



On some properties of the discrete Lyapunov exponent

José M. Amigó^{a,*}, Ljupco Kocarev^{b,c}, Janusz Szczepanski^d

^a Centro de Investigación Operativa, Universidad Miguel Hernández Avda. de la Universidad s/n. 03202 Elche, Spain

^b Macedonian Academy of Sciences and Arts, Skopje, Macedonia

^c Institute for Nonlinear Science, University of California San Diego, 9500 Gilman Drive. La Jolla, CA 92093-0402, USA

^d Institute of Fundamental Technological Research, Polish Academy of Sciences, Swietokrzyska 21, 00-049 Warsaw, and Kazimierz Wielki University in Bydgoszcz, Poland

ARTICLE INFO

Article history:

Received 25 April 2008

Received in revised form 23 July 2008

Accepted 29 July 2008

Available online 23 August 2008

Communicated by C.R. Doering

ABSTRACT

One of the possible by-products of discrete chaos is the application of its tools, in particular of the discrete Lyapunov exponent, to cryptography. In this Letter we explore this question in a very general setting.

© 2008 Elsevier B.V. All rights reserved.

1. Introduction

In [1] some of the present authors laid the foundations of what we call *discrete chaos*—a formal approach to the idea that maps on finite sets (say, finite-state approximations of chaotic maps) may have different diffusion and mixing properties. Along with the theoretical framework, the main tool of discrete chaos presented there was the *discrete Lyapunov exponent*, a quantity defined for any bijection on a discrete and linearly ordered subset of a metric space. The connection between the greatest Lyapunov exponent of a chaotic map f in d dimensions and the discrete Lyapunov exponent of the bijection obtained from f via discretization and truncation of typical orbits, was also studied in [1]; in the one-dimensional case, in which this relation is simplest to state, the discrete Lyapunov exponent converges to its continuous counterpart in the ‘continuous limit’, i.e., when the discretization gets finer and, consequently, the length of the orbit goes to infinity. A similar property holds also for the *discrete entropy*, another tool of discrete chaos introduced in [2].

Permutations of comparatively large numbers of elements are typically used in chaotic cryptography as primitives, where they arise as discretizations of chaotic maps [3]. It is therefore natural to use chaotic cryptography as a testbed of the tools of discrete chaos. An interesting proposal along these lines was made in [4]: to use the discrete Lyapunov exponent for selecting permutations resistant to differential cryptanalysis. Rather than proposing further potential usages of the discrete Lyapunov exponent, we will explore in this Letter some basic properties and a few related topics that bear upon this question. Specifically, we examine in Section 3

those permutations that maximize the discrete Lyapunov exponent, and in Section 4, the statistical distribution of the discrete Lyapunov exponents of permutations randomly chosen. Finally, in Section 5 we discuss the previous results from the point of view of chaotic cryptography.

2. The discrete Lyapunov exponent

Let $\mathcal{S} = \{s_0, \dots, s_{M-1}\}$ be a linearly ordered finite set, $s_i < s_{i+1}$, endowed with a metric $d(\cdot, \cdot)$, and $\pi : \mathcal{S} \rightarrow \mathcal{S}$ be a bijection or, equivalently, an M -permutation. We define the *discrete Lyapunov exponent* (DLE) of π as

$$\lambda_\pi = \frac{1}{M} \sum_{i=0}^{M-1} \log \frac{d(\pi(s_i), \pi(s_{i+1}))}{d(s_i, s_{i+1})}, \quad (1)$$

where the definition of s_M , the right neighbor of s_{M-1} , depends on the ‘topology’ of \mathcal{S} . In the applications we will consider below, π will be a permutation on a finite subset \mathcal{S} of \mathbb{R} endowed with the Euclidean distance $d(s_i, s_j) = |s_i - s_j|$ and the standard order. The case $\mathcal{S} = \{0, 1\}^l$ (i.e., the set of binary strings of length l) lexicographically ordered and endowed with the Hamming distance, is also of interest in applications, but the limit of (1) when $N \rightarrow \infty$ is ill-defined. For an approach based on topological methods dealing with maps on binary states, see [5]. We will use natural logarithms to calculate λ_π .

