies the estimated value $\hat{j}$ by using it to decrypt the observed ciphertext. If the recovered plaintext is something meaningful, the attack stops; otherwise, she turns to search the correct value of j in a small neighborhood of $\hat{j}$ until a meaningful plaintext is obtained.

[2] Please note that this can be done on her own computer, as long as she has the encryption/decryption software installed.

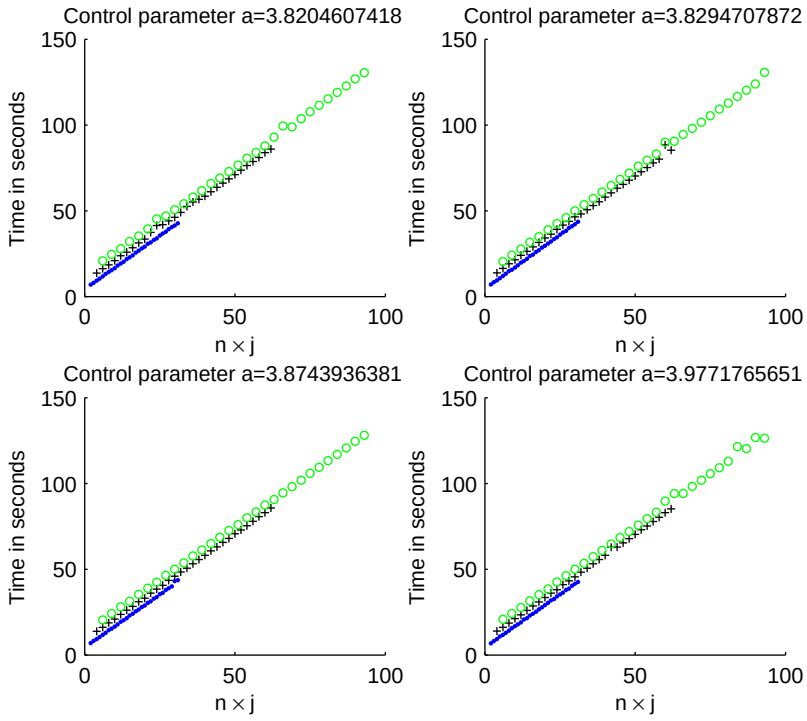

Fig. 8.4 Encryption time for images of size 256×256 and different values of the number of iterations n and the number of encryption rounds.

As a result of the previous analysis, the number of encryption rounds and the number of iterations of the map should be public parameters of the chaos-based cryptosystem instead of part of the key.

Problem 10. Faulty derivation of the parameters of the chaotic system from the key. In some chaos-based cryptosystems the key is used to derive the values of the parameters necessary to iterate a chaotic system and finally encrypt the information. If this mapping implies a reduction of the key space, i.e., that it is only used a subset of the possible values of those parameters, then a brute-force attack on the values of the parameter could be much less demanding than an attack on the secret key.

One important step in the design of a chaos-based cryptosystem is to decide what the key is. One possibility is to use the control parameters and the initial conditions of the underlying chaotic systems as the secret key or as part of the secret key. Another option is to establish the values of the control parameters and the initial conditions of the maps from the secret key through a certain function. In this sense, it must be assured that the image set of that

function is the whole set of possible values of the control parameters and the initial conditions. Otherwise, a brute-force attack can be performed on the reduced space of control parameters and initial condition values with a lower computational cost than the one on the key space. A cryptosystem with this problem was introduced in [87] and was later cryptanalyzed in [9].

Problem 11. Encryption procedure equivalent to a map dependent only on the key. If the transformation of the plaintext into the ciphertext is determined by a procedure equivalent to a map only dependent on the key, then known/chosen-plaintext attacks may be performed to reconstruct the transformation procedure.

In some encryption schemes the transformation of the plaintext into the ciphertext is led either by a procedure derived using only the key, or by a sampling process on a sequence of values generated using only the key. In those situations, it could be possible to estimate either the key or to make up some function somehow equivalent to the encryption procedure. For example, if the encryption procedure consists of searching plaintexts in pseudo-random sequences generated by iterating a chaotic map, since the pseudo-random sequence remains unchanged unless the key is modified, then it is possible to reconstruct the pseudo-random sequence through a chosen-plaintext attack (see [14, 13]). This problem also exists in those schemes where the encryption procedure consists of a permutation-only stage which is fixed unless the control parameters and initial conditions change, i.e., unless the the secret key is updated. In order to clarify this matter, let us consider again the cryptosystem defined in [44].

Case study 8.2.5 ([28]) *Cryptanalysis of the cryptosystem defined in [44]*

As mentioned above, the cryptosystem under consideration consists of two stages: a shuffling stage and a masking stage. Assuming that the size of the plain-image $\mathbf{I}$ is $M \times N$ and the cipher-image is $\mathbf{I}'$, the encryption scheme proposed in [44] can be described by the following two procedures.

- *Shuffling procedure*
  In this procedure, the plain-image $\mathbf{I}$ is permuted to form an intermediate image $\mathbf{I}^*$ according to a total shuffling matrix $\mathbf{P}^*$, which is derived by pseudo-randomly permuting the rows and columns of the original position matrix $\mathbf{P} = [(i, j)]$. The pseudo-random row and column permutations are generated by iterating the logistic map with $\lambda = 4$ from a given initial condition x_0.
- *Masking procedure*
  In this procedure, the intermediate image $\mathbf{I}^*$ is further masked by a keystream $\{B(i)\}_{i=1}^{MN}$ as follows: $\forall i = 1 \sim MN$, $I'(i) = I^*(i) \oplus B(i) \oplus I'(i-1)$, where $I(i)$, $I'(i)$ denote the i-th pixels of $\mathbf{I}^*$ and $\mathbf{I}'$ (counted from left to right and from top to bottom), respectively, and $I'(0) = 128$.

The keystream $\{B(i)\}_{i=1}^{MN}$ is generated by iterating Lorenz [75] and Chen [35] Systems and doing some postprocessing on all the variables of state. When a variation of stream cipher is created, as in the case under study, obtaining the keystream is totally equivalent to obtaining the key whenever different plain-images are encrypted using the same key. Upon this hint, in [28] we have carried out a chosen-plaintext attack to recover both the keystream and the shuffling matrix of the cryptosystem described in [44]. Let us choose a plain-image $\mathbf{I}_1$ such that $\forall i, j = 1 \sim MN$, $I_1(i) = I_1(j) = \theta$. In this case, the shuffling part does not work, so we have $\mathbf{I}_1^* = \mathbf{I}_1$. Then, we can recover the keystream as follows: $\forall i = 1 \sim MN$, $B(i) = I_1(i) \oplus I_1'(i) \oplus I_1'(i-1)$. After removing the masking part, we can try to recover the shuffling matrix. According to the general cryptanalysis on permutation-only ciphers in [69], only $\lceil \log_{256}(MN) \rceil$ chosen plain-images are needed to recover the shuffling matrix $\mathbf{P}^*$. In total we need $\lceil \log_{256}(MN) \rceil + 1$ chosen plain-images to perform this chosen-plaintext attack.

As a conclusion, the encryption function that transforms a unit of plaintext into a unit of ciphertext should depend on the key and on the whole plaintext.

(a) (b) (c)

Fig. 8.5 Illustration of the low sensitivity to the change of the plain-image: (a) the first plain-image $\mathbf{I}_0$; (b) the second plain-image $\mathbf{I}_1$ (only the center pixel is different from $\mathbf{I}_0$); (c) the differential cipher-image $\mathbf{I}_0' \oplus \mathbf{I}_1'$.

Problem 12. Low sensitivity to the change of plaintext. In some encryption architectures plaintexts with slightest differences are associated to very similar ciphertexts, which is a clear violation of the diffusion property.

