2005 International Symposium on Nonlinear
Theory and its Applications (NOLTA2005)
Bruges, Belgium, October 18-21, 2005

# Chaos-based Cryptography: an overview

Ljupco Kocarev[1], José M. Amigó[2], and Janusz Szczepanski[3]

[1]1 Institute for Nonlinear Science
University of California San Diego
9500 Gilman Drive, La Jolla, CA 92093–0402, USA
Email: lkocarev@ucsd.edu
[2] Centro de Investigación Operativa,
Universidad Miguel Hernández, 03202 Elche, Spain.
[3] Institute for Fundamental Technological Research,
Polish Academy of Sciences, Swietokrzyska 21, PL-00-049 Warsaw, Poland.

**Abstract**—We review some of the recent work on chaos-based cryptography. We argue that if a chaotic map $f$ is used in cryptography, then it should be implemented as a bijection $F_M : D \to D$, where $D$ is a finite set with cardinality $M$, such that, for large $M$, $F_M$ 'approximates well' the chaotic map $f$. Several examples, including chaotic block cypher and chaotic public-key encryption algorithm, are given.

## 1. Introduction

The research on network security has considerably grown in the last decade. There is a need for using cryptographic tools (algorithms, protocols, etc.) in order to ensure privacy in data transfer among users. Recently, new cryptographic techniques based on *chaos theory* have been developed [1, 2, 3, 4, 5, 6]. In this paper we review our recent work on chaos-based cryptography.

Chaotic systems are defined on real numbers. Any encryption algorithm which uses chaotic maps when implement on a computer (finite-state machine) becomes a transformation from a finite set onto itself. Because of its wide dynamic range, the floating-point implementation seems to be the most appropriate for software realizations (implementation) of chaotic maps. However, there are two reasons for not using floating-point arithmetic in chaos-based cryptography. First, floating-point numbers are not uniformly distributed over any given interval of the real axis [7]. Furthermore, one may observe the existence of redundant number representations. Indeed, due to the normalized calculations in floating-point arithmetic, some floating-point numbers represent the same real signal value. Second, the authors think the most important reason, there are no analytical tools for understanding the periodic structure of the periodic orbits in the floating-point implementation of chaotic maps (when implement on a computer all chaotic maps are periodic: all trajectories are eventually periodic). On the other hand, when using integers one may hope if a possible link between number theory and chaos theory has been established, as in the case of the toral automorphisms, to understand the structure of the orbits.

## 2. Chaotic cryptographic primitives

Let $f : S \to S$ be an $N$-dimensional chaotic map. For simplicity, we assume that the phase space $S$ is either an $N$-dimensional cube $[0,1]^N$ or an $N$-dimensional torus. Let $F_M : \{0,1,\dots M-1\}^N \to \{0,1,\dots M-1\}^N$ be a bijection which is generated from $f$ (we do not specify here how $F_M$ is defined, however some examples will be presented bellow).

**Definition 2.1** *We say that $F_M$ is a chaotic cryptographic primitive if for large $M$, $F_M$ approximates well the chaotic map $f$.*

Although the above definition is intuitive, it does not say anything unless the phrase *approximates well* is precisely defined. However, this is beyond the scope of the paper, and therefore, we present only examples.

**Example 2.2** *Let $D = \{0/M, 1/M, \dots (M-1)/M\}^N$ and*

$$f_M : D \to D$$

*be a bijection induced by $f$ when the phase space $[0,1]^N$ is discretized (quantized) with $\{0/M, \dots, (M-1)/M\}^N$. We assume that as the discretization becomes finer, or as $M$ goes to infinity, $f_M$ approaches $f$; in this sense, we say $f_M$ approximates well $f$. Clearly, the map $f_M$ induces a map $F_M : \{0,1,\dots M-1\}^N \to \{0,1,\dots,M-1\}^N$ in a natural way.*

**Example 2.3** *Let $X$ be a set, $\mathcal{A}$ a $\sigma$-algebra of subsets of $X$ and $\mu$ a positive measure on $(X,\mathcal{A})$. Suppose $T$ is an automorphism of the space $(X,\mathcal{A},\mu)$, i.e., $T$ is a one-to-one map of $X$ onto itself such that, for all $A \in \mathcal{A}$, we have $TA$, $T^{-1}A \in \mathcal{A}$ and $\mu(A) = \mu(TA) = \mu(T^{-1}A)$. We consider sequences of finite partitions $\{\mathcal{P}_n\}$ of the space $X$ and sequences of automorphisms $\{T_n\}$ such that $T_n$ preserves $\mathcal{P}_n$. The automorphism $T_n$* preserves the partition *$\mathcal{P}_n$, if it sends every element of $\mathcal{P}_n$ into an element of the same partition.*