Henceforth we assume without loss of generality that the M -permutation π is defined on $\{0, 1, \dots, M-1\}$, setting if necessary $\pi(i) = \pi(s_i)$ and $d(i, j) = d(s_i, s_j)$. Furthermore, anticipating the important case considered below that the integers $0, 1, \dots, M-1$ are added and multiplied modulo M , we set $\{0, 1, \dots, M-1\} = \mathbb{Z}_M$.

The justification for calling (1) a discrete Lyapunov exponent is as follows. Let $x_{j+1} = f(x_j)$, $j = 0, 1, \dots, M-1$, be a typical tra-

* Corresponding author.

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

jectory of length M of a chaotic self-map f of a one-dimensional interval I , such that $x_{j+1} \neq x_j$ for all j and $|x_{M-1} - x_0| < \varepsilon$. Define $f(x_{M-1}) = x_0$ and order x_0, x_1, \dots, x_{M-1} in I to obtain $x_{n_0} < x_{n_1} < \dots < x_{n_{M-1}}$, so as x_{n_i} and $x_{n_{i+1}}$ are neighbors in the metric sense. Furthermore, set $s_i = \lfloor x_{n_i} N \rfloor$, where N is chosen such that $s_i \neq s_j$ for all $i \neq j$. The map f induces then the obvious permutation

$$F_M(i) = j \quad \text{if } f(x_{n_i}) = x_{n_j}$$

on $(\mathbb{Z}_M, <, |\cdot|)$.

Theorem 1. (See [1].) Let I be a one-dimensional interval and $f : I \rightarrow I$ be a chaotic map with piecewise continuous derivative. Then $\lim_{M \rightarrow \infty} \lambda_{F_M} = \lambda_f$, where λ_f is the Lyapunov exponent of f .

In [1] the reader can also find a generalization of Theorem 1 to higher dimensions.

We reserve the notation F_M for permutations on $(\mathbb{Z}_M, <, |\cdot|)$ induced by interval maps $f : I \rightarrow I$ in the way explained above. Such permutations are commonly used in chaotic cryptography [3]. In this ‘linear’ case,

$$\lambda_{F_M} = \frac{1}{M} \sum_{i=0}^{M-1} \ln |F_M(r_i) - F_M(i)|,$$

where $r_i = i + 1$ for $0 \leq i \leq M - 2$ and we choose $r_{M-1} = M - 2$ as the right neighbor of $s_{M-1} = M - 1$. Other conventions for the right neighbor of the rightmost state are possible (see e.g. [3]), but they do not affect our present analysis.

Example 1. For the right shift modulo M , defined on $\mathbb{Z}_M = \{0, \dots, M - 1\}$ as $\theta_M(s) = s + 1$ for $s = 0, 1, \dots, M - 2$ and $\theta_M(M - 1) = 0$, we find

$$\lambda_{\theta_M} = \frac{2}{M} \ln(M - 1).$$

In [6, Theorem II.2] we proved that when $M = 2m$, the permutation

$$\Pi_{2m}(s) = \begin{cases} m + k & \text{if } s = 2k, \quad 0 \leq k \leq m - 1, \\ k & \text{if } s = 2k + 1, \quad 0 \leq k \leq m - 1, \end{cases} \quad (2)$$

on $\mathbb{Z}_{2m} = \{0, \dots, 2m - 1\}$ has the greatest possible DLE for a $2m$ -permutation, namely,

$$\lambda_{\Pi_{2m}} = \frac{m+1}{2m} \ln m + \frac{m-1}{2m} \ln(m+1). \quad (3)$$

For this reason, we will also use the notation

$$\lambda_{\Pi_{2m}} = \lambda_{2m}^{\max}. \quad (4)$$

In the next section we will see that Π_{2m} is quite different from the permutations F_{2m} .

3. Properties of Π_{2m}

The permutations Π_{2m} have some interesting properties that we touch upon in the following points 3.1–3.3.

3.1. From (4) and (3) we have:

$$\lambda_{2m}^{\max} \sim \ln m,$$

where \sim stands for ‘asymptotically as $m \rightarrow \infty$ ’. Thus, for m large, the maximal DLE of a permutation on $2m$ elements is approximately $\ln m$.