This problem is specially relevant when considering the encryption of images. This being the case, the encryption scheme must guarantee that two images differing in just one pixel determine two totally different cipher-images. This requirement is not satisfied if encryption is performed through just one encryption round, as it occurs with the cryptosystem proposed in [44] (Case study 8.2.5). For that cryptosystem, given two plain-images $\mathbf{I}_0$ and $\mathbf{I}_1$ with only one pixel difference at the position (i, j), the difference will be permuted

to a new position (i^*, j^*) according to the shuffling matrix $\mathbf{P}^*$. Then, because all plain-pixels before (i^*, j^*) are identical for the two plain-images, the ciphertexts will also be identical. This shows the low sensitivity of the image encryption scheme to changes in the plain-image. Figure 8.5 gives an example of this problem. It can be seen how the differential cipher-image is equal to zero for any pixel before (i^*, j^*) and equal to a constant value after that position.

8.2.3 Implementation problems

Problem 13. Degradation of the efficiency of digital chaos-based cryptosystems based on chaotic systems. In digital chaos-based cryptography the encryption procedure is performed in discrete time and discrete space. Therefore, if the underlying chaotic system is defined in continuous domain, then it is necessary to apply some numerical methods to obtain the chaotic orbits. The application of these numerical methods increases the time to compute the orbits, and thus reduces the encryption efficiency.

The rule of evolution of continuous-time chaotic systems requires to solve a system of differential equations [49, p. 160]. From a general point of view, the solution of those differential equations cannot be accomplished analytically, and thus numerical methods must be applied. Numerical methods for the resolution of differential equations are highly time consuming. As a result, for a given encryption architecture with the underlying chaotic system defined in continuous-time, the encryption time is greater than the encryption time obtained when the chosen dynamical system is a chaotic map.

Case study 8.2.6 ([28]) *Evaluation of the encryption time of the chaos-based cryptosystem proposed in [44].*

For the sake of argument, let us recall our cryptanalytic work [28] on the chaos-based cryptosystem proposed in [44]. This cryptosystem is intended to encrypt images through the concatenation of a shuffling and masking procedures. The shuffling procedure is based on the iteration of the logistic map, whereas masking is built upon the iteration of two continuous-time chaotic systems: Lorenz [75] and Chen Systems [35]. The Lorenz System is given by

$$\begin{aligned} \frac{dx_1}{dt} &= \alpha x_1 + \alpha x_2, \\ \frac{dx_2}{dt} &= -x_1 x_3 + \beta x_1 - x_2, \\ \frac{dx_3}{dt} &= x_1 x_2 - \rho x_3, \end{aligned} \tag{8.26}$$

where α, β, and ρ are control parameters. The Lorenz system is chaotic for a set of parameters $\alpha = 10$, $\beta = 28$, and $\rho = 8/3$. On the other hand, the

Chen System is defined as

$$\begin{aligned}\frac{dx_1}{dt} &= \eta(x_2 - x_1),\\ \frac{dx_2}{dt} &= (\sigma - \eta)x_1 - x_1x_3 + \sigma x_2,\\ \frac{dx_3}{dt} &= x_1x_2 - \delta x_3,\end{aligned} \tag{8.27}$$

being chaotic for a different set of parameters such as $\eta = 35$, $\sigma = 28$, and $\delta = 3$. Because the chaotic iterations of Lorenz and Chen Systems involve complicated numerical differential functions, the encryption speed is expected to be very slow compared with other traditional ciphers. To asses this fact, we derived a modified encryption scheme from the original one by replacing Lorenz and Chen Systems with the logistic map, and then compared the encryption speeds of the two cryptosystems. Both cryptosystems were implemented using MATLAB on a PC with a 1.6 GHz processor and 512 MB of RAM. For images of size 256×256, the typical encryption time for the original cryptosystem in [44] was around 5.8 s, while the modified cryptosystem based on the logistic map required on average around 1.2 s to encrypt an image. The experiments have clearly shown that using continuous chaotic systems can drastically reduce the encryption speed. Since there are also no other obvious merits in using continuous chaotic systems rather than a simple discrete-time chaotic map, the use of Lorenz and Chen Systems in the image encryption scheme under study is unnecessary. Instead, these continuous-time chaotic systems can be replaced by a simpler discrete-time chaotic map without compromising the security. This statement is a general rule when designing encryption procedures working in discrete time.

Problem 14. Non-invertible encryption procedure. The iteration of the chaotic systems sustaining chaos-based cryptosystems implies working with real numbers. Since the implementation of chaos-based cryptosystems is done with finite precision arithmetic, round-off operations could lead to a non-invertible encryption procedure.

One critical point when working with dynamical systems and the analysis of their dynamics is the selection of a proper simulation framework. Indeed, the computer-based analysis of dynamical systems could lead to some conclusions different from those expected from theory. This divergence also influences and conditions chaos-based cryptosystems, as pointed out in [76] for the case of CSK. Thus, if the characteristics and problems of finite-precision are not handled properly, then it is possible that the orbits generated as base of the encryption procedure can not be regenerated exactly during the decryption stage and, consequently, the original plaintext can not be recovered even when the key is known. This problem is not only relevant for fixed-point arithmetic but also for floating-point one. Indeed, the round-off quantization

errors could lead to the occurrence of a non-invertible function for encryption and, as a result, the decryption process will be impossible.

Case study 8.2.7 ([29, 26, 7]) *Non-invertible cryptosystems defined in [93, 34, 94].*

The cryptosystems introduced in [93, 34, 94] are examples of the consequences of not handling conveniently the limitations of finite precision arithmetics, as we have pinpointed in [29, 26, 7]. To clarify the problem under consideration, let us recall the scope depicted in [93], whose goal is to encrypt images. The cryptosystem described in [93] generates a ciphertext consisting of a number of real values. Encryption is performed through j encryption rounds, being $\{x_c^i(r)\}_{i=1}^J$ (c = R, G and B, $r \in \{1, 2, \ldots, j-1\}$) the output in the r-th encryption round corresponding to color component c of the i-th pixel of the image of length $J = M \times N$. All the operations to encrypt an image in [93] are performed using floating-point arithmetic. The output of the r-th round is given as $x_c^i(r) = x_n + x_c^i(r-1)$, where x_n is the resulting value of iterating the logistic map n times from x_0. Hence, if during the decryption process we want to recover $x_c^i(r-1)$ (the original value of the i-th element in the last round), we have to iterate n times the logistic map from x_0 to get x_n and, after that, to substract this value from $x_c^i(r)$. However, the resulting value of this previous operation might not match the actual value of $x_c^i(r-1)$, due to the *wobbling precision problem* that exists when dealing with floating-point operations [48, p. 39]. This wobbling precision problem also causes the resulting guessed value of $x_c^i(r-1)$ to depend on the cryptosystem implementation. Therefore, if an image is encrypted on one platform and decrypted on another, and the implementations of floating-point arithmetics on both platforms are not compatible with each other, then the decrypted image might not match the original one. In [93] the cryptosystem was implemented using Microsoft Visual C# .NET 2005 and no comment was given about the wobbling precision problem in the decryption process. However, we have experimentally verified that this problem indeed exists when the cryptosystem is implemented using MATLAB on a PC with a 3 GHz processor and 2 GB RAM. A very useful measure of the performance of the decryption procedure is the Mean Square Error or MSE. For P and P' being a plain image and the decrypted image respectively, the MSE for the color component c is defined as

$$MSE_c = \sum_{i=1}^{m} (P_c^i - {P'}_c^i)^2 / J, \tag{8.28}$$

where $c \in \{R, G, B\}$, $J = M \times N$ is the number of pixels of the images considered and the sequences $\left\{P_c^i\right\}_{i=1}^J$ and $\{P_c'\}_{i=1}^J$ are the result of scanning P and P' in the raster order. Consequently, for a well designed encryption/decryption scheme the MSE should be 0 for each color component. Unfortunately, for the cryptosystem under study, the values of MSE for all three color components are generally not equal to 0 due to the wob-

bling precision problem associated to the floating-point arithmetic. In order to evaluate the underlying decryption error of the cryptosystem defined in [93], a 512×512 plain-image "Lena" was encrypted and decrypted using the same key $(n, j, \lambda) = (30, 1, 3.9)$. The results showed that the three MSEs obtained for the red, green and blue components of the decrypted image with respect to the original one were 6.49, 0.018, 0.057, respectively. For another key $(n, j, \lambda) = (30, 3, 3.9)$, the obtained MSEs were 206.96, 123.45, 58.65, respectively. Figure 8.6 shows the decrypted image and the error image when the cryptosystem was implemented in MATLAB using a third key $(n, j, \lambda) = (5, 2, 3.9)$.

