A dynamical systems approach to the discrimination of the modes of operation of cryptographic systems

Jeaneth Machicao

Scientific Computing Group, São Carlos Institute of Physics, University of São Paulo (USP),
PO Box 369, 13560-970, São Carlos, SP, Brazil - www.scg.ifsc.usp.br

Jan M. Baetens

KERMIT, Department of Mathematical Modeling, Statistics and Bioinformatics,
Ghent University, Coupure links 653, 9000 Ghent, Belgium - www.kermit.ugent.be

Anderson G. Marco

Scientific Computing Group, São Carlos Institute of Physics, University of São Paulo (USP),
PO Box 369, 13560-970, São Carlos, SP, Brazil - www.scg.ifsc.usp.br

Bernard De Baets

KERMIT, Department of Mathematical Modeling, Statistics and Bioinformatics,
Ghent University, Coupure links 653, 9000 Ghent, Belgium - www.kermit.ugent.be

Odemir M. Bruno

Scientific Computing Group, São Carlos Institute of Physics, University of São Paulo (USP),
PO Box 369, 13560-970, São Carlos, SP, Brazil - www.scg.ifsc.usp.br

(Dated: April 13, 2015)

Evidence of signatures associated with cryptographic modes of operation is established. Motivated by some analogies between cryptographic and dynamical systems, in particular with chaos theory, we propose an algorithm based on Lyapunov exponents of discrete dynamical systems to estimate the divergence among ciphertexts as the encryption algorithm is applied iteratively. The results allow to distinguish among six modes of operation, namely ECB, CBC, OFB, CFB, CTR and PCBC using DES, IDEA, TEA and XTEA block ciphers of 64 bits, as well as AES, RC6, Twofish, Seed, Serpent and Camellia block ciphers of 128 bits. Furthermore, the proposed methodology enables a classification of modes of operation of cryptographic systems according to their strength.

I. INTRODUCTION

The propagation and continuous flow of information are of utter importance for the development of stable economies throughout the world as they are a prerequisite for successful business transactions, short- and long-range communication, and so on [1]. Often this information has to be encrypted in such a way that it can be safely transferred between the sender and recipient without allowing others to read the information that is present in such an encrypted message [2]. On the other hand, malicious persons and organizations, but also governmental organizations, are continuously striving to break the key with which messages were encrypted because this might enable them to get those pieces of information that are needed to achieve their criminal, protective, or other goals [3][4]. It is probably due to the impact of Turing’s success in breaking the Enigma that humanity became aware of the importance of cryptography in general, and the vulnerability of ciphers more in particular [5].

Since this major breakthrough, the functioning of the industrial, financial and public sector has become strongly dependent on the advances of cryptography. For instance, while the availability of worldwide networks has enabled rapid dissemination of information, it has also stimulated cryptographic innovations because a significant share of this information may only be available to a few parties. In this manner, technological progress during the last decades has increased the need for secured communication and transactions, information shielding, and so on [3][4].

In the last few decades, modern cryptography replaced mechanical schemes with new computing models. This modern focus influenced the classical design of ciphers far beyond the original purpose. Nowadays, there are two class of cryptographic algorithms depending on the key: symmetric and asymmetric. Symmetric encryption algorithms use the same key for both encryption of plaintext and decryption of ciphertext. This class of algorithm is also divided into two categories: stream ciphers and block ciphers. Block ciphers have gained wide popularity since the introduction of the first adopted encryption: The Data Encryption Standard (DES) [6], in the mid-1970s, yet nowadays this cipher is considered prone to brute force attacks. To overcome this shortcoming...
the International Data Encryption Algorithm (IDEA) \[7\] was designed in 1991 to replace DES. Ever since, there has been a pursuit for the development of new algorithms that meet the rising security expectations. In 1997, the National Institute of Standards and Technology (NIST) \[8\] selected the official Advanced Encryption Standard (AES) among many competitors, namely Serpent \[9\], Twofish \[10\], RC6 \[11\], Rijndael \[12\], etc.