On the other hand, given any piecewise smooth, interval map f and a permutation $F_{2m} : \mathbb{Z}_{2m} \rightarrow \mathbb{Z}_{2m}$ induced by f , we have

$$\lambda_{F_{2m}} \sim \ln \lambda_f,$$

Table 1
Cycle decomposition of some Π_{2m}

$2m$	# cycles	Cycle lengths
46	2	23, 23
48	4	3, 3, 21, 21
50	7	2, 8, 8, 8, 8, 8, 8
52	1	52
54	4	4, 10, 20, 20
56	4	2, 18, 18, 18
58	1	58
60	1	60
62	12	2, 3, 3, 6, 6, 6, 6, 6, 6, 6, 6, 6

where λ_f is the Lyapunov exponent of f (Theorem 1). This means that the family of permutations Π_{2m} cannot be obtained by discretization and subsequent refinement of any single chaotic map.

The best we can do in this regard is, for each fixed m , to choose an interval map f such that $\lambda_{F_{2m}} \simeq \lambda_{2m}^{\max}$. For example, any piecewise linear interval map f with slopes $\pm m$ has (metric and topological) entropy $\ln m$, hence $\lambda_{F_{2m}} \sim \ln m$ according to Theorem 1.

3.2. Another difference between Π_{2m} and F_{2m} is their cycle structure. By construction, the permutations F_{2m} consist of a single cycle. Table 1 gives a flavor of the diversity of the cycle decomposition of Π_{2m} according to the value of $2m$. In the case of reducible permutations, we observe that the decomposition is, in general, quite uniform, with cycles of the same or similar lengths, or a few groups with that property. The same holds for much longer tables of cycle-decompositions of Π_{2m} , with m running into a few hundreds.

At this point, some definitions are in order. A permutation is said to be *irreducible* if it cannot be decomposed into disjoint cycles. Recall that the elements of \mathbb{Z}_D are the residual classes of \mathbb{Z} modulo D , whose least positive representatives are $\{0, 1, \dots, D - 1\}$; moreover, those $n, 1 \leq n \leq D - 1$, that are prime to D (i.e., the greatest common divisor of n and D is 1) build a complete set of representatives of the multiplicative group modulo D , which is denoted by \mathbb{Z}_D^* . Thus, the cardinality of \mathbb{Z}_D^* , $|\mathbb{Z}_D^*|$, is precisely the value $\phi(D)$ of Euler’s *totient function* ϕ , defined as the number of positive integers not greater than and prime to D . For example, if p is a prime number, then $\mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$, and $|\mathbb{Z}_p^*| = \phi(p) = p - 1$. An element $g \in \mathbb{Z}_D^*$ is called a *cyclic generator* of \mathbb{Z}_D^* if $\{g^n : 0 \leq n \leq \phi(D) - 1\} = \mathbb{Z}_D^*$ (where $g^0 = 1$), i.e., if the powers of g generate all of \mathbb{Z}_D^* . Finally, a *primitive root* for a modulus D is a cyclic generator of \mathbb{Z}_D^* .

Theorem 2. Π_{2m} is irreducible if and only if $2m + 1$ is a prime with primitive root 2 (i.e., if \mathbb{Z}_{2m+1}^* is cyclic and generated by 2).

Proof. The proof is easier if we consider the permutation $\tilde{\Pi}_{2m} : \{1, 2, \dots, 2m\} \rightarrow \{1, 2, \dots, 2m\}$, defined as $\tilde{\Pi}_{2m}(s) = \Pi_{2m}(s - 1) + 1$ i.e.,

$$\tilde{\Pi}_{2m}(s) = \begin{cases} k & \text{if } s = 2k, \quad 1 \leq k \leq m, \\ m + k + 1 & \text{if } s = 2k + 1, \quad 0 \leq k \leq m - 1. \end{cases}$$

Observe that $\lambda_{\tilde{\Pi}_{2m}} = \lambda_{\Pi_{2m}}$. The nice feature about $\tilde{\Pi}_{2m}$ is that its inverse, $\tilde{\Pi}_{2m}^{-1} : \{1, 2, \dots, 2m\} \rightarrow \{1, 2, \dots, 2m\}$, has a structure that allows us to easily recognize for which values of $2m$ it is irreducible. Indeed,

$$\tilde{\Pi}_{2m}^{-1}(s) = \begin{cases} 2s & \text{if } 1 \leq s \leq m, \\ 2s - (2m + 1) & \text{if } m + 1 \leq s \leq 2m. \end{cases}$$