*An automorphism $T$ of the space $(X,\mathcal{A},\mu)$ possesses an approximation by periodic transformations with speed*

*$f(n)$, if there exists a sequence of automorphisms $T_n$ preserving $\mathcal{P}_n$ such that*

$$\sum_{k=1}^{q_n} \mu(TP_k^{(n)} \triangle T_n P_k^{(n)}) < f(q_n), \quad n = 1, 2, \ldots.$$

*where $\triangle$ stands for symmetric set difference and $f$ is a function on the integers such that $f(n) \to 0$ monotonically.*

**Definition 2.4** *We say that a cipher (block cipher, stream cipher, or public-key algorithm) is chaotic if its building blocks (for example, S-boxes, diffusion transformations, one-way functions, and so on) are chaotic cryptographic primitives.*

## 3. Examples of chaotic primitives

### 3.1. Finite-state tent map

For a positive integer $M \geq 2$, let $f_A : [0, M] \to [0, M]$, $0 < A < M$ be a re-scaled skew tent, defined as

$$F_A = \begin{cases} X/A, & (0 \leq X \leq A), \\ (M - X)/(M - A), & (A < X \leq M). \end{cases}$$

The map $F_A$ is one-dimensional, exact, and therefore mixing and ergodic. The Lyapunov exponent $\lambda$ is given by

$$\lambda = -\frac{A}{M} \log \frac{A}{M} - \frac{M - A}{M} \log \frac{M - A}{M}. \tag{1}$$

The finite-state tent map $F_A : \{1, 2, \ldots M\} \to \{1, 2, \ldots M\}$ is defined as

$$F_A(X) \equiv \begin{cases} \left\lceil \frac{M}{A} X \right\rceil, & (1 \leq X \leq A), \\ \left\lfloor \frac{M}{M-A}(M - X) \right\rfloor + 1, & (A < X \leq M). \end{cases} \tag{2}$$

Note that $F_A$ is a bijection.

### 3.2. Finite-state Chebyshev maps

Chebyshev polynomial map $T_p : R \to R$ of degree $p$ is defined using the following recurrent relation:

$$T_{p+1}(x) = 2xT_p(x) + T_{p-1}(x), \tag{3}$$

with $T_0 = 1$ and $T_1 = x$. The interval $[-1, 1]$ is invariant under the action of the map $T_p$: $T_p([-1, 1]) = [-1, 1]$. Therefore, the Chebyshev polynomial restricted to the interval $[-1, 1]$ is a well-know chaotic map for all $p > 1$: it has a unique absolutely continuous invariant measure with positive Lyapunov exponent $\ln p$. For $p = 2$, the Chebyshev map reduces to the well-know logistic map. Finite-state Chebyshev map $F_p : \{0, 1, \ldots, N - 1\} \to \{0, 1, \ldots, N - 1\}$ is defined as:

$$y = T_p(x) (\mathrm{mod} N), \tag{4}$$

where $x$ and $N$ are integers.

### 3.3. Finite-state two-dimensional torus automorphisms

Another prototype of a chaotic map is a torus automorphism. An automorphism of the two-torus is implemented by $2 \times 2$ matrix $M$ with integer entities and determinant $\pm 1$. The requirement that the matrix $M$ has integer entities ensures that $M$ maps torus into itself. The requirement that the determinant of the matrix $M$ is $\pm 1$ guarantees invertibility.

Let $M$ be a 2-torus automorphism

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = M \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ 1), \tag{5}$$

where $x, y \in [0, 1]$. Let $2k$ be the trace (which is an integer) of the automorphism $M$. It is well-known that for $k > 1$ (we will consider only positive $k$) that the automorphism $M$ has strong chaotic properties, and in particular, it has a dense set of unstable periodic orbits.

Finite-state 2d torus map is defined as

$$\begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} = \begin{pmatrix} g + 1 & g \\ 1 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} \mod 256, \tag{6}$$

where $X_1, X_2, Y_1, Y_2 \in P_S$, and $P_s = \{0, 1, \ldots, 255\}$. This map can serve as a diffusion layer because its inverse is well-defined on the integer space on which cryptographical transformations are based. A special case $g = 1$ is known as the pseudo-Hadamard transform (PHT). The PHT is used in various cryptosystems because it requires only two additions in a digital processor.

An example of a finite-state four-dimensional torus is given by:

$$\begin{pmatrix} Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{pmatrix} = G \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \end{pmatrix} \mod 256, \tag{7}$$

where $X_i, Y_i \in P_S$ $(1 \leq i \leq 4)$ and $G = (g_{ij})$, $0 \leq g_{ij} \leq 255$ $(1 \leq i, j \leq 4)$.