Fig. 8.6 Simulations with MATLAB (a) Ciphertext of the plain-image "Lena" (b) Recovered image of "Lena" using the same key (c) The error image between the original and the recovered "Lena".

Problem 15. Dynamical degradation. The implementation of chaotic systems in finite precision in digital computers leads often to dynamical properties completely different from the theoretical and expected ones. If this deviation is not considered during the design of chaos-based cryptosystems, it could imply a reduction of the performance and even a compromise of the security of the resulting cryptosystem.

This problem is closely related to the previous one, although the point of interest moves to degradation of dynamical properties of the implemented chaotic system with respect to the theoretical model. Consequently, the design of an encryption scheme using a chaotic system must be done by considering its practical implementation (not only the theoretical model). In [5] some consequences of the dynamical degradation of a chaotic map are shown in the context of cryptography, whereas in [68] one can find a thorough analysis of the dynamical degradation of a specific chaotic map and some ways to overcome this problem.

Problem 16. Lack of details in the description. According to Kerckhoffs' principle [80, p. 14], the security of a cryptosystem can not be based on the secrecy of its encryption and decryption procedures. In other words,

when dealing with the security of cryptosystems, everything is known except the key. Furthermore, the key of any cryptosystem has to be easy to establish and to exchange, and the key space must be defined in an explicit and clear way.

The consecution of security through obscurity is something to avoid when designing an encryption scheme. All the operations involved in the encryption/decryption procedures must be unmistakably explained, and the secret key must be clearly specified along with an exact estimation of the size of the key space. The security of the cryptosystem must be only related to the difficulty of recovering the key, and it can not depend on the lack of knowledge about the inner operation of the encryption and decryption procedures. Moreover, this lack of details implies a lack of security because without a careful investigation by the cryptography community, many security holes might not be able to be distinguished by the designers themselves.

Case study 8.2.8 ([26, 28]) *Non-exhaustive definition of the encryption and decryption scheme implying loss of chaoticity or randomness of keystreams [34, 44].*

In [21, Sec. 2.2] we have analyzed the loss of chaoticity in the cryptosystem defined in [34]. Indeed, in that cryptosystem part of the key is given by a set of functions changing the values of the control parameters of a Hénon map as the plaintext is encrypted. The authors of [34] do not define explicitly and rigorously those functions, which could result in a security flaw, as we have shown in [26] for the set of functions given by Eqs. (8.4)-(8.6). Another example of the kind of problem under consideration can be found in some encryption schemes built upon continuous-time chaotic systems. Certainly, when working with this type of chaotic systems it is necessary to use numerical methods to compute the chaotic orbits. The decryption procedure requires to generate the same chaotic orbits as in the encryption stage and, consequently, its computation must be done using the same numerical method and the same time step. Moreover, the influence of both the numerical method and the time step on the performance of the cryptosystem must be thoroughly evaluated. Let us take up again the cryptosystem defined in [44]. The masking stage of that cryptosystem is driven by a keystream derived from the orbits of Lorenz and Chen Systems. In [44], the authors did not say anything about the time step τ of iterating the Lorenz and Chen systems. However, the randomness of the keystream is tightly dependent on the value of the time step. As an extreme example, if $\tau = 10^{-20}$, we will get a keystream of identical elements (according to the algorithm described in Sec. 2.3 of [44]).

8.3 Design rules for chaos-based cryptography

According to the above problems, we proceed with the concretion and systematization of the guidelines to observe when designing a chaos-based digital cryptosystem. These guidelines, that can be interpreted as the extension of the set of rules provided in [6].

Rule 1 ***Exhaustive and rigorous definition of the chaotic encryption and decryption algorithms.***

The design of any encryption system must be guided by Kerckhoffs' principles, and thus the consecution of security through obscurity must be totally discarded. The designed cryptosystem must be easily reproducible, in order to make its implementation, use and further analysis easy. Indeed, guaranteeing the security of an encryption procedure is a quite complex and elusive problem, so the more people participate in the analysis, the more complete the security assessment will be. Regarding specifically chaos-based cryptosystems, the design rule here referred implies that:

a) The encryption/decryption algorithms must assure control parameters determining the chaotic behavior of the selected maps.
b) The final cryptosystems must be evaluated by means of the classical cryptanalytic framework [21, Sec. 1.2.2].
c) It must be confirmed that an attacker cannot get enough information about the underlying chaotic orbits, and thus she cannot carry out an estimation of control parameters and/or initial condition.

Rule 2 ***Exhaustive and rigorous definition of the key and the key space.***

In chaos-based cryptography it is mandatory to specify clearly and carefully the relationship between the secret key and the parameters determining the temporal evolution of the underlying chaotic maps, i.e., the control parameters and the initial conditions. In some cryptosystems either the control parameters or the initial conditions or both are part of the secret key, whereas in others they are just design parameters and, consequently, publicly known. Another possibility is that the secret key determines the values of the control parameter(s) and initial condition(s). In all situations it must be verified that the underlying dynamical systems involved in the considered chaos-based cryptosystem evolve as required, i.e., in a chaotic way. In other words, the values of the control parameters used during encryption and decryption must determine a positive value of the largest component of the Lyapunov Exponent (LE). In this respect, this rule is related to the diffusion property, since it is intended to make the relationship between the key (or the plaintext) and the ciphertext as complex as possible. The goal is to erase any possible pattern or redundancy in the ciphertext, and thus to avoid inference of the secret key from the ciphertext. In the context of chaos-based cryptography,

diffusion is connected to the local rate of divergence of orbits. As a result, chaotic maps with high values of LE must be selected. It is also possible to use chaotic maps with small LE if the encryption of each unit of plaintext is performed iterating several times the chaotic map. Nevertheless, it implies a reduction of the efficiency of the cryptosystem, and thus it is preferable to discretize the key space to guarantee the *avalanche effect*, i.e., the result of encrypting a plaintext with two slightly different keys must produce totally different ciphertexts. The tools for verification of the avalanche effect are the same used in the assessment of parameter mismatch (next rule), i.e., the statistical distance and the MRE (MultiResolution Entropy) . The discretization of the key space implies a reduction of its size, which could result in a degradation of the protection against brute-force attacks. A possible solution to this problem is to discretise the orbits of the chaotic maps instead of the key space. As we have shown in [21, Sec. 2.2] for the skew tent map, this strategy determines an increasing of the LE and, consequently, of diffusion.

On the other hand, the determination of LE entails some inaccuracies [90] and, consequently, it is highly advisable to analyze the chaoticity of orbits using auxiliary tools as the entropy measures referred in [21, Secs. 2.4 and 2.5]. Finally, either LE or the different entropy measures can bring to light a somehow one-to-one relationship between the rate of divergence of orbits and the control parameter(s). In this case, if a chaos-based cryptosystem allows an estimation of the rate of divergence, then it could be possible to estimate the control parameter(s), which represents a vulnerability of the cryptosytem being the control parameter(s) part or determined by the secret key.

Rule 3 ***Selection of chaotic maps with high sensitivity to control parameter mismatch.***

The size of the key space of any cryptosystem must be large enough to avoid the feasibility of a brute-force attack. This is a common requirement of all encryption systems, and it has to be fulfilled in accordance with the computational capacity of any possible attacker. As it is pointed out in [6, Rule 15], today's computer speed requires a key space of size larger than 2^{100}. As indicated by the previous rule, in digital chaos-based cryptography the specification of the key space is mainly guided by the calculation of the LE. Consequently, the resolution in the computation of the LE is a measure of the maximum number of possible keys, and thus an approximation of the size of the key space. To get a number of keys larger than $2^{100} \approx 10^{30}$, the resolution must be 10^{-30}. However, with that resolution, thousands of keys would become equivalent, unless there is a strong sensitivity to parameter mismatch. It implies that the concretion of the key space must be accompanied of an exhaustive analysis of the orbits generated for each value of the control parameters. Indeed, it must be tested that the orbits are different enough to assure that the encryption procedure possesses confusion and diffusion properties. Useful tools in this regard are the statistical distance [21, Sec. 2.6] and the MRE [21, Sec 2.5.2].