It follows that the orbit of 1 under $\tilde{\Pi}_{2m}^{-1}$, $\mathcal{O}(1) = \{\tilde{\Pi}_{2m}^{-k}(1) : 0 \leq k \leq 2m - 1\}$, is given by

$$\mathcal{O}(1) = \{2^k \bmod(2m + 1) : 0 \leq k \leq 2m - 1\}. \quad (5)$$

Now, Π_{2m} is a cycle if and only if $\tilde{\Pi}_{2m}$ is a cycle if and only if $\tilde{\Pi}_{2m}^{-1}$ is a cycle (the cycles of $\tilde{\Pi}_{2m}$ and $\tilde{\Pi}_{2m}^{-1}$ are the same but traversed in reversed order). But $\mathcal{O}(1) = \mathbb{Z}_{2m+1}^*$ if and only if (i) $2m + 1$ is an odd prime (so that all numbers $1 \leq s \leq 2m$ are coprime to $2m + 1$), and, on account of (5), (ii) 2 is a cyclic generator of \mathbb{Z}_{2m+1}^* (or, equivalently, a primitive root for the modulus $2m + 1$). \square

From the table in [7, p. 864] of the least positive primitive roots of the prime numbers below 10,000, it follows that the primes under 102 with primitive root 2 are the following: 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83 and 101. Therefore, Π_{2m} (along with $\tilde{\Pi}_{2m}$ and $\tilde{\Pi}_{2m}^{-1}$), $2 \leq 2m \leq 100$, is irreducible (i.e. consists of a single cycle) for

$$2m = 2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82, 100. \quad (6)$$

From the same table in [7] it also follows that Π_{2^n} , $1 \leq n \leq 13$, is irreducible only for $n = 1, 2$.

3.3. This brings us to the next property. When $M = 2^n$, the permutation Π_{2^n} on $\mathbb{Z}_{2^n} = \{0, 1, \dots, 2^n - 1\}$ induces a permutation on n -bit blocks. Indeed, any number $s \in \mathbb{Z}_{2^n}$ can be represented in the form $s = b_{n-1}2^{n-1} + \dots + b_\nu 2^\nu + \dots + b_0$, where the bits $b_\nu \in \{0, 1\}$ are easily obtained with a pipelined quotient-remainder decomposition $s = 2q + r$, $0 \leq r < q$, replacing $s \leftarrow q$ after the first loop and $q \leftarrow r$ from then on, until $q = 0$; the successive remainders are b_0, \dots, b_{n-1} (in this order). Thus we can identify a number $s \in \mathbb{Z}_{2^n}$ with an n -bit block $\mathbf{b}(s) = b_{n-1} \dots b_\nu \dots b_0 \equiv \mathbf{b} \in \{0, 1\}^n$. As a result, any permutation $s \mapsto \pi(s)$ on \mathbb{Z}_{2^n} induces a corresponding permutation on n -bit blocks that we will denote by the same letter: $\mathbf{b} \mapsto \pi(\mathbf{b})$, where $\pi(\mathbf{b})$ is the n -bit representation of $\pi(s) \in \mathbb{Z}_{2^n}$. Denote by $\mathbf{b}^{(\nu)}$ the n -bit block obtained from \mathbf{b} by flipping the ν th bit of \mathbf{b} from the right, i.e., $\mathbf{b}^{(\nu)} = b_{n-1} \dots \bar{b}_\nu \dots b_0$, $0 \leq \nu \leq n - 1$, where $\bar{b}_\nu = b_\nu \oplus 1$ is the complementary bit to b_ν . Let us study the propagation of a single bit flip under the action of Π_{2^n} .