To date, block ciphers are the most important elements in many cryptographic systems \[3\]. A block cipher breaks a message into blocks of elements (bits) and then encrypts one block (plaintext) at a time producing its corresponding output block (ciphertext). However, a block cipher by itself allows for the encryption of only one block, such that it is recommended to use a mode of operation in conjunction \[13\]. This mode of operation specifies a mechanism to improve the corresponding block cipher, while encrypting all of the blocks, one by one, as it goes along.

Motivated by the analogies between cryptographic and dynamical systems, on the one hand, and the lack of a means to discriminate between different modes of operation that can be used to encrypt a message with a block cipher using a single key, on the other hand, we demonstrate in this paper how Lyapunov exponents can be relied upon for tackling this problem. More specifically, by contemplating the whole of a cipher, ciphertext and key as an utter discrete dynamical system, \(i.e.,\) a cellular automaton (CA), and by resorting to the notion of Lyapunov exponents as they have been conceived for such systems \[14\] \[15\], we show how these measures can be exploited to identify the mode of operation that was used during the encryption process.

Although the cryptographic process of encrypting and decrypting information does not constitute a dynamical system as such, it has been reported that it is possible to draw parallels between cryptographic and dynamical systems \[16\] \[19\]. Hence, drawing upon such parallels, we have a means to exploit similar tools as the ones that have been conceived in the framework of dynamical systems in order to characterize cryptographic systems. Taking into account that the stability of a dynamical system is generally acknowledged as its main characteristic because it gives insight into its intrinsic nature \[20\] \[21\], it is natural to verify whether the dynamical systems viewpoint of a cryptographic system allows for a similar notion in order to better understand the latter. An exploration of this is further motivated by the fact that several researchers have noticed a close resemblance between a cryptographic system on the one hand, and a chaotic system, on the other hand \[22\] \[25\], and the large number of chaos-based cryptosystems \[26\] \[27\].

Classically, the stability of a dynamical system is assessed by computing its so-called largest Lyapunov exponent that quantifies how it behaves if it is evolved from two different but close initial conditions \[20\]. Either the corresponding phase space trajectories diverge or converge in which case we refer to the system as unstable or asymptotically stable, respectively, or the system is conservative, which means that the initial separation remains.

As the fields of cryptography and dynamical systems are not yet strongly interwoven, the basic definitions and concepts that relate to those systems and that are of interest within the framework of this paper are presented in Section \[11\] while the dynamical systems viewpoint on cryptographic systems is presented in Section \[11\] together with the proposed method for identifying the underlying mode of operation. Finally, the strengths of the proposed method are illustrated and discussed in Section \[14\] by means of computer experiments.

II. PRELIMINARIES

In this section we introduce the specificities of both cryptographic and dynamical systems that are indispensable for a clear understanding this paper.

A. Block ciphers and modes of operation

Classically, an encryption system encloses three major components, namely a cipher, a key, and finally, a ciphertext. The former constitutes a sequence of instructions that must be executed in order to encrypt a given plaintext, which may be envisaged as a sequence of \(N\) bits, such that it can be represented as a Boolean vector \(P\) of length \(N\). The result of this encryption process using a key \(K\), which is a sequence of \(k\) bits, is a so-called ciphertext, which may be represented in a similar fashion as a Boolean vector \(C\) of length \(N\) \[3\].

Of course, the real plaintext size varies and is mostly different from the length of the blocks for which a block cipher is designed. Consequently, common ciphers cannot be applied directly for the encryption of arbitrary-length plaintext \[28\]. In order to overcome this issue, so-called block ciphers have been designed and implemented. A block cipher slices the plaintext of length \(N\) into \(b\) blocks of \(n\) bits, after which each of these blocks is encrypted/decrypted by a block cipher, denoted as \(E_K\) and \(E_K^{-1}\), respectively. Mathematically, the encryption of a plaintext \(P = (P_1, P_2, \ldots, P_k)\) of length \(n\) into a ciphertext of the same length can be formalized as \(C = E(K, P) = E_K(P)\), where \(E : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n\).