Rule 4 ***The selected chaotic map should not allow total characterization of its dynamics from partial knowledge of this dynamics.***

The total characterization of the dynamics of a chaotic map requires the knowledge of the initial condition and the control parameter(s). When considering a chaos-based cryptosystem, it could be possible for an attacker to guess either the initial condition or control parameter(s). Upon the guessed information, the attacker could use some of the general attack strategies [21, Sec. 1.2.2] to get some additional information about the orbits of the underlying chaotic map. For some chaotic maps, this additional information and the guessed information drive to the estimation of the rest of parameter(s) describing the dynamics of the map. For example, if the chaotic map selected for an encryption architecture is a unimodal map, and the encryption architecture allows to infer the symbolic sequences of the map through some attack, then the knowledge of the control parameter allows to recover the initial condition.

Rule 5 ***Analysis of the performance of chaotic orbits as source of entropy.***

From the point of view of cryptography, the appealing of chaos is mainly motivated by its random-like behavior. Actually, "the battle" of any cryptographer is to look for sources of uncertainty that can be further used to conceal the information. The design of a cryptosystem is the specification of a series of transformation procedures based on sources of indetermination and applied on the source of information. In chaos-based cryptography, all or some of the transformation procedures use chaos as source of indetermination. Since the security of the whole cryptosystem lies on the efficiency of each transformation procedure, the entropy must be evaluated. Again, the assessment can be done upon tools as those described in [21, Secs. 2.6 and 2.5.2]. Furthermore, this assessment can also be refined by considering every transformation procedure as a *Pseudo Random Number Generator* (PRNG). Upon this consideration, evaluation can be fulfilled using the battery of statistical tests of the National Institute of Standard & Technology (NIST) [84]. Nevertheless, if chaos is used as base of a stream cipher, then it is also necessary to analyze the possibility of reconstructing the symbolic dynamics in order to verify the feasibility of estimation for the control parameter(s) and initial condition(s) as it is done in [21, Chapters 3 and 4].

Rule 6 ***Chaotic maps with uniform invariant density functions and measure of the invariant set independent of the control parameters should be used.***

If this requirement is satisfied, then the chaotic cryptosystem possesses the confusion property. If the underlying dynamical system evolves, as expected,

chaotically, then it possesses the ergodic property and thus orbits are statistically independent of the control parameter(s) and initial condition(s). As a result, the ciphertext should be statistically undistinguishable from the output of a truly random function, and should be statistically the same for all the keys.

Rule 7 ***The ciphertext space must be defined in such a way that the reconstruction of the dynamics of the underlying chaotic maps is not possible.***

Ciphertexts of chaos-based cryptosystems must not leak information about the symbolic dynamics, the return map or any other shortcut to reconstruct the dynamics of the underlying chaotic maps.

Rule 8 ***The encryption/decryption time must not depend on the value of the secret key of a chaos-based cryptosystem.***

If it is necessary to perform encryption through several rounds and several iterations of the underlying chaotic maps, then the number of encryption rounds and the number of iterations must be publicly known. They can not be considered as part of the secret key, since a mere analysis of the encryption/decryption time allows an estimation of those values.

Rule 9 ***Resistance to classical attacks.***

The cryptanalysis of chaos-based cryptosystems combined techniques from the theory of dynamical systems and from the cryptanalysis of conventional cryptography. In this concern, it must be verified the robustness of the cryptosystem against known-plaintext, chosen-plaintext, known-ciphertext (or ciphertext-only), and chosen-ciphertext attacks [100, p. 95]. Specialized attacks must also be evaluated [99]. For digital chaos-based block ciphers resistance to differential [102] and linear cryptanalysis [53] must be proved.

Rule 10 ***Resistance to application-specific attacks.***

The encryption of information with special features must be defined carefully in order to avoid the leaking of such features in the ciphertext. This is the case of digital images and videos. In digital images (videos) there exists strong correlation between different pixels (transform coefficients), which can be used to develop some effective correlation-based attacks.

8.4 Chaos-based cryptography: a conclusion but not the end of the road

Recalling the main conclusions of our works in the field of cryptanalysis, a theoretical framework is next proposed in order to fulfill the set of rules previously explained. This theoretical basis is conceived as a manner to achieve

at least the same level of security and efficiency of conventional cryptography, but using the theory of chaotic dynamical systems as core instead of the theory of numbers.

Nowadays, the information (whether analog or digital) is processed by computers. This means that however chaos enters the encryption (key-stream generation, masking, etc.), the finite precision of the computer (or any other finite-state machine for this matter) will degrade chaotic orbits to periodic orbits — occasionally of a very long period. Although this may be acceptable from a practical point of view, it is not from a theoretical one. Put in other words, the concept and virtues of chaos are not exportable without change to the realm of discrete and finite mathematics.

If there is no chaos in a finite-state space, what is then a "chaotic" cipher? To answer this question in a satisfactory way, one has to go away from the real numbers (there are no real numbers in the real world) and use algorithms on integer numbers or finite fields, while preserving the spirit of chaos-based cryptography. A paradigmatic example was given by Pichler and Scharinger, and reproduced in [43], where several chaotic maps were discretized and used for image encryption. Let us remember it at this point.

Let $I^2 = [0,1] \times [0,1] \subset \mathbb{R}^2$ endowed with the Lebesgue measure, and let $B : I^2 \to I^2$ be the *baker map*,

$$B(x,y) = \begin{cases} (2x, \frac{1}{2}y), & 0 \leq x < \frac{1}{2}, \\ (2x-1, \frac{1}{2}y + \frac{1}{2}), & \frac{1}{2} \leq x \leq 1. \end{cases}$$

The baker map is a chaotic bijection of the unit square I^2 onto itself. This map stretches the left rectangle $[0,1/2) \times [0,1)$ horizontally onto the "bottom" rectangle $[0,1) \times [0,1/2)$, while the right rectangle $[1/2,1) \times [0,1)$ is similarly mapped onto the "top" rectangle $[0,1) \times [1/2,1)$.

Pichler and Scharinger generalized this map in the following way [43]. The unit square I^2 is now divided into k vertical rectangles $[F_{i-1}, F_i) \times [0,1)$, $i = 1, ..., k$, $F_i = p_1 + ... + p_i$, $F_0 = 0$, with $p_1 + ... + p_k = 1$. The *generalized baker map* stretches each rectangle horizontally by the factor of $1/p_i$, while it is contracted vertically by the factor of p_i. Finally, all transformed rectangles are stacked on top of each other. Formally,

$$B(x,y) = \left(\frac{1}{p_i}(x - F_i), p_i y + F_i \right)$$

for

$$(x,y) \in [F_i, F_i + p_i) \times [0,1).$$

If we denote this map by $B_{(p_1,...,p_k)}$, then the standard baker map corresponds to $B_{(1/2,1/2)}$. The generalized baker map inherits all important properties of the baker map such as sensitivity to initial conditions and parameters, mixing and bijectiveness.

One possibility of discretizing $B_{(p_1,...,p_k)}$ on an integer lattice is the following. Let N be an integer, and let $n_1, ..., n_k$ be integers such that each n_i divides N, and $n_1 + ... + n_k = N$. Denoting $N_i = n_1 + ... + n_i$, the lattice point (r, s), with $N_{i-1} \leq r < N_i$, $N_0 = 0$, and $0 \leq s < N$, is mapped by the *discretized generalized baker map* $B_{(n_1,...,n_k)}$ to[3]

$$B_{(n_1,...,n_k)}(r,s) = \left(\frac{N}{n_i}(r - N_i) + s \bmod \frac{N}{n_i}, \frac{n_i}{N}\left(s - s \bmod \frac{N}{n_i}\right) + N_i\right).$$

Coming back to the question, what a chaotic cipher on a finite-state space should be, the answer (intentionally vague) proposed in [15] and repeated in the next section, was inspired by this and similar examples. Other technique, studied in [59] in the framework of *discrete chaos*, furnish permutations by truncation of chaotic orbits. Since the discretized map, whatever the discretization method used, is desired to somehow inherit the properties of the continuous chaotic map, the former should become increasingly close to the latter in the 'continuous' limit. In the case of the discretized baker map, the continuous limit refers to an ever finer coarse-graining of the unit square. In the framework of discrete chaos, the continuous limit refers to ever longer orbits segments, and the closeness refers to the convergence of the discrete LE(s) of the permutation to the LE(s) of the chaotic map.

