Available online at www.sciencedirect.com
ScienceDirect

Physics Letters A 366 (2007) 211–216

PHYSICS LETTERS A

www.elsevier.com/locate/pla

Theory and practice of chaotic cryptography

J.M. Amigó [a,*], L. Kocarev [b], J. Szczepanski [c]

[a] *Centro de Investigación Operativa, Universidad Miguel Hernández, Avda. de la Universidad, 03202 Elche, Spain*
[b] *Institute for Nonlinear Science, University of California, San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0402, USA*
[c] *Institute of Fundamental Technological Research, Polish Academy of Science, Swietokrzyska 21, 00-049 Warsaw, Poland*

Received 6 February 2006; received in revised form 31 January 2007; accepted 2 February 2007

Available online 13 February 2007

Communicated by A.R. Bishop

Abstract

In this Letter we address some basic questions about chaotic cryptography, not least the very definition of chaos in discrete systems. We propose a conceptual framework and illustrate it with different examples from private and public key cryptography. We elaborate also on possible limits of chaotic cryptography.

1. Introduction

Chaos-based cryptography (sometimes called 'chaotic' cryptography) has been around for more than a decade by now. During this time of foundation and development, it came to mean different things, mostly depending on the implementation. So, we can speak of additive masking [1], chaos shift keying [2], two-channel communication [3], message embedding [4], etc. At the beginning, the message carriers were analogue signals, so that chaos theory could be applied as such. Later, the signals became digital and, hence, the application of chaos theory was not justified any more. Further concern came from the fact that, in general, the proposers of chaotic ciphers did not take due care about security or performance issues. As a result, most of these cryptosystems were shown to be weak against one or the other type of attack, while the safer ones were typically too slow to compete with conventional ciphers. In the mean time, authors became more cautious about cryptanalysis and implementation, which is absolutely necessary if chaotic cryptography has to consolidate as a real alternative; see [5] for a review of attacks on chaos-based ciphers and a battery of practical recommendations about security. In any case, chaotic cryptography continues to be an active research field, as shown by the large number of papers being published, and it is thriving in form of new and interesting proposals in all areas of modern cryptology.

Roughly speaking, there are two approaches when using chaotic dynamics in cryptography. The first one uses chaotic systems to generate pseudo-random sequences, which are then used as keystreams to mask the plaintext in a manifold of ways. In the second approach, the plain text is used as initial state and the ciphertext follows from the orbit being generated (see, e.g., [6] and [7] for an interesting review). The first approach corresponds to stream ciphers, while the second to block ciphers, both in secret and public key cryptography. See [8–13] for new cryptographic techniques. Beside these traditional applications, chaos-based schemes are currently being proposed for more novel applications too, like hashing, key-exchange protocols, authentication, etc., although we will not deal with them here.

One major issue in digital chaotic cryptography is the numerical implementation. Since computers can represent real numbers up to certain precision only, the orbits computed differ, in general, from the theoretical ones. (As a matter of fact, numerical precision does not deteriorate along the orbit if its calculation involves multiplications only by integers, as in the case of affine transformations on the n-torus.) More fundamentally, any orbit in a finite-state phase space is necessarily periodic or, put in other words, there is no chaos in finite-state systems (but see [14]). To circumvent this problem, the practitioners of chaotic cryptography usually resort to high precision

[*] Corresponding author.
E-mail addresses: jm.amigo@umh.es (J.M. Amigó), lkocarev@ucsd.edu (L. Kocarev), jszczepa@ippt.gov.pl (J. Szczepanski).

0375-9601/$ – see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.physleta.2007.02.021

arithmetic libraries with which several hundreds of exact decimal digits can be obtained. Notwithstanding, there are two good reasons for not using floating-point arithmetic in chaos-based cryptography. First, 'random' floating-point numbers are not uniformly distributed over any given interval of the real axis (see [15, Section 4.2.4]). Furthermore, there exist redundant number representations. Indeed, due to the normalized calculations in floating-point arithmetic, different floating-point numbers can represent the same real signal value. Second—the most important reason—there are no analytical tools for understanding the periodic structure of the orbits in the floating-point implementation of chaotic maps. Consequently, we recommend to formulate the discrete chaotic dynamics on the integers, as we do below.