Take first $\nu \geq 1$ and suppose $b_\nu = 0$. If $s^{(\nu)} = b_{n-1}2^{n-1} + \dots + \bar{b}_\nu 2^\nu + \dots + b_0$, then $s^{(\nu)} = s + 2^\nu$, and (see (2))

$$\begin{aligned} \Pi_{2^n}(s^{(\nu)}) &= \Pi_{2^n}(s + 2^\nu) \\ &= \begin{cases} 2^{n-1} + k + 2^{\nu-1} & \text{if } s = 2k, \quad 0 \leq k \leq 2^{n-1} - 1, \\ k + 2^{\nu-1} & \text{if } s = 2k + 1, \quad 0 \leq k \leq 2^{n-1} - 1. \end{cases} \end{aligned}$$

In both cases,

$$\Pi_{2^n}(s^{(\nu)}) - \Pi_{2^n}(s) = 2^{\nu-1}.$$

This means that, given the input blocks \mathbf{b} and $\mathbf{b}^{(\nu)}$ differing only in the ν th bit from the right, $\nu \geq 1$, then the corresponding outputs $\Pi_{2^n}(\mathbf{b})$ and $\Pi_{2^n}(\mathbf{b}^{(\nu)})$ differ only in the $(\nu - 1)$ th bit from the right. The case $\nu \geq 1$ and $b_\nu = 1$ for all ν , $1 \leq \nu \leq n - 1$ (i.e., $s = 2^n - 1$ or $s = 2^n - 2$) reduces to the previous case by interchanging s and $s^{(\nu)}$.

It remains to consider a flip in the least significant (or rightmost) bit. In the case $\nu = 0$ and, say, $b_0 = 0$ (otherwise interchange s and $s^{(0)}$), we have $s = b_{n-1}2^{n-1} + \dots + b_1 2 = 2(b_{n-1}2^{n-2} + \dots + b_1)$ and $s^{(0)} = b_{n-1}2^{n-1} + \dots + b_1 2 + \bar{b}_0 = s + 1$. Thus (see (2)),

$$\Pi_{2^n}(s) = 2^{n-1} + b_{n-1}2^{n-2} + \dots + b_1,$$

$$\Pi_{2^n}(s^{(0)}) = \Pi_{2^n}(s + 1) = b_{n-1}2^{n-2} + \dots + b_1$$

and

$$\Pi_{2^n}(s) - \Pi_{2^n}(s^{(0)}) = 2^{n-1}.$$

This time we conclude that the outputs $\Pi_{2^n}(\mathbf{b})$ and $\Pi_{2^n}(\mathbf{b}^{(0)})$ differ only in the most significant (or leftmost) bit b_{n-1} .

In terms of differential cryptanalysis, we can restate the above property as follows: The input difference $(0, \dots, 0, 1, 0, \dots, 0)$ with the entry 1 at the k th position, transforms with probability one into the output difference $(0, \dots, 0, 0, 1, \dots, 0)$ with the entry 1 cyclically shifted one position to the right.

4. Properties of the discrete Lyapunov exponent

In this section we are going to consider the DLE of a permutation from a different point of view. Take randomly a $2m$ -permutation; what are the odds that its DLE is comparable to the maximal DLE λ_{2m}^{\max} ? Fig. 1, which we have borrowed from [6] for the reader's convenience, shows the normalized histograms of the DLE for permutations on \mathbb{Z}_M with $M = 16, 32, 64, 128$ and 256 , estimated by Monte Carlo sampling. Here we see how the distribution of DLE values gets more and more peaked with M . Hence, as M increases, one may expect randomly chosen M -permutations to have about the same discrete Lyapunov exponent, the dispersion of the values being the smaller the greater M . We will check now this property for the 2^{128} -permutations defined by two standard block ciphers: The Advanced Encryption Standard (AES) and Serpent.

4.1. Advanced encryption standard

The Advanced Encryption Standard (AES) is a symmetric cipher designed for 128, 192 and 256 bit block lengths but, for simplicity, we consider here the first implementation only. AES applies the following transformations:

(i) The *ByteSub* transformation $S(x)$ is a byte-level S -box (thus, $S: \{0, 1\}^8 \rightarrow \{0, 1\}^8$) defined as

$$S(x) = Bx^{-1} + b,$$

where $x^{-1} \in GF(2^8)$ is the multiplicative inverse of x if $x \neq 0$ or 0 if $x = 0$, B is an 8×8 binary matrix obtained by successively rotating the bits of its first row $B_{1j} = (1, 0, 0, 0, 1, 1, 1, 1)$ to the right, and $b = (1, 1, 0, 0, 0, 1, 1, 0)^{\text{transpose}}$. The *ByteSub* transformation defines a permutation π on $\{0, \dots, 255\}$ with $\lambda_\pi = 4.00$, while $\lambda_{256}^{\max} = 4.86$ (see (3)). The role of the *ByteSub* transformation is to mix in a strong nonlinear way the input information.