8.4.1 Chaos-based cryptography on integer numbers and finite fields

The idea underlying the above construction of the discretized generalized baker map (namely, to define a permutation via discretization of a chaotic map) provides an approach to chaos-based cryptography that is compliant with the standards of conventional cryptography. This idea was captured with different degrees of generality in [16, 102] (definition of permutations via periodic approximations of automorphisms) and also in [15] (definition of chaotic cryptographic primitives). The minimal framework we need for this formulation is that of measure theory.

We say that $(X, \mathcal{A}, \mu)$ is a measure space if X is a non-empty set, $\mathcal{A}$ is a sigma-algebra of subsets of X and μ is a measure on $(X, \mathcal{A})$. If $\mu(X) < \infty$, $(X, \mathcal{A}, \mu)$ is called a finite-measure space. Typically, X will be a compact topological or even metric space (think of a finite interval of $\mathbf{R}^n$ or of an n-torus). We say that $\mathcal{P} = \{A_1, ..., A_N\} \subset \mathcal{A}$ is a partition of X if $\cup_{n=1}^{N} A_n = X$ and $A_i \cap A_j = \emptyset$ for all $i \neq j$. A norm of $\mathcal{P}$ is a measure of its 'coarseness' (e.g., maximal length, maximal diameter, etc. of the elements of $\mathcal{P}$). In order to streamline the notation, we will usually refer only to X, with the underlying

[3] The cipher proposed in [43] based on the discretized generalized baker map, was cryptanalyzed in [98].

$\mathcal{A}$ and μ being understood. Furthermore, chaos refers to dynamical systems and these call for measure-invariant self-maps on finite-measure spaces, i.e., maps $f : X \to X$ such that $f^{-1}A \in \mathcal{A}$ and $\mu(f^{-1}A) = \mu(A)$ for all $A \in \mathcal{A}$.

A generalization of the discretized generalized baker map is the following [36]. Suppose f is an automorphism of the finite-measure space $(X, \mathcal{A}, \mu)$, i.e., f is a one-to-one map of X onto itself such that both f and f^{-1} are μ-invariant. We consider sequences of finite partitions $\{\mathcal{P}_n\}$ of the space X, $\mathcal{P}_n = \{P_k^{(n)} : 1 \leq k \leq q_n\}$, such that $\lim_{n\to\infty} \mathcal{P}_n = \mathcal{E}$ (the partition of X into separate points) and sequences of automorphisms $\{f_n\}$ such that f_n preserves $\mathcal{P}_n$ (i.e., f_n sends every element of $\mathcal{P}_n$ into an element of the same partition). We say that an automorphism f of the space $(X, \mathcal{A}, \mu)$ possesses an approximation by periodic transformations with speed $\vartheta(n)$, if there exists a sequence of automorphisms f_n preserving $\mathcal{P}_n$ such that

$$\sum_{k=1}^{q_n} \mu\left(f(P_k^{(n)}) \triangle f_n(P_k^{(n)})\right) < \vartheta(q_n), \quad n = 1, 2, \ldots.$$

where $\triangle$ stands for symmetric set difference and ϑ is a function on the integers such that $\vartheta(n) \to 0$ monotonically. The sequence $(\mathcal{P}_n, f_n)$ is a discrete approximation of (X, f).

A further generalization brings us to the concept of *discrete approximation*. This time we leave deliberately open the way the 'discrete approximation' converges to the continuous map.

Definition 1. *[15]* Let X be a finite-measure space and $f : X \to X$ a map. Let $X_\Delta = \{A_1, ..., A_{N(\Delta)}\}$ be a family of partitions of X, labelled by a parameter Δ, say, the partition norm, such that $\lim_{\Delta\to 0} X_\Delta = \mathcal{E}$, the partition of X into separate points. Furthermore, given a family of maps $f_\Delta : X_\Delta \to X$, define the extensions $\bar{f}_\Delta : X \to X$ as $\bar{f}_\Delta(x) = f_\Delta(A_n)$ if $x \in A_n \in X_\Delta$. We say that (X_Δ, f_Δ) is a discrete approximation of (X, f) if, moreover, $\lim_{\Delta\to 0} \bar{f}_\Delta = f$ in some relevant sense (depending on the structure we put on X).

This definition of discrete approximation is an idealization of what actually happens when computing real functions with computers. Intuitively, discrete approximation of chaotic maps are expected to generate permutations with 'nice' mixing properties and, therefore, appropriate for cryptographic applications.

Definition 2. *[15]* Discrete approximations of chaotic systems (X, f) in form of permutations $(\mathbf{Z}_M, F_M)$ are called chaotic cryptographic primitives. Furthermore, we say that a cryptographic algorithm is chaotic if some of its building blocks is a chaotic cryptographic primitive.

Thus, a stream cipher whose keystream is generated by a chaotic primitive is a chaos-based cryptosystem. Let us present a few examples of chaotic primitives (see also [15, 17]).

Example 1. The Renyi map, $\phi_\beta : [0,1) \to [0,1)$, is defined as

$$\phi_\beta(x) = \beta x \bmod 1,$$

where $1 < \beta \in \mathbb{R}$. A discretized (or digitalized) Renyi map f can be defined on the set $\{0, 1, ..., 2^n - 1\}$ by

$$f(k) = \lfloor \beta \cdot k \rfloor \bmod 2^n.$$

The derivation proceeds via the approximation of real numbers in $[0,1)$ by dyadic rationals. The *discretized Renyi map* was used in [1] to generate random numbers.

Example 2. The Chebyshev polynomial maps $T_n : \mathbf{R} \to \mathbf{R}$ of degree $n = 0, 1, ...$ are defined by the recursion

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \text{ for } n \geq 2,$$

with $T_0(x) = 1$, $T_1(x) = x$. The interval $[-1,1]$ is invariant under the action of the map T_n: $T_n([-1,1]) = [-1,1]$. Alternatively, one can define

$$T_n(x) = \cos(n \arccos x), \quad -1 \leq x \leq 1.$$

The Chebyshev polynomial T_n restricted to $[-1,1]$ is a well-known chaotic map for all $n \geq 2$: it has a unique absolutely continuous invariant measure,

$$\mu(x) = \frac{1}{\pi\sqrt{1-x^2}},$$

and LE $\ln n > 0$ with respect to μ. For $n = 2$, the Chebyshev map reduces to the logistic map.

It is straightforward to prove that Chebyshev polynomials have the semi-group property:

$$T_r(T_s(x)) = T_s(T_r(x)) = T_{rs}(x).$$

Let p be a prime number so as $\mathbb{Z}_p$ is a field. The *Chebyshev map* over the finite field $\mathbb{Z}_p$, $F_{n,p} : \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}$, is defined as

$$F_{n,p}(\xi) = T_n(\xi) \pmod{p}.$$

The semi-group property of the 'discrete' (or finite state) Chebyshev maps $F_{n,p}$ can be used in key-exchange protocols or even in public-key algorithms [79, 58, 57]. However, this kind of maps (as any other) does not guarantee security itself, and a convenient key-exchange protocol along with an adequate encryption procedure should be provided to achieve not only security, but also computational efficiency (see the cryptanalysis of [110] in [2]).

Other examples of chaotic primitives used in ciphers published in the literature, include the discrete logistic map and toral automorphisms (see, e.g., [58, 77]).

As a last example, let us discuss a synchronization-based cipher.