If the length \(N\) of the plaintext is not a whole multiple of \(b\), additional bits are padded to the last block of the plaintext.

These block ciphers encrypt a plaintext in accordance with a well-defined procedure, which is commonly referred to as the mode of operation of a block cipher. A block cipher encrypts one block at a time, and it is the mode of operation that allows a block cipher to encrypt blocks consecutively in a secure way. Most of them use an initialization vector (IV), denoted \(\gamma\), which adds randomness to the encryption process \[3\]. For instance, the
counter mode uses a special method for generating counters in order to guarantee that each block in the sequence is different from every other block [14].

From the many block ciphers currently available, we will focus on the well-studied ones, being DES [6] \((n = 64, k = 56)\), IDEA [7], TEA [29] and XTEA [30] \((n = 64, k = 128)\), as well as AES [12], RC6 [11], Twofish [10], Serpent [9], Seed [31] and Camellia [32] \((n = 128, k = 128)\). The specifications of these block ciphers and the modes of operation are public, so they can be implemented [13].

In 2001 the NIST compiled and recommended five modes of operation—most of them were developed 30 years ago—to be used with a block cipher, namely the Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes [13]. In addition to these NIST modes, there are many others, among which the Propagating Cipher-Block Chaining (PCBC) [3] mode will be considered in this paper.

Mathematically, the encryption of an arbitrary-length plaintext by means of a block cipher in combination with the ECB mode of operation can be formulated as:

\[
C_j = E_K(P_j), \quad j = 1, 2, \ldots, b,
\]

where \(C_j\) represents the encrypted counterpart of the \(j\)-th block of plaintext \(P_j\). Similarly, the formalism for the CBC mode is given by

\[
C_j = E_K(C_{j-1} \oplus P_j), \quad j = 1, 2, \ldots, b,
\]

where \(\oplus\) is the mod 2 operator and \(C_0 = \gamma\). For the OFB mode one may write:

\[
C_j = P_j \oplus O_{j-1}, \quad j = 1, 2, \ldots, b,
\]

where \(O_j = E_K(O_{j-1})\) with \(O_0 = E_K(\gamma)\) and \(\gamma\) is randomly selected from \(\{0,1\}^n\). Table I lists the formulas for the other modes of operation that are considered in this paper.

In the remainder, a mode of operation of a block cipher is denoted as \(M_{E_K}\) : \(\{0,1\}^N \rightarrow \{0,1\}^N\), which maps a given plaintext \(P\) of length \(N\) to a corresponding ciphertext \(C\) of equal length, so that we may write \(C = M_{E_K}(P)\). In order to clarify the functioning of a cryptographic system, we show in Fig. 1 a cryptographic system with \(b = 2\) blocks of \(n = 3\) bits that uses the CBC mode of operation. We consider an exemplary plaintext \(P = (P_1, P_2)\), for which it holds that \(P_1 = 010, P_2 = 001\) and \(\gamma = 101\). Note that the outputs generated by \(E_K\) are chosen only for illustration, e.g., \(C_1 = E_K(C_0 \oplus P_1) = E_K(111) = 100\). We can see clearly that a single application of the function \(M_{E_K}\) consists of \(b\) applications of \(E_K\) since the latter has to be applied to each of the plaintext blocks \(P_j\) in order to construct the ciphertext \(C\).

\[
\begin{array}{|c|c|}
\hline
\text{t} & \text{C}_t \\
\hline
0 & (101) \\
1 & (100) \\
\hline
\end{array}
\]

**FIG. 1:** Example of the CBC mode of operation with \(b = 2\) blocks, \(n = 3\) bits and block cipher \(E_K\).

### B. Analogies between cryptographic and dynamical systems

Although cryptographic systems, as the ones given by Eqs. (1)–(3) and those listed in Table I, do not constitute dynamical systems, we can draw some parallels between both types of system, which might enable us to gain a deeper understanding of the former [10,17,22,24]. More specifically, we may envisage such a cryptographic system as a one-dimensional CA, which can be represented by means of a triplet \((T, S, \Psi)\). The first element of this triplet refers to a one-dimensional array of ‘cells’ \(c_i\), each of which bears one of the states enclosed in the finite set \(S = \{0,1\}\), and which are updated at discrete time steps by means of a global transition function \(\Psi\). The state of the \(i\)-th cell in \(T\) at the \(t\)-th time step will be denoted as \(s(c_i, t)\). Essentially, upon putting \(\Psi \equiv M_{E_K}\), a mode of operation \(M_{E_K}\) may be envisaged as such a global transition function.