The scope of this Letter is to formalize the concept of chaotic cryptography at the light of those principles that have stood the pass of time. Furthermore, it should be explained, what 'chaos' means in discrete systems. We propose a definition of discrete chaos and show that discretization and truncation of chaotic orbits cannot provide the most chaotic permutations in the limit of ever finer discretizations, what unveils some basic (though asymptotic) shortcoming of this technique. Independently of the approach to discrete chaos, the cryptographic primitives and ciphers considered in the literature share definitively some general properties that characterize them as chaotic. We have tried to distilled them out of the great variety of such proposals and hope that our present contribution will bring some unifying ideas into the picture.

2. Chaotic cryptographic primitives

We have explained in the introduction how chaotic cryptography uses discrete approximations of chaotic maps, rather than chaotic maps themselves. These approximations, in turn, can be directly translated into maps on the integers—the kind of maps used by conventional cryptography. We begin by formalizing the concept of discrete approximation.

The minimal framework we need is that of measure theory. We say that $(X, \mathcal{A}, \mu)$ is a measure space if X is a nonempty 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 $\mathbb{R}^n$ or of an n-torus). In this cases, $\mathcal{A}$ can be chosen to be the Borel sigma-algebra (generated by the open sets) and μ the corresponding Lebesgue measure. By a chaotic map on X we will understand a μ-invariant map $f : X \to X$ (i.e., $f^{-1}A \in \mathcal{A}$ and $\mu(f^{-1}A) = \mu(A)$ for all $A \in \mathcal{A}$) that is strong mixing with respect to μ (i.e., $\lim_{n\to\infty} \mu(A_1 \cap f^{-n}A_2) = \mu(A_1)\mu(A_2)$ for all $A_1, A_2 \in \mathcal{A}$). Finally, we say that $\mathcal{P} = \{A_1, \ldots, A_N\} \subset \mathcal{A}$ is a partition of X if $\bigcup_{n=1}^{N} A_n = X$ and $A_i \cap A_j = \emptyset$ for all $i \neq j$. A norm of $\mathcal{P}$ is any uniform measure of the size of its elements (e.g., maximal length, maximal diameter, etc.). In order to streamline the notation, we will usually refer only to X, with the underlying $\mathcal{A}$ and μ being understood.

Definition 2.1. Let X be a finite-measure space and $f : X \to X$ a map. Let $X_\Delta = \{A_1, \ldots, A_{N(\Delta)}\}$ 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, as the following example shows.

Example 2.2. Let $X = [0, 1]$, $X_\Delta = \{I_i\colon\ 0 \leqslant i \leqslant 10^e - 1\}$, where $I_i = [i10^{-e}, (i + 1)10^{-e})$ for $0 \leqslant i \leqslant 10^e - 2$, $I_{10^e-1} = [1 - 10^{-e}, 1]$ and $\Delta = 10^{-e}$. Set

$$f_\Delta(I_i) = f\bigl(i10^{-e}\bigr),$$

where $f : [0, 1] \to [0, 1]$ is a continuous function, and

$$\bar{f}_\Delta(x) = \sum_{j=0}^{10^e-1} f\bigl(j10^{-e}\bigr)\chi_{I_j}(x)$$

(where χ_{I_j} is the characteristic function of I_j, i.e., $\chi_{I_j}(x) = 1$ if $x \in I_j$ and 0 otherwise), so that $\bar{f}_\Delta(x) = f(i10^{-e})$ iff $i10^{-e} \leqslant x < (i + 1)10^{-e}$. Because of continuity, $|f(x) - f(y)| < \varepsilon$ if $|x - y| < \delta$. Choose now $\Delta \leqslant \delta$ and $i = \lfloor x10^e \rfloor$ to conclude that $|f(x) - \bar{f}_\Delta(x)| = |f(x) - f(i10^{-e})| < \varepsilon$. Hence, (X_Δ, f_Δ) is a discrete approximation of (X, f).