Example 3. *Message-embedding* is an encryption algorithm in which the message m_t is directly injected (or "embedded") in a chaotic dynamic $f_\theta : J \to J$, where $J \subset \mathbb{R}^q$ and $\theta = (\theta_1, ..., \theta_D)$ is an, in general, multi-component parameter which acts as the secret key or is part of the secret key of the cipher. In the simplest versions, encryption takes place at the *sender* according to one of the following schemes:

$$\text{(I)} \begin{cases} x_{t+1} = f_\theta(x_t, m_t) \\ y_t = h_\theta(x_t, m_t) \end{cases} \text{ and (II)} \begin{cases} x_{t+1} = f_\theta(x_t, m_t) \\ y_t = h'_\theta(x_t) \end{cases}, \tag{8.29}$$

the difference being the so-called *relative degree* r [81]; $r = 0$ in case (I) and $r > 0$ in case (II). h_θ is called the *output function* of the sender, since y_t is the message conveyed from the sender to the receiver through the communicaction channel. In general, $h_\theta : J \to \mathbb{R}^{q'}$ with $q' \leq q$ (ideally $q' = 1$). The *receiver* is a kind of 'mirrored' dynamical system, generated by a family of maps $\tilde{f}_\theta$ and endowed with output functions $\tilde{h}_\theta$. The retrieval of the message (plaintext) at the receiver is achieved in two steps: (i) *synchronization* [45, 108], based on a suitable choice of $\tilde{f}_\theta$, and (ii) *estimation* of m_t by means of a suitable function which depends on the internal state $\hat{x}_t$ of the receiver and the output y_t, the only information transmitted from the sender to the receiver.

Two mechanisms have been proposed in the literature to recover m_t: (i) the inverse system approach [41] and, in case of noisy channels, (ii) the unknown input observer approach (UIO) [52, 82]. In both cases, the equations governing the receiver are:

$$\begin{cases} \hat{x}_{t+r+1} = \tilde{f}_\theta(x_{t+r}, y_t, ..., y_{t+r}) \\ \hat{m}_{t+r} = g_\theta(\hat{x}_{t+r}, y_t, ..., y_{t+r}) \end{cases},$$

with $r \geq 0$ and g such that

$$\hat{m}_{t+r} = g_\theta(\hat{x}_{t+r}, y_t, ..., y_{t+r}) = m_t \text{ when } \hat{x}_{t+r} = x_t.$$

The existence of an inverse system or an UIO is guaranteed under the assumption that the system (8.29-I) or (8.29-II) is left invertible. In our setting, *left invertibility* means that there exists an integer $R \geq 0$ such that the input m_t is uniquely determined by the knowledge of the state x_t along with the output sequence $y_t, ..., y_{t+R}$.

Message-embedding is very attractive because synchronization is assured without any restriction on the variation rate of m_t. For cryptographic applications it is sometimes convenient to decompose the dynamic f_θ in two actions in order to eventually incorporate boolean and arithmetic operations. Such is the case of the *hybrid message-embedding* technique, where the chaotic

dynamic is decomposed as follows:

$$\text{(I')} \quad \begin{cases} u_t = \nu_e(x_t, m_t) \\ x_{t+1} = q_\theta(x_t, u_t) \\ y_t = r_\theta(x_t, u_t) \end{cases} \quad \text{and} \quad \text{(II')} \quad \begin{cases} u_t = \nu_e(x_t, m_t) \\ x_{t+1} = q_\theta(x_t, u_t) \\ y_t = r'_\theta(x_t) \end{cases} , \tag{8.30}$$

for sender systems with relative degree $r = 0$ (I') and $r > 0$ (II'). u_t is sometimes called the *pre-ciphertext* in hybrid message-embedding.

Message-embedding and hybrid message-embedding can be used with letters taken from finite fields (and boolean operations in the hybrid scheme) [81]. Under the further assumption of *flatness* [81], they have been proved to be structurally equivalent to a self-synchronizing stream cipher —a well-tested architecture in conventional cryptography. We conclude that the security of these chaos-based ciphers relies on the security of the corresponding chaotic primitives (f_θ in (8.29), and q_θ and/or ν_e in (8.30)).

References

1. Addabbo, T., Alioto, M., Fort, A., Pasini, A., Rocchi, S., Vignoli, V.: A class of maximum-period nonlinear congruential generators derived from the reńyi chaotic map. IEEE Transactions on Circuits and Systems–I: Regular Papers **54**(4), 816–828 (2007)
2. Alvarez, G.: Security problems with a chaos-based deniable authentication scheme. Chaos, Solitons & Fractals **26**(1), 7 – 11 (2005)
3. Alvarez, G., Arroyo, D., Nunez, J.: Application of Gray code to the cryptanalysis of chaotic cryptosystems. In: 3rd International IEEE Scientific Conference on Physics and Control (PhysCon'2007, 3rd - 7th, September 2007, Potsdam, Germany) (2007). URL http://lib.physcon.ru/?item=1358
4. Alvarez, G., Li, S.: Estimating short-time period to break different types of chaoitc modulation based secure communications. arxiv:nlin.CD/0406039 (2004). http://arxiv.org/abs/nlin/0406039
5. Alvarez, G., Li, S.: Breaking an encryption scheme based on chaotic baker map. Physics Letters A **352**(1-2), 78–82 (2006)
6. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos **16**(8), 2129–2151 (2006)
7. Alvarez, G., Li, S., Hernandez, L.: Analysis of security problems in a medical image encryption system. Computers in Biology and Medicine **37**(3), 424–427 (2007)
8. Alvarez, G., Li, S., Montoya, F., Romera, M., Pastor, G.: Breaking projective chaos synchronization secure communication using filtering and generalized synchronization. Chaos, Solitons & Fractals **24**(3), 775–783 (2005)
9. Alvarez, G., Montoya, F., Pastor, G.: Cryptanalysis of a discrete chaotic cryptosystem using external key. Physics Letters A **319**, 334–339 (2003)
10. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of a chaotic encryption system. Physics Letters A **276**, 191–196 (2000)
11. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of an ergodic chaotic cipher. Physics Letters A **311**, 172–179 (2003)
12. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Breaking parameter modulated chaotic secure communication system. Chaos, Solitons & Fractals **21**(4), 793–797 (2004)

13. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Cryptanalysis of dynamic look-up table based chaotic cryptosystems. Physics Letters A **326**, 211–218 (2004)
14. Alvarez, G., Montoya, F., Romera, M., Pastor, G.: Keystream cryptanalysis of a chaotic cryptographic method. Computer Physics Communications **156**, 205–207 (2004)
15. Amigó, J., Kocarev, L., Szczepanski, J.: Theory and practice of chaotic cryptography. Physics Letters A **366**(3), 211 – 216 (2007)
16. Amigó, J., Szczepanski, J.: Approximations of dynamical systems and their applications to cryptography. International Journal of Bifurcation and Chaos **13**, 1937–1948 (2003)
17. Amigó, J.M.: Intelligent Computing Based on Chaos, Eds. L. Kocarev and Z. Galias and S. Lian, chap. Chaos-based cryptography, pp. 291–314. Springer Verlag (2009)
18. Amigó, J.M., Szczepanski, J., Kocarev, L.: A chaos-based approach to the design of cryptographically secure substitutions. Physics Letters A **343**, 55–60 (2005)
19. Argenti, F., Benzi, S., Re, E.D., Genesio, R.: Stream cipher system based on chaotic maps. In: Mathematics and Applications of Data/Image Coding, Compression, and Encryption III, *Proceedings of SPIE*, vol. 4122, pp. 10–17. SPIE (2001)
20. Ariffin, M., Noorani, M.: Modified Baptista type chaotic cryptosystem via matrix secret key. Physics Letters A **372**, 5427–430 (2008)
21. Arroyo, D.: Framework for the analysis and design of encryption strategies based on discrete-time chaotic dynamical systems. Ph.D. thesis, ETSIA of the Polytechnic University of Madrid, Madrid, Spain (2009). Avalaible online at http://digital.csic.es/handle/10261/15668
22. Arroyo, D., Alvarez, G., Amigó, J.M.: Estimation of the control parameter from symbolic sequences: Unimodal maps with variable critical point. Chaos: An Interdisciplinary Journal of Nonlinear Science **19** (2009). Art. no. 023125
23. Arroyo, D., Alvarez, G., Amigó, J.M., Li, S.: Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. Communications in Nonlinear Science and Numerical Simulation **16**(2), 805–813 (2011)
24. Arroyo, D., Alvarez, G., Li, S.: Some hints for the design of digital chaos-basedcryptosystems: lessons learned from cryptanalysis. In: Second IFAC Conference on Analysis and Control of Chaotic Systems. Queen Mary, University of London (2009)
25. Arroyo, D., Alvarez, G., Li, S., Li, C., Fernandez, V.: Cryptanalysis of a new chaotic cryptosystem based on ergodicity. International Journal of Modern Physics B **23**(5), 651–659 (2009)
26. Arroyo, D., Alvarez, G., Li, S., Li, C., Nunez, J.: Cryptanalysis of a discrete-time synchronous chaotic encryption system. Physics Letter A **372**(7), 1034–1039 (2008)
27. Arroyo, D., Li, C., Li, S., Alvarez, G.: Cryptanalysis of a computer cryptography scheme based on a filter bank. Chaos, Solitons & Fractals **41**, 410–413 (2009)
28. Arroyo, D., Li, C., Li, S., Alvarez, G., Halang, W.A.: Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos, Solitons & Fractals **41**(5), 2613–2616 (2009)
29. Arroyo, D., Rhouma, R., Alvarez, G., Li, S., Fernandez, V.: On the security of a new image encryption scheme based on chaotic map lattices. Chaos: An Interdisciplinary Journal of Nonlinear Science **18** (2008). Art. no. 033112
30. Banerjee, S., Yorke, J.A., Grebogi, C.: Robust chaos. Physical Review Letters **80**, 14 (1998)
31. Baptista, M.S.: Cryptography with chaos. Physics Letters A **240**(1-2), 50–54 (1998)
32. Beth, T., Lazic, D.E., Mathias, A.: Cryptanalysis of cryptosystems based on remote chaos replication. In: Advances in Cryptology – EuroCrypt'94, *Lecture Notes in Computer Science*, vol. 950, pp. 318–331. Springer-Verlag, Berlin (1994)
33. Brumley, D., Boneh, D.: Remote timing attacks are practical. In: Proceedings of the 12th USENIX Security Symposium, pp. 1–14. USENIX Association (2003)