## 4. Examples of chaotic encryption algorithms

### 4.1. Substitutions based on the approximation of mixing maps

Let $F$ be a permutation of $n$-bit blocks and, as usual, denote by $LP_F$ and $DP_F$ the linear approximation probability and differential approximation probability of $F$, respectively (see [8] for precise definitions of these 'probabilities'). $LP_F$ and $DP_F$ measure the immunity of the block cipher $F$ to attacks mounted on the corresponding cryptanalysis, immunity being higher the smaller their values. In [8] we have shown that if $F$ is a cyclic periodic approximation of a mixing automorphism and some assumptions are fulfilled, then $LP_F$ and $DP_F$ 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. Therefore, we have proven, as suggested by Shannon, that mixing transformations may indeed be used in encryption systems, providing an alternative to the traditional algebraic methods.

As an example we consider the 2D torus chaotic map, for which the elements of the matrix $M = (m_{ij})$ are

$$m_{11} = 587943273, \quad m_{12} = 185921552200509715,$$
$$m_{21} = 2, \quad m_{22} = 632447247.$$

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

### 4.2. Public-key encryption algorithm

Finite-state Chebyshev map has been recently suggested for generalization of RSA public-key encryption algorithm. The algorithm consists of two algorithms: algorithm for key generation and algorithm for encryption.

*Algorithm for key generation.* Alice should do the following:

1. Generate two large random (and distinct) primes $p$ and $q$, each roughly the same size.
2. Compute $N = pq$ and $\phi = (p^2 - 1)(q^2 - 1)$.
3. Select a random integer $e$, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Compute the unique integer $d$, $1 < d < \phi$, such that $ed \equiv 1 (\mathrm{mod} \phi)$.
5. Alice's public key is $(N, e)$; Alice's private key is $d$.

*Algorithm for encryption.*

1. Encryption. To encrypt a message $m$, Bob should do the following:
   (a) Obtain Alice's authentic public key $(N, e)$.
   (b) Represent the message as an integer in the interval $[1, N - 1]$.
   (c) Compute $c = T_e(m) (\mathrm{mod} N)$ and send to Alice.
2. Decryption. To recover the message $m$ from $c$, Alice should do the following:
   (a) Use the private key $d$ to recover $m = T_d(c) (\mathrm{mod} N)$.

The following property of the finite-state Chebyshev map holds:

$$T_d(T_e(x)) \equiv x (\mathrm{mod} N).$$

This is the crucial property used for design public-key encryption algorithm based on finite-state Chebyshev map, see [9] for details.

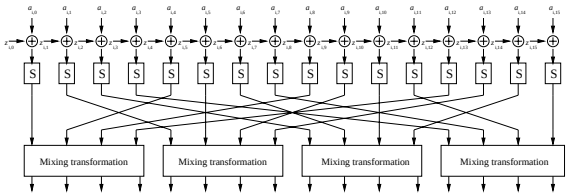


Figure 1: Round function of the 128-bit uniform cipher: each $a_{1,i}$ $0 \le i \le 15$, is a byte, and the mixing transformation has branch number 4.

### 4.3. Block cipher

Recently we have designed a 128-bit chaotic block cipher with the S-boxes defined with the finite tent map and chaotic mixing transformation defined as finite-state 4-dimensional torus map [10]. Consider a 128 bit uniform cipher given in Figure 1 for which the mixing transformation has branch number 4, for the definition of branch number see [10]. We also consider the Feistel cipher with block diagram shown in Figure 2, where the $F$ function is given in Figure 3. The following theorems are proven in [10]:

**Theorem 4.1** *Every 4-round differential trail of the uniform cipher has at least 16 active S-boxes.*

**Theorem 4.2** *Every 4-round differential trail of the Feistel cipher has at least 10 active S-boxes.*

As calculated in [10], the values of $DP$ and $LP$ for the chaotic S-box are $DP \le 2^{-4}$ and $LP \le 2^{-3}$, respectively. We suggest that the cipher has 16 rounds. With the help of Theorems 4.1 and 4.2, we can estimate the values of $DP$ and $LP$ for the whole cipher.

- *Chaotic uniform cipher* – For the uniform cipher with block diagram shown in Figure 1, we have $DP \le 2^{-256}$ and $LP \le 2^{-192}$.
- *Chaotic Feistel cipher* – For the Feistel cipher with block diagram shown in Figure 2, where the $F$ function is given in Figure 3, we have $DP \le 2^{-160}$ and $LP \le 2^{-120}$.