Clearly, the intervals I_i of Example 2.2 consist of all real numbers being internally represented by our ideal computer as $i10^{-e}$. Equivalently, we could have defined f_Δ rather on a discrete set $S \subset [0, 1]$ as, e.g., $f_\Delta(i10^{-e}) = \lfloor f(i10^{-e})10^e \rfloor 10^{-e}$ on $\{0, 10^{-e}, \ldots, 1 - 10^{-e}, 1\}$. We go from one to the other formulation by taking S to comprise, say, the left endpoints of X_Δ (except for the rightmost interval, where we take also the right endpoint) and restricting f_Δ from X_Δ to S or, in the other direction, by extending f_Δ from S to X_Δ constantly on each element of X_Δ. But the formulation with partitions is technically more convenient (especially in higher-dimensional intervals) since then f_Δ extends straightforwardly to $\bar{f}_\Delta$ and, in fact, both can be identified—as we will do wherever convenient.

The next example may result less familiar.

Example 2.3. (See [16].) 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, $\mathcal{P}_n = \{P_k^{(n)}\colon\ 1 \leqslant k \leqslant q_n\}$, 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

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

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) (with the conventional label $\Delta \to 0$ replaced here by $n \to \infty$).

Moreover, it is straightforward to translate discrete approximations (f_Δ, X_Δ) into maps on, say, $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$. In fact, if

$$f_\Delta(A_i) = x_i \in A_j,$$

set first $F_\Delta(i) = j$, where $1 \leqslant i, j \leqslant N(\Delta)$, to get a map on the labels of $X_\Delta = \{A_1, \ldots, A_{N(\Delta)}\}$. Furthermore, if $x_i = f_\Delta(A_i)$ and $x_j = f_\Delta(A_j)$ belong to different partition elements for all $i \neq j$, the map F_Δ will be a bijection on $\{1, \ldots, N(\Delta)\}$ or, equivalently, a permutation of $N(\Delta)$ elements. More generally, the orbits of F_Δ will decompose into eventually periodic and periodic cycles on subsets of $\{1, \ldots, N(\Delta)\}$; call F_M the restriction of F_Δ to an invariant set $S_M = \{i_1, \ldots, i_M\}$, $F_\Delta(S_M) = S_M$, and, without loss of generality, identify its invariant domain with $\mathbb{Z}_M$, $M \leqslant N(\Delta)$.

Throughout, we will also assume that the permutation F_M is irreducible, i.e., its domain $\mathbb{Z}_M$ cannot be further decomposed in invariant subsets under the action of F_Δ. These irreducible pieces can be directly generated by means of orbits. Indeed, let (X_Δ, f_Δ) be, as before, a discrete approximation of (X, f), and let (notation as in Definition 2.1) $x_{j+1} = \bar{f}_\Delta(x_j) \in A_{n_{j+1}}$, $j = 0, 1, \ldots, M-2$, be a length M trajectory of $x_0 \in A_{n_0}$ under $\bar{f}_\Delta$ such that $A_{n_j} \neq A_{n_k}$ for $j \neq k$, $0 \leqslant j, k \leqslant M-2$, and $A_{n_{M-1}} = A_{n_0}$; set $\bar{f}_\Delta(x_{n_{M-1}}) = x_{n_0}$. The map f (or, equivalently, $\bar{f}_\Delta$) induces then the obvious permutation

$$F_M(n_i) = n_j \quad \text{if } \bar{f}_\Delta(x_{n_i}) = x_{n_j} \tag{1}$$

on $\{n_0, \ldots, n_{M-1}\}$ and thus also on $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$, $M \leqslant N(\Delta)$.

Intuitively, discrete approximation of chaotic maps are expected to generate permutations with 'nice' mixing properties and, therefore, appropriate for cryptographic applications.