Finally, we identify a given plaintext \(P\) with \(s(\cdot,0)\) in such a way that the \(i\)-th bit of the \(j\)-th block in \(P\) is denoted as \(s(c_i^j,0)\). The transition function \(M_{E_K}\) may be applied iteratively so that a distinct ciphertext \(C^t\) is evolved at every time step \(t\). As such, a cryptographic system can be transformed into a CA, and we may write

\[
s(\cdot, t + 1) = M_{E_K}(s(\cdot, t)),
\]

or equivalently, \(C^{t+1} = M_{E_K}(C^t)\), where \(C^1 = M_{E_K}(P)\).

In Fig. 2 we show an illustration of the CBC mode of operation by using Eq. (4) for the first two time steps in the evolution of its corresponding CA. Note that text styling has been added to make the effect of the mode of operation tractable, and also, that the same plaintext

| CFB | CTR | PCBC |
|-----|-----|-----|
| \(C_j = P_j \oplus E_K(C_{j-1})\) | \(C_j = P_j \oplus O_j\) | \(C_j = E_K(P_j \oplus P_{j-1} \oplus C_{j-1})\) |
| \(C_1 = P_1 \oplus E_K(\gamma)\) | \(O_j = E_K(\gamma)\) | \(C_1 = E_K(P_1 \oplus \gamma)\) |

**TABLE I:** Mathematical representation of the CFB, CTR and PCBC modes.
and $\gamma$ values are used as the ones given in Fig. [1] As the mode of operation is applied iteratively, at every consecutive time step $\gamma$ is put equal to $C_0^t$ because one has to select a new point in phase space that is the closest to the reference direction, which basically constitutes an orientation of the new initial configuration $C_0^{t+1}$ into the direction of $C_0^t$. For reasons of uniformity, $\gamma$ is the only parameter that can contain this initial configuration.

Recently, sundry methods have been developed to unravel the dynamical properties of utter discrete dynamical systems such as CA [14, 15, 53, 54]. As such, by relying on these for grasping the dynamics of a cryptographic system’s corresponding CA, we might be able to gain deeper insight into the dynamics of the former. More specifically, we will show in the remainder of this paper how Lyapunov exponents of CAs may be relied upon for identifying the mode of operation of the underlying cryptographic systems, in the same way as these measures have shown their usefulness for characterizing utter discrete dynamical systems [14, 15, 53, 54].

III. A CELLULAR AUTOMATON VIEW ON CRYPTOGRAPHIC SYSTEMS

Suppose that the CA counterpart of a given cryptographic system $\mathcal{S} = (\mathcal{C}, \mathcal{P}, M_{E_K})$ is denoted as $\mathcal{C}$. We can investigate the dynamics of the former in general, and its stability more in particular, by computing its so-called Lyapunov exponent, which quantifies how the dynamical system behaves in the long run if it is evolved from two close initial conditions. Clearly, in our setting, this means that we will assess the sensitivity of the equivalent CA $\mathcal{C}$ to a small perturbation of the plaintext since we put $s(\cdot, 0) = \mathcal{P}$. Hence, this should yield insights into the behaviour of the cryptographic system if the plaintext is perturbed.