34. Chee, C.Y., Xu, D.: Chaotic encryption using dicrete-time synchronous chaos. Physics Letters A **348**(3-6), 284–292 (2006)
35. Chen, G., Ueta, T.: Yet another chaotic attactor. International Journal of Bifurcation and Chaos **9**(7), 1465–1466 (1999)
36. Cornfeld, I., Fomin, S.V., Sinai, Y.: Ergodic theory. Springer, New York (1982)
37. Cuomo, K., Oppenheim, A.V., Strogatz, S.: Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Transactions on Circuits and Systems–II: Analog and Digital Signal Processing **40**(10), 626–633 (1993)
38. Dedieu, H., Kennedy, M., Hasler, M.: Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. IEEE Transactions on Circuits and Systems–II: Analog and Digital Signal Processing **40**, 634–641 (1993)
39. Dedieu, H., Ogorzalek, M.J.: Identifiability and identification of chaotic systems based on adaptive synchronization. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **44**(10), 948–962 (1997)
40. Feki, M.: An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons & Fractals **18**(1), 141–148 (2003)
41. Feldmann, U., Hasler, M., Schwarz, W.: Communication by chaotic signals: the inverse system approach. International Journal of Circuit Theory and Applications **24**, 551–579 (1996)
42. Fradkov, A.L., Markov, A.Y.: Adaptive synchronization of chaotic systems based on speed gradient method and passification. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **44**, 905–912 (1997)
43. Fridrich, J.: Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos **8**, 1259–1284 (1998)
44. Gao, T., Chen, Z.: Image encryption based on a new total shuffling algorithm. Chaos, Solitons & Fractals **38**(1), 213–220 (2008)
45. González-Miranda, J.: Synchronization and control of chaos. Imperial College Press, London (2004)
46. Habutsu, T., Nishio, Y., Sasase, I., Mori, S.: A secret key cryptosystem by iterating a chaotic map. In: Advances in Cryptology – EuroCrypt'91, *Lecture Notes in Computer Science*, vol. 547, pp. 127–140. Springer (1991)
47. Hasler, M.: Synchronization of chaotic systems and transmission of information. International Journal of Bifurcation and Chaos **8**(4), 647–659 (1998)
48. Higham, N.J.: Accuracy and Stability of Numerical Algorithms, 2 edn. SIAM (1961)
49. Hirsch, M.W., Smale, S.: Differential equations, dynamical systems, and linear algebra. Academic Press, Inc., San Diego, California (1974)
50. Hu, G., Feng, Z., Meng, R.: Chosen ciphertext attack on chaos communication based on chaos synchronization. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **50**(2), 275–279 (2003)
51. Huijberts, H., Nijmeijer, H., Willems, R.: System identification in communication with chaotic systems. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **47**, 800–808 (2000)
52. Inoue, E., Ushio, T.: Chaos communication using unknown input observers. Electronics and Communications in Japan (Part III: Fundamental Electronic Science) **84**(12), 21–27 (2001)
53. Jakimoski, G., Kocarev, L.: Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **48**(2), 163–169 (2001)
54. Jiang, Z.P.: A note on chaotic secure communication systems. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **49**(1), 92–96 (2002)
55. Kocarev, L.: Chaos-based cryptography: A brief overview. IEEE Circuits and Systems Magazine **1**(2), 6–21 (2001)
56. Kocarev, L., Halle, K., Eckert, K., Chua, L.O., Parlitz, U.: Transimission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos **2**(4), 973–977 (1992)

57. Kocarev, L., Makraduli, J., Amato, P.: Public-key encryption based on Chebyshev polynomials. Circuits, Systems, and Signal Processing **24**, 497–517 (2005)
58. Kocarev, L., Sterjev, M., Fekete, A., Vattay, G.: Public-key encryption with chaos. Chaos: An Interdisciplinary Journal of Nonlinear Science **14**(4), 1078–1082 (2004)
59. Kocarev, L., Szczepanski, J., Amigo, J., Tomovski, I.: Discrete chaos–I: Theory. IEEE Transactions on Circuits and Systems–I: Regular Papers **53**(6), 1300–1309 (2006)
60. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Advances in Cryptology – CRYPTO'96, *Lecture Notes in Computer Science*, vol. 1109, pp. 104–113. Springer (1996)
61. Kolumban, G., Kennedy, M., 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), 1129–1140 (1998)
62. Letellier, C., Gouesbet, G.: Topological characterization of reconstructed attractors modding out symmetries. Journal de Physique II **6**(11), 1615–1638 (1996)
63. Li, C., Li, S., Alvarez, G., Chen, G., Lo, K.T.: Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations. Physics Letters A **369**, 23–30 (2007)
64. Li, S.: Analyses and new designs of digital chaotic ciphers. Ph.D. thesis, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China (2003). Available online at http://www.hooklee.com/pub.html
65. Li, S., Alvarez, G., Chen, G.: Breaking a chaos-based secure communication scheme designed by an improved modulation method. Chaos, Solitons & Fractals **25**(1), 109–120 (2005)
66. Li, S., Alvarez, G., Chen, G.: Return-map cryptanalysis revisited. International Journal of Bifurcation and Chaos **16**(5), 1557–1568 (2006)
67. Li, S., Alvarez, G., Li, Z., Halang, W.: Analog chaos-based secure communications and cryptanalysis: a brief survey. In: J. Kurths, A. Fradkov, G. Chen (eds.) 3rd Int. IEEE Scientific Conference on Physics and Control (PhysCon 2007), p. 92. Potsdam, Germany (2007). Full edition available at http://www.hooklee.com/Papers/PhysCon2007.pdf
68. Li, S., Chen, G., Mou, X.: On the dynamical degradation of digital piecewise linear chaotic maps. International Journal of Bifurcation and Chaos **15**(10), 3119–3151 (2005)
69. Li, S., Li, C., Chen, G., Bourbakis, N.G., Lo, K.T.: A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing: Image Communication **23**(3), 212–223 (2008)
70. Li, S., Mou, X., Cai, Y.: 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, pp. 316–329. Springer (2001)
71. Li, T.Y., Yorke, J.A.: Period three implies chaos. The American Mathematical Monthly **82**, 985–992 (1975)
72. Lian, K.Y., Liu, P.: Synchronization with message embedded for generalized Lorenz chaotic circuits and its error analysis. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **47**(9), 1418–1424 (2000)
73. Ling, B.W.K., Ho, C.Y.F., Tam, P.K.S.: Chaotic filter bank for computer cryptography. Chaos, Solitons & Fractals **34**, 817–824 (2007)
74. Liu, L., Wu, X., Hu, H.: Estimating system parameters of Chua's circuit from synchronizing signal. Physics Letters A **324**(1), 36–41 (2004)
75. Lorenz, E.: Deterministic nonperiodic flow. Journal of the Atmospheric Sciences **20**, 130–141 (1963)
76. Manjunath, G., Fournier-Prunaret, D.: A qualitative analysis of deciphering errors in chaos shift keying. International Journal of Bifurcation and Chaos **19**(6), 2085–2092 (2009)