Definition 2.4. Discrete approximations of chaotic systems (X, f) in form of permutations $(\mathbb{Z}_M, F_M)$ 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.

In turn, the chaotic cryptographic primitives $(\mathbb{Z}_M, F_M)$ can be eventually used to generate permutations on other sets, notably the set $\{0, 1\}^n$ of n-bit blocks (with $M = 2^n$).

3. Discrete chaos

Before illustrating in the next section the concepts of chaotic cryptographic primitives and algorithms with examples, we would like to elaborate on chaotic cryptographic primitives $(\mathbb{Z}_M, F_M)$ from the point of view of discrete chaos [14].

Definition 3.1. Let $S = \{\xi_0, \xi_1, \ldots, \xi_{M-1}\}$ be a linearly ordered set by means of the order $\prec$, endowed with a metric $d(\cdot,\cdot)$, and let $F : S \to S$ be a bijection (or, equivalently, an M-permutation). We define the discrete Lyapunov exponent of f on $(S, \prec, d)$, λ_F, as

$$\lambda_F = \frac{1}{M-1} \sum_{i=0}^{M-2} \ln \frac{d(F(\xi_i), F(\xi_{i+1}))}{d(\xi_i, \xi_{i+1})}.$$

As in the usual definition of Lyapunov exponent, we have also taken natural logarithms. Without loss of generality, we may assume $(S, \prec) = (\mathbb{Z}_M, <)$ setting, if necessary, $F(i) \equiv F(\xi_i)$ and $d(i, j) \equiv d(\xi_i, \xi_j)$. Observe that λ_F depends both on the order $<$ and on the metric d, but it is invariant under rescaling and, furthermore, has the same invariances as d.

Example 3.2. Suppose that $M = 2m$, d is Euclidean distance, and define

$$F_M^{\max}(\xi) = \begin{cases} m + k & \text{if } \xi = 2k,\ 0 \leqslant k \leqslant m-1, \\ k & \text{if } \xi = 2k+1,\ 0 \leqslant k \leqslant m-1, \end{cases}$$

on $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$. The discrete Lyapunov exponent of $F_M^{\max}$ is

$$\lambda_{F_M^{\max}} = \frac{m}{2m-1} \ln m + \frac{m-1}{2m-1} \ln(m+1).$$

Observe for further reference that $\lim_{M\to\infty} \lambda_{F_M^{\max}} = \infty$.

Theorem 3.3. *(See [17].) Let I be a one-dimensional interval and $f : I \to I$ a chaotic map with respect to the measure μ, whose derivative is piecewise continuous. Then $\lim_{M\to\infty} \lambda_{F_M} = \lambda_f$, where*

$$\lambda_f = \int_I \ln\bigl|f'(x)\bigr|\, d\mu(x)$$

is the Lyapunov exponent of f.

From the results in [18] and [19] it can be proved that if $|f'| \leqslant C$, then

$$|\lambda_{F_M} - \lambda_f| \leqslant \frac{C}{M}.$$

The generalization of Theorem 3.3 to chaotic maps on higher-dimensional intervals requires the introduction of the discrete Lyapunov exponent of order $\nu = 1, 2, \ldots$; see [14] for details.

Given a family of permutations $(\mathbb{Z}_M, F_M)$, how can be decided whether they are chaotic cryptographic primitives, i.e., whether there a chaotic map f exists such that F_M is generated by f in the way explained above? In virtue of Theorem 3.3, a necessary condition is $0 < \lim_{M\to\infty} \lambda_{F_M} < \infty$. In particular, this excludes those families of permutations (like $(\mathbb{Z}_M, F_M^{\max})$) such that $\lim_{M\to\infty} \lambda_{F_M} = \infty$. On the other hand, given a family of permutations $(\mathbb{Z}_M, F_M)$ generated by a chaotic map f