For an $8 \to 8$ S-box one has $DP \ge 2^{-7}$ and $LP \ge 2^{-8}$. We did not attempt to optimize the values of $DP$ and $LP$ for a chaotic S-box and used $DP \le 2^{-4}$ and $LP \le 2^{-3}$. However, different approaches yield chaos-based S-boxes with $DP \le 2^{-5}$ and $LP \le 2^{-5}$ [8].

## 5. Conclusions

In this work we have summarized our recent work on chaos-based cryptography. Although at theoretical level it seems that chaotic systems are ideal candidates for cryptographic primitives (see for example the statement proven in [8] that periodic approximations of mixing maps have

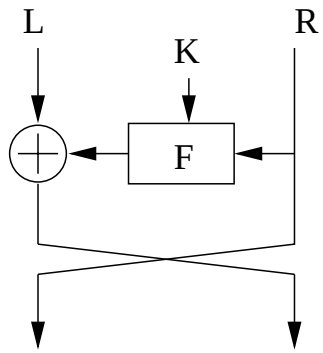


Figure 2: Feistel structure

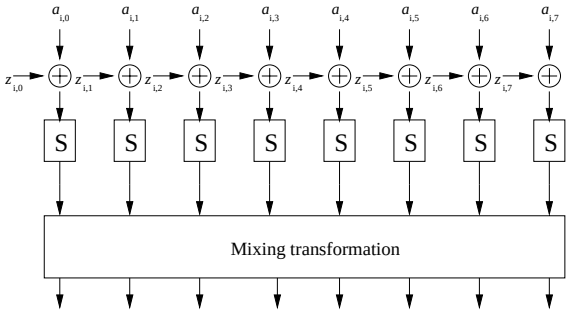


Figure 3: The $F$ function of the 128-bit Feistel cipher: each $a_{i,k}$, $0 \le k \le 7$, is a byte, and the mixing transformation has a branch number 4.

arbitrary close to optimal immunity to linear and differential cryptanalysis), at the practical level chaotic maps are still slower than corresponding conventional cryptographic algorithms. Thus, for example, chaos-based pubic key algorithm suggested in [9] is slower than RSA, and block encryption algorithm proposed in [10] is also slower than the best conventional algorithms, such as AES.

**Acknowledgments**

LK is grateful to K. Aihara, G. Jakimoski, and N. Masuda for stimulating discussions. This research is supported in part by the NSF.

**References**

[1] G. Jakimoski and L. Kocarev, "Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps," IEEE Trans. on Circuits and Systems, Part I, Vol. 48(2), 2001, pp. 163 – 169.

[2] L. Kocarev, "Chaos-Based Cryptography: a Brief Overview," (Invited paper), IEEE Circuits and Systems Magazine, Vol. 1(3), 2001, pp. 6 – 21.

[3] L. Kocarev and G. Jakimoski, "Unpredictable Pseudo-Random Bits Generated by Chaotic Maps," IEEE Trans. on Circuits and Systems, Part I, 2003.

[4] R. Tenny, L. S. Tsimring, L. Larson, and H. D. I. Abarbanel, "Using Distributed Nonlinear Dynamics for Public Key Encryption," Phys. Rev. Lett. **90**, 047903 (2003);

[5] R. Mislovaty, E. Klein, I. Kanter, and W. Kinzel, "Public Channel Cryptography by Synchronization of Neural Networks and Chaotic Maps," Phys. Rev. Lett. **91**, 118701 (2003);

[6] L. Kocarev, M. Sterjev, and P. Amato, "RSA encryption algorithm based on torus automorphism," Proceeding of ISCAS 2004, vol. IV, 2994, pp. 578 – 581.

[7] D. E. Knuth, *The Art of Computer Programming*, Reading, MA: Addison Wesley, 1998, vol. 2.

[8] J. Szczepanski, J.M. Amigo, T. Michalek, and L. Kocarev, "Cryptographically secure substitutions based on the approximation of mixing maps," IEEE Transactions on Circuits and Systems, VOL. 52, NO. 2, FEBRUARY 2005 443 - 453

[9] L. Kocarev, M. Sterjev, A. Fekete and G. Vattay, "Public-key Encryption with Chaos," CHAOS, Vol 14 (4) pp. 1078 - 1082, 2004; L. Kocarev, J. Makraduli, and P. Amato, "Public-Key Encryption Based on Chebyshev Polynomials," Circuits, Systems and Signal Processing, in press.

[10] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic Ciphers: from theory to practical algorithms," IEEE Transactions on Circuits and Systems, in press.