77. Masuda, N., Jakimoski, G., Aihara, K., Kocarev, L.: Chaotic block ciphers: from theory to practical algorithms. IEEE Transactions on Circuits and Systems–I: Regular Papers **53**(6), 1341–1352 (2006)
78. Matthews, R.: On the derivation of a "chaotic" encryption algorithm. Cryptologia **13**, 29–42 (1989)
79. Maze, G.: Algebraic methods for constructing one-way trapdoor functions. Ph.D. thesis, University of Notre Dame (2003)
80. Menezes, A., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press (1997)
81. Millérioux, G., Amigó, J.M., Daafouz, J.: A connection between chaotic and conventional cryptography. IEEE Transactions on Circuits and Systems–I: Regular Papers **55**(6), 1695–1703 (2008)
82. Millerioux, G., Daafouz, J.: Unknown input observers for message-embedded chaos synchronization of discrete-time systems. International Journal of Bifurcation and Chaos **14**(4), 1357–1368 (2004)
83. Millerioux, G., Mira, C.: Coding scheme based on chaos synchronization from noninvertible maps. International Journal of Bifurcation and Chaos **8**, 2019–2029 (1998)
84. NIST: A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 Revision 1A (2010). URL http://csrc.nist.gov/rng/rng2.html
85. Orúe, A., Alvarez, G., Pastor, G., Romera, M., Montoya, F., Li, S.: A new parameter determination method for some double-scroll chaotic systems and its applications to chaotic cryptanalysis. Communications in Nonlinear Science and Numerical Simulations **15**(11), 3471–3483 (2010)
86. Orúe, A., Fernandez, V., Alvarez, G., Pastor, G., Romera, M., Montoya, F.: Determination of the parameters for a Lorenz system and application to break the security of two-channel chaotic cryptosystems. Physics Letters A **372**(34), 5588–5592 (2008)
87. Pareek, N.K., Patidar, V., Sud, K.K.: Discrete chaotic cryptography using external key. Physics Letters A **309**, 75–82 (2003)
88. Parker, A., Short, K.M.: Reconstructing the keystream form a chaotic encrypiton scheme. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **48**(5), 624–630 (2001)
89. Parlitz, U., Chua, L.O., Kocarev, L., Halle, K.S., Shang, A.: Transmission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos **2**(4), 973–977 (1992)
90. Pastor, G., Romera, M., Montoya, F.: A revision of the Lyapunov exponent in 1D quadratic maps. Physica D **107**, 17–22 (1997)
91. Pecora, L.M., Carroll, T.L.: Synchronization in chaotic systems. Physical Review Letters **64**(8), 821–824 (1990)
92. Pérez, G., Cerdeira, H.A.: Extracting messages masked by chaos. Physical Review Letters **74**(11), 1970–1973 (1995)
93. Pisarchik, A.N., Flores-Carmona, N.J., Carpio-Valadez, M.: Encryption and decryption of images with chaotic map lattices. Chaos: An Interdisciplinary Journal of Nonlinear Science **16**(3) (2006). Art. no. 033118
94. Rajendra, U., Bhat, S., Kumar, S., Min, L.: Transimission and storage of medical images with patient information. Comput. Biol. Med. **33**, 303–310 (2003)
95. Rhouma, R., Solak, E., Arroyo, D., Li, S., Alvarez, G., Belghith, S.: Comment on "modified Baptista type chaotic cryptosystem via matrix secret key" [Phys. Lett. A 372 (2008) 5427]. Physics Letters A **373**(37), 3398–3400 (2009)
96. Shannon, C.: Communication theory of secrecy systems. Bell System Technical Journal **28**, 656–715 (1949)
97. Skrobek, A.: Approximation of a chaotic orbit as a cryptanalytical method on Baptista's cipher. Physics Letters A **372**(6), 849–859 (2008)

98. Solak, E., Çokal, C., Yildiz, O.T., Biyikoğlu, T.: Cryptanalysis of Fridrich's chaotic image encryption. International Journal of Bifurcation and Chaos **20**(5), 1405–1413 (2010)
99. Stamp, M., Low, R.M.: Applied cryptanalysis: breaking ciphers in the real world. John Wiley & Sons, Inc., Hoboken, New Jersey, USA (2007)
100. Stinson, D.: Cryptography: Theory and Practice. CRC Press (1995)
101. Storm, C., Freeman, W.J.: Detection and classification of nonlinear dynamic switching events. Physical Review E **58**, 1159–1162 (2002)
102. Szczepanski, J., Amigó, J., Michalek, T., Kocarev, L.: Cryptographically secure substitutions based on the approximation of mixing maps. IEEE Transactions on Circuits and Systems–I: Regular Papers **52**, 443–453 (2005)
103. Tao, C., Du, G.: A new approach to breaking down chaotic secure communication. International Journal of Bifurcation and Chaos **13**(9), 2689–2698 (2003)
104. Tao, C., Du, G., Zhang, Y.: Decoding digital information from the cascaded heterogeneous chaotic systems. International Journal of Bifurcation and Chaos **13**(6), 1599–1608 (2003)
105. Vaidya, P.G., Angadi, S.: Decoding chaotic cryptography without access to the superkey. Chaos, Solitons & Fractals **17**(2-3), 379–386 (2003)
106. Wang, X., Duan, C., Gu, N.: A new chaotic cryptography based on ergodicity. International Journal of Modern Physics B **22**(7), 901–908 (2008)
107. Wang, X., Zhan, M., Lai, C.H., Hu, G.: Error function attack of chaos synchronization based encrypiton schemes. Chaos: An Interdisciplinary Journal of Nonlinear Science **14**(1), 128–137 (2004)
108. Wu, C.W.: Synchronization in coupled chaotic circuits and systems. World Scientific, New Jersey (2002)
109. Wu, C.W., Chua, L.O.: A simple way to synchronize chaotic systems with applications to secure communications systems. International Journal of Bifurcation and Chaos **3**(6), 1619–1627 (1993)
110. Xiao, D., Liao, X., Wong, K.: An efficient entire chaos-based scheme for deniable authentication. Chaos, Solitons & Fractals **23**(4), 1327–1331 (2005)
111. Yang, T.: Recovery of digital signals from chaotic switching. International Journal of Circuit Theory and Applications **23**(6), 611–615 (1995)
112. Yang, T.: A survey of chaotic secure communication systems. Intenational Journal of Computational Cognition **2**(2), 81–130 (2004)
113. Yang, T., Wu, C.W., Chua, L.O.: Cryptography based on chaotic systems. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **44**(5), 469–472 (1997)
114. Yang, T., Yang, L.B., Yang, C.M.: Breaking chaotic secure communications using spectrogram. Physics Letters A **247**(1-2), 105–111 (1998)
115. Yang, T., Yang, L.B., Yang, C.M.: Breaking chaotic switching using generalized synchronization. IEEE Transactions on Circuits and Systems–I: Fundamental Theory and Applications **45**(10), 1062–1067 (1998)
116. Zhang, Y., Tao, C., Jiang, J.J.: Theoretical and experimental studies of parameter estimation based on chaos feedback synchronization. Chaos: An Interdisciplinary Journal of Nonlinear Science **16**(4) (2006). Art. no. 043122