on, say, $[0,1]$, it is impossible, in general, to recover f since, on the way from f to F_M, essential information on f gets lost. Only in cases similar to Example 2.2, in which each F_M has been gained via a uniform partition $X_\Delta = \{I_i\colon\ 0 \leqslant i \leqslant N(\Delta) - 1\}$, $M \leqslant N(\Delta)$, and the action of F_M is known on $\{0, 1, \ldots, N(\Delta) - 1\}$ for a sequence $N(\Delta) \to \infty$, we can reverse the recipe (1),

$$f_\Delta(I_i) = \frac{n_j}{M} \quad \text{if } F_M(i) = j,$$

and reconstruct $([0,1], f)$ by means of the discrete approximations (X_Δ, f_Δ) in the usual way.

Definition 3.4. We say that the family of permutations $(\mathbb{Z}_M, F_M)$ is discretely chaotic if $0 < \lim_{M\to\infty} \lambda_{F_M} < \infty$.

This definition can be generalized to non-bijective maps on ordered sets; see [14] for details.

It can be proven [14] that $\lambda_{F_M} \leqslant \lambda_{F_M^{\max}}$ for all permutations F_M on $\mathbb{Z}_M = \{0, 1, \ldots, M-1\}$ endowed with Euclidean distance $d(i,j) = |i - j|$. Thus, we may claim that $F_M^{\max}$ is the ‘most discretely chaotic’ map on $(\mathbb{Z}_M, <, |\cdot|)$ in the sense that its discrete Lyapunov exponent takes the largest possible value—but $(\mathbb{Z}_M, F_M^{\max})$ is not a chaotic cryptographic primitive because $\lim_{M\to\infty} \lambda_{F_M} = \infty$. We come to the conclusion that discretization and truncation of chaotic orbits cannot deliver the most discretely chaotic permutations—at least on $(\mathbb{Z}_M, <, |\cdot|)$. This no-go result sets a kind of theoretical limit to the possibilities of chaotic cryptography.

4. Examples of chaotic primitives

In this section, we present some typical chaotic primitives that, furthermore, are used in ciphers proposed in the literature.

4.1. Finite-state tent map

For a positive integer $M \geqslant 2$ and $a \in \mathbb{R}$ with $0 < a < M$, let $f_a\colon [0, M] \to [0, M]$ be the rescaled skew tent map

$$f_a(x) = \begin{cases} \frac{x}{a} & (0 \leqslant x \leqslant a), \\ \frac{M-x}{M-a} & (a \leqslant x \leqslant M). \end{cases}$$

The map f_a is one-dimensional, exact, and therefore mixing and ergodic. Its Lyapunov exponent λ_{f_a} is given by

$$\lambda_{f_a} = -\frac{a}{M} \ln \frac{a}{M} - \frac{M-a}{M} \ln \frac{M-a}{M}.$$

For a hash function based on the (discretization) of the tent map, see [20].

The *finite-state tent map* $F_{A,M}\colon \{1, 2, \ldots, M\} \to \{1, 2, \ldots, M\}$ is the bijection defined as

$$F_{A,M}(\xi) \equiv \begin{cases} \left\lceil \frac{M}{A}\xi \right\rceil & (1 \leqslant \xi \leqslant A), \\ \left\lfloor \frac{M}{M-A}(M-\xi) \right\rfloor + 1 & (A \leqslant \xi \leqslant M), \end{cases}$$

where A takes integer values in $\{1, 2, \ldots, M\}$. The inverse of $F_{A,M}$ is calculated as

$$F_{A,M}^{-1}(\eta) \equiv \begin{cases} \xi_1 & \text{if } \theta(\eta) = \eta,\ \frac{\xi_1}{A} > \frac{M-\xi_2}{M-A}, \\ \xi_2 & \text{if } \theta(\eta) = \eta,\ \frac{\xi_1}{A} \leqslant \frac{M-\xi_2}{M-A}, \\ \xi_1 & \text{if } \theta(\eta) = \eta + 1, \end{cases}$$

where

$$\xi_1 \equiv \left\lfloor \frac{A}{M}\eta \right\rfloor, \qquad \xi_2 \equiv \left\lceil \left(\frac{A}{M} - 1\right)\eta + M \right\rceil$$

and

$$\theta(\eta) \equiv \eta + \left\lfloor \frac{A}{M}\eta \right\rfloor - \left\lceil \frac{A}{M}\eta \right\rceil + 1.$$

The encryption and decryption functions are $F_{A,M}^{n}(\xi)$ and $F_{A,M}^{-n}(\eta)$, respectively, where n is the numbers of rounds.