Taking into account that the smallest possible perturbation in such a two-state setting boils down to flipping one bit of the first block of the plaintext $\mathcal{P}$, $P_1$ constitutes the most influential block (initial condition) to the mode of operation. Besides, it holds that the initial damage vector $h(\cdot, 0) = \mathcal{P} \oplus \mathcal{P}^*$, where $\oplus$ is the mod 2 operator, contains only one non-zero element. In the remainder, a cell $c_i^t$ for which holds that $h(c_i^t, 0) = 1$ will be referred to as a defective cell. After pinning down a plaintext $\mathcal{P}$ and its perturbed version $\mathcal{P}^*$ that fulfills the latter criterion, we can evolve the equivalent CA $\mathcal{C}$ from both $s(\cdot, 0) = \mathcal{P}$ and $s^*(\cdot, 0) = \mathcal{P}^*$ for one time step in order to obtain $s(\cdot, 1)$ and $s^*(\cdot, 1)$. Here, it should be recalled that one time step in the evolution of a CA corresponds to one application of the mode of operation $M_{E_K}$, which involves the update of several blocks. Having updated all the blocks, we can compute the damage vector at the first time step

$$h(c_i^t, 1) = \begin{cases} 1 & \text{if } s^*(c_i^t, 1) \neq s(c_i^t, 1), \\ 0, & \text{else.} \end{cases}$$

Consequently, the total number of defects at the first time step can be computed as

$$c_1 = \sum_{j=1}^{b} \sum_{i=1}^{n} h(c_i^t, 1). \tag{5}$$

At this point, the reader might think that the damage vector during subsequent time steps should be computed similarly, but this is certainly not the case because one would then neglect the fact that the defects can cancel out each other due to the discrete nature of the CA’s state space [14, 15]. The discrepancy between the number of defective cells and the number of defects is not yet clear after the first time step because every defective cell at $t = 1$ traces back to the same initial defective cell.

However, as soon as the CA is evolved one more time step, a discrepancy emerges between these quantities. This can be understood by explicitly tracking all possible pathways along which defects at $t = 1$ may propagate and accumulate during one subsequent time step (see Fig. 3). It is interesting to have a closer look at how nine defects can arise at the second time step in the evolution of the CA notwithstanding there are only five defective cells, which should be contributed to the fact that several of them may enclose multiple defects due to the existence of several pathways along which defects can propagate.
Taking into consideration this reasoning, the correct number of defects at the t-th time step, denoted \( \epsilon_t \), should be computed in accordance with the following six-step procedure.

1. Let the cryptographic system evolve for one time step, i.e., \( C^1 = M_{E_K}(P) \), and analogously for its perturbed version \( C^{1*} = M_{E_K}(P^*) \), both using the same initialization vector \( \gamma \).

2. Calculate the damage vector \( h_1 \) given by Eq. 5 and set the initialization vector as the last block calculated for both versions, i.e., \( \gamma = C^1_t \) and \( \gamma^* = C^{1*}_t \), as explained in Section II-B.

3. For every \( c^1_i \) for which \( h(c^1_i,1) = 1 \), create a replica \( R^1_i \) such that \( R^1_i(c^1_i,1) = s^*(c^1_i,1) = \pi(c^1_i,1) \), where \( \pi(c^1_i,1) \) is the Boolean complement of \( s(c^1_i,1) \), and \( R^1_i(c^1_q,1) = s(c^1_q,1) \), for every \( c^1_q \neq c^1_i \). Use the set \( A_1 \) to store these replicas.

4. Let the cryptographic system evolve one more time step, i.e., compute \( s(\cdot,2) \) and \( R(\cdot,2) \), which boils down to evaluating \( M_{E_K}(R^1_i) \) with the same \( \gamma^* \) for all replicas \( R \in A_1 \).

5. Calculate the total number of defects at the second time step as follows:

\[
\epsilon_2 = \sum_{R^1_i \in A_1} \sum_{j=1}^b \sum_{i=1}^n h(c^1_i,2) \tag{6}
\]

and set the initialization vector as the last block calculated for both versions, i.e., \( \gamma = C^2_t \) and \( \gamma^* = C^{2*}_t \).

6. For every \( c^2_i \) and \( R \in A_1 \) for which \( R(c^2_i,2) \neq s(c^1_i,2) \), create a replica \( R^2_i \) such that \( R^2_i(c^2_i,2) = \pi(c^2_i,2) \) and \