(ii) Let $b_{0,0}, \dots, b_{0,3}, \dots, b_{3,0}, \dots, b_{3,3}$ be the 16 bytes (128 bits) of the input block. The *ShiftRow* transformation takes the words

$$w_0 = (b_{0,0}, b_{0,1}, b_{0,2}, b_{0,3}),$$

$$w_1 = (b_{1,0}, b_{1,1}, b_{1,2}, b_{1,3}),$$

$$w_2 = (b_{2,0}, b_{2,1}, b_{2,2}, b_{2,3}),$$

$$w_3 = (b_{3,0}, b_{3,1}, b_{3,2}, b_{3,3}) \quad (7)$$

and returns $w_i \ggg C_i$, $i = 0, 1, 2, 3$, where $w \ggg C$ is the rotation of the sequence w of bytes to the right by C bytes. The values of C_i are $C_i = i$, $i = 0, 1, 2, 3$. The role of the *ShiftRow* permutation is just to permute all 16 bytes of the input block, thus it is a permutation on $\{0, 1, \dots, 15\}$. Its DLE turns out to be 1.81, to be compared to the maximum one (for $2m = 16$), $\lambda_{16}^{\max} = 2.13$.

(iii) Given an input block in the form (7), the *MixColumn* transformation can be viewed as a linear transformation in $GF(2^8)^4$. In fact, if $c_j = (b_{0,j}, b_{1,j}, b_{2,j}, b_{3,j})$, $0 \leq j \leq 3$, is the j th column of (7), then *MixColumn* is

$$c_j \mapsto \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} c_j,$$

where the matrix entries are pair of hexadecimal numbers representing bytes in the usual way. Therefore, *MixColumn* induces a

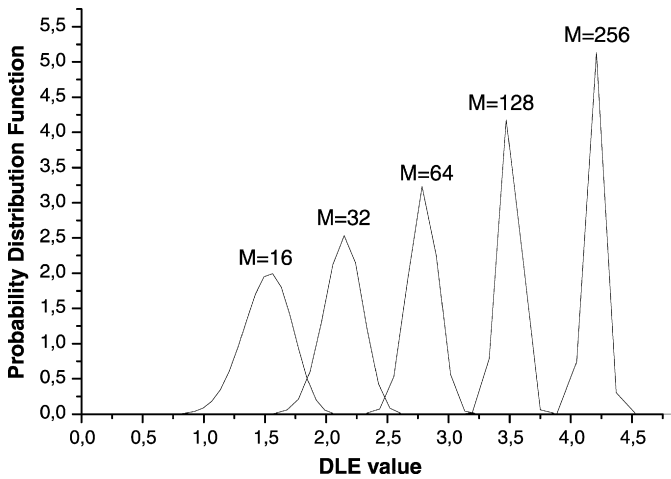


Fig. 1. Normalized histograms of the discrete Lyapunov exponent (DLE) λ_π for permutations π on \mathbb{Z}_M and $M = 16, 32, 64, 128, 256$.

permutation on $\{0, 1, \dots, 2^{32} - 1\}$. We have found the Lyapunov exponent of *MixColumn* to be 17.91 ($\lambda_{2^{32}}^{\max} = 21.49$).

In addition to the analysis of the single transformations, the behavior of their composition (i.e., of the Rijndael cipher) has been evaluated. To this aim, we assign to each 128 bit block an integer in $\{0, 1, \dots, 2^{128} - 1\}$ via its binary representation. The computation of the DLE has been performed on 7000 iterations of the AES map obtaining DLE = 20.93 after the first round and DLE = 87.22 after the second and subsequent rounds (to be compared with $\lambda_{2^{128}}^{\max} = 88.03$).

4.2. Serpent

Serpent handles 128-bit messages using a key that can be either 128-, 192-, or 256-bits long. The basic cryptographic operations are (see [8] for details):

(i) S-boxes. Serpent uses eight S-boxes, S_0, \dots, S_7 , mapping 4-bits inputs into 4-bits outputs, the string $b_3b_2b_1b_0$ being identified with the decimal number $b_32^3 + b_22^2 + b_12^1 + b_0 \in \{0, 1, \dots, 15\}$.