4.2. Finite-state Chebyshev maps

The Chebyshev polynomial maps $T_n\colon \mathbb{R} \to \mathbb{R}$ of degree $n = 0, 1, \ldots$ are defined the recursion

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

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

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

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

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

and Lyapunov exponent $\ln n > 0$ 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:

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

The *finite-state Chebyshev map* $F_{n,M}\colon \{0, 1, \ldots, M-1\} \to \{0, 1, \ldots, M-1\}$, $M \in \mathbb{N}$, is defined as

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

The semi-group property of the finite-state Chebyshev maps can be used in key-exchange protocols or even in public-key algorithms [21].

4.3. Finite-state n-dimensional torus automorphisms

An automorphism of the n-torus $\mathbb{R}^n/\mathbb{Z}^n$ is implemented by an $n \times n$ matrix U_n with integer entries and determinant ±1. The requirement that the matrix U_n has integer entries ensures that U_n maps the torus into itself. The requirement that the determinant of the matrix U_n is ±1 guarantees invertibility. U_n is strong mixing if none of its eigenvalues is a root of unity.

The logarithm of the largest eigenvalue of U_n coincides with the Lyapunov exponent of the automorphism (with respect to Lebesgue measure). Torus automorphisms are typically used in diffusion layers (i.e., to spread local changes).

The n-torus automorphism

$$y = U_n x \pmod 1,$$

where $x, y \in [0,1]^n$, generates the *finite-state n-torus map*

$$\eta = U_n \xi \pmod M,$$

where $M \in \mathbb{N}$ and $\xi, \eta \in (\mathbb{Z}_M)^n$. As an example, consider the family of 2-dimensional *cat maps*

$$\begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix} = \begin{pmatrix} g+1 & g \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} \pmod{256},$$

where $\xi_1, \xi_2, \eta_1, \eta_2, g \in \mathbb{Z}_{256}$. The special case $g = 1$ is known as the *pseudo-Hadamard transform* (PHT),

$$H_2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$

and it is used in various cryptosystems because it requires only two additions in a digital processor.

Finite-state maps of the 2- and 4-torus have been proposed in the literature for the diffusion layers of, for instance, 8-byte Feistel ciphers whose half-round function acts on 4-byte blocks [22]. A half-round consists of four chaotic 4 × 4 S-boxes, each one built by interleaving the PHT and the 4-byte Hadamard-type permutation

$$R_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

in the form

$$\begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \eta_4 \end{pmatrix} = H_4 R_4 H_4 \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \\ \xi_4 \end{pmatrix} \pmod{256},$$

where

$$H_4 = \begin{pmatrix} H_2 & 0 \\ 0 & H_2 \end{pmatrix}.$$

The *branch number* and the minimal Euclidean stretching of this sort of mixing transformations (or layers) were studied in [22]. The branch number is the sum of the number of active input S-boxes and the number of active output S-boxes, minimized over the input space; it is an important parameter in differential cryptanalysis.

Affine transformations on the n-torus in chaos synchronization-based cryptography have been studied in [23]. As mentioned in the introduction, these maps have the nice property that the precision of the initial point does not degrade along its orbit.

4.4. *Substitutions based on the approximation of mixing maps*

From the mathematical point of view, a block cipher is a family of permutations on binary vectors, parameterized by the key. Alternatively, we may focus only on the permutations defined by some components of the cipher like, most notably, square substitution boxes. Thus, let F_n be a permutation of n-bit blocks (or an $n \times n$ 'S-box'). Define the linear approximation probability of F_n (LP_{F_n} for short) as

$$\mathrm{LP}_{F_n} = \max_{\alpha, \beta \neq 0} \mathrm{LP}_{F_n}(\alpha, \beta),$$

where

$$\mathrm{LP}_{F_n}(\alpha, \beta) = (2p-1)^2 = 4\left(p - \frac{1}{2}\right)^2,$$
$$p = \frac{\#\{\xi \in \mathbb{Z}_2^n \colon \xi \circ \alpha = F_n(\xi) \circ \beta\}}{2^n}$$

and $\xi \circ \alpha := \xi_1\alpha_1 \oplus \cdots \oplus \xi_n\alpha_n$ is the parity of the bitwise product of ξ and α (and analogously for $F_n(\xi) \circ \beta$). Next, define the differential approximation probability of F_n (DP_{F_n} for short) as

$$\mathrm{DP}_F = \max_{\alpha \neq 0, \beta} \mathrm{DP}_F(\alpha, \beta),$$

where α is the so-called input difference, β the output difference and

$$\mathrm{DP}_F(\alpha, \beta) = \frac{\#\{\xi \in \mathbb{Z}_2^n \colon F(\xi) \oplus F(\xi \oplus \alpha) = \beta\}}{2^n}.$$

Here $\xi \oplus \alpha = (\xi_1 \oplus \alpha_1, \ldots, \xi_n \oplus \alpha_n)$ denotes the componentwise XOR (or vector addition modulo 2) of the n-bit blocks ξ and α (and analogously for $F(\xi) \oplus F(\xi \oplus \alpha)$); see [24] for details. LP_{F_n} and DP_{F_n} measure the immunity of the block cipher F_n to attacks mounted on linear and differential cryptanalysis, respectively, immunity being higher the smaller their values. In [24] we have shown that if F_n is a cyclic periodic approximation of a mixing automorphism F and some assumptions are fulfilled, then LP_{F_n} and DP_{F_n} get asymptotically close to their greatest lower bounds $1/2^n$ and $1/2^{n-1}$, respectively, thus obtaining an arbitrarily close-to-optimal immunity to both cryptanalyses—the faster the approximation of F_n to F, the higher the immunity of the permutation F_n [24]. Therefore, we have proven, as suggested by Shannon, that, in principle, mixing transformations may indeed be used in encryption systems. Unfortunately, the proofs are non-constructive so that one has to content oneself with heuristic implementations of the underlying idea.

As an example, consider the 2-torus automorphism $U_2 = (t_{ij})$ with

$$t_{11} = 587943273, \qquad t_{12} = 185921552200509715,$$
$$t_{21} = 2, \qquad t_{22} = 632447247.$$

For this chaotic map, the corresponding (heuristic) periodic approximation with $n = 18$ has the following values of DP and LP: $\mathrm{LP} = 0.00002629$ with $|\mathrm{LP} - 2^{-18}| = 2.25 \times 10^{-5}$, and $\mathrm{DP} = 0.00003052$ with $|\mathrm{DP} - 2^{-17}| = 2.29 \times 10^{-5}$ [24].

5. Final remarks and conclusions

In this Letter we have proposed some theoretical concepts underlying digital chaos-based cryptography and presented some basic implementations of chaotic cryptographic primitives. Needless to say, our exposition is far from exhaustive, being rather meant as a general view of what is going on in a field of rapid growth. Also for this reason, we have renounced to present here more recent developments in chaotic cryptology, since time is needed to asses their security.