(ii) Linear transformations. Serpent takes four 32-bit words and performs on them several linear operations.

The encryption proceeds basically in 32 rounds. In the simplest version, the input to the i th round is first XORed with the round key K_i , next each 4-bit sub-block is input in parallel into 32 copies of the same S-box $S_{i \bmod 8}$, and finally (except in the last round) the output of the S-boxes is submitted to the linear transformations. In order to measure the diffusion property of the whole algorithm, we dropped the XOR operation with the round key and followed the orbit of a sample of 128-bit random messages. The result is DLE = 84.16 after the first round and DLE = 87.22 after the second and subsequent rounds.

By comparison we conclude that, from the second round on, the DLEs of the permutations defined on $\mathbb{Z}_{2^{128}}$ by the ciphers AES and Serpent coincide, as expected from an extremely peaked distribution.

5. Discussion and conclusion

Permutations on $\mathbb{Z}_M = \{0, 1, \dots, M - 1\}$ with relatively large M s, arise in a natural way in chaotic cryptography [3]. It is in this context that we want now to discuss briefly the results of the previous sections.

(A) Permutations with long cycles, such as F_M , are used in the random number generation. Theorem 2 states that Π_{2m} is a cycle only for some particular values of $2m$. Since these values are not bounded, this fact should not limit its practical applicability for random number generation.

(B) We say that a permutation on bit blocks satisfies the avalanche criterion if a single bit change on the input results in, at least, a certain percentage of output bits changed (in the strict avalanche criterion, this percentage is 50%) [8]. The avalanche criterion (among other criteria) has to be satisfied by the substitution boxes (or “S-boxes”) of block ciphers. Property 3.3 excludes Π_{2^n} from being used in conventional block ciphers.

(C) The distribution of the DLE values, Section 4, allows us to distinguish ‘typical’ from ‘special’ permutations and, as a matter of fact, it leads to a kind of statistical rejection test: if π is a $2m$ -permutation and λ_π is not close to λ_{2m}^{\max} , then π is not ‘typical’ enough and should be rejected. In this sense, the 2^{128} -permutation defined by AES with only one round (DLE = 20.93) is far from ‘typical’ ($\lambda_{2^{128}}^{\max} = 88.03$). The 2^{128} -permutation defined by Serpent with only one round should be also rejected on the same grounds. Needless to say, this is a rejection but not an acceptance test: depending on the scope of π , additional criteria should be checked.

In general, we conclude that typical (in the sense just explained) permutations F_M , obtained from chaotic interval maps, are better choices for chaotic cryptographic applications than others, like Π_{2m} , which may have a higher discrete Lyapunov exponent but which do not proceed from such maps.

Acknowledgements

We are very thankful to our referees for their valuable comments. We thank also T. Michalek, J.J. Rodríguez-Salas and L. Santamaría for helping us with the numerical simulations. This work has been financed by the Spanish Ministry of Science and Education under project MTM05-04948.

References

- [1] L. Kocarev, J. Szczepanski, J.M. Amigó, I. Tomovski, IEEE Trans. Circuits Syst. 53 (2006) 1300.
- [2] J.M. Amigó, L. Kocarev, I. Tomovski, Physica D 228 (2007) 77.
- [3] J.M. Amigó, L. Kocarev, J. Szczepanski, Phys. Lett. A 366 (2007) 211.
- [4] G. Jakimoski, K.P. Subbalakshmi, IEEE Trans. Circuits Syst. II 54 (2007) 499.
- [5] F. Benatti, A. Verjovsky, F. Zertuche, J. Math. Phys. 47 (2006) 022705.
- [6] J.M. Amigó, L. Kocarev, J. Szczepanski, IEEE Trans. Circuits Syst. II 54 (2007) 882.
- [7] M. Abramowitz, I.A. Stegun, Handbook of Mathematical Functions, Dover, New York, 1965.
- [8] J. Pieprzyk, T. Hardjono, J. Seberry, Fundamentals of Computer Security, Springer, Berlin, 2003.