To complete the picture, some words of caution are in order here. Although, at theoretical level, it seems that chaotic systems are ideal candidates for cryptographic primitives (remember, for example, that periodic approximations of mixing automorphisms have arbitrary close to optimal immunity to linear and differential cryptanalysis, Section 4.4), at the practical level, chaotic ciphers are still slower than the corresponding conventional ones. Thus, the public-key cipher proposed in [21], based on the finite-state Chebyshev map, is slower than RSA, and the 128-bit block cipher proposed in [22], that includes sixteen 8×8 S-boxes (all the same) designed with the finite-state tent map and a finite-state 4-dimensional torus map as chaotic mixing transformation, is also slower than the best conventional algorithms, such as AES. In connection with this, let us remind that we showed in Section 3 that chaotic cryptographic primitives cannot be the most discretely chaotic permutations in the sense of Definition 3.4. Since this result is of asymptotic nature, we believe that it has no practical consequences but, nevertheless, it does put limits (if theoretical) to chaotic cryptography.

We may conclude that reaching the same standards of security and speed as in conventional cryptography, should be the priority of chaotic cryptography in the next future.

Acknowledgements

The authors are very thankful to the referees for their constructive criticism. This work was partially funded by the Spanish Ministry of Science and Education (Ref. MTM2005-04948) and by European Funds FEDER.

References

[1] K.M. Cuomo, A.V. Oppenheim, S.H. Strogatz, IEEE Trans. Circuits Systems II 40 (1993) 626.
[2] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, A. Shang, Int. J. Bifur. Chaos 2 (1992) 973.
[3] Z.P. Jiang, IEEE Trans. Circuits Systems I 49 (2002) 92.
[4] G. Millerioux, J. Daafouz, IEEE Trans. Circuits Systems I 50 (2003) 1270.
[5] G. Alvarez, S. Li, Int. J. Bifur. Chaos 16 (2006) 2129.
[6] M.S. Baptista, Phys. Lett. A 240 (1998) 50.
[7] R. Schmitz, J. Franklin Inst. 338 (2001) 429.
[8] G. Jakimoski, L. Kocarev, IEEE Trans. Circuits Systems I 48 (2001) 163.
[9] L. Kocarev, IEEE Circuits Systems Magazine 1 (2001) 6.
[10] L. Kocarev, G. Jakimoski, IEEE Trans. Circuits Systems I 50 (2003) 123.
[11] R. Tenny, L.S. Tsimring, L. Larson, H.D.I. Abarbanel, Phys. Rev. Lett. 90 (2003) 047903.
[12] R. Mislovaty, E. Klein, I. Kanter, W. Kinzel, Phys. Rev. Lett. 91 (2003) 118701.
[13] L. Kocarev, M. Sterjev, P. Amato, in: Proceeding of ISCAS 2004, vol. IV, pp. 578–581.
[14] L. Kocarev, J. Szczepanski, J.M. Amigó, I. Tomovski, IEEE Trans. Circuits Systems I 53 (2006) 1300.
[15] D.E. Knuth, The Art of Computer Programming, vol. 2, Addison–Wesley, Reading, MA, 1998.
[16] I.P. Cornfeld, S.V. Fomin, Y.G. Sinai, Ergodic Theory, Springer, New York, 1982.
[17] J.M. Amigó, L. Kocarev, J. Szczepanski, Phys. Lett. A 355 (2006) 27.
[18] L. Kocarev, J. Szczepanski, Phys. Rev. Lett. 93 (2004) 234101.
[19] J.M. Amigó, J. Szczepanski, Int. J. Bifur. Chaos 13 (2003) 1937.
[20] X. Yi, IEEE Trans. Circuits Systems II 52 (2005) 354.
[21] L. Kocarev, M. Sterjev, A. Fekete, G. Vattay, Chaos 14 (2004) 1078;
L. Kocarev, J. Makraduli, P. Amato, Circuits Systems Signal Process. 24 (2005) 497.
[22] N. Masuda, G. Jakimoski, K. Aihara, L. Kocarev, IEEE Trans. Circuits Systems I 53 (2006) 1341.
[23] L. Rosier, G. Millerioux, G. Bloch, Systems Control Lett. 55 (2006) 223.
[24] J. Szczepanski, J.M. Amigó, T. Michalek, L. Kocarev, IEEE Trans. Circuits Systems I 52 (2005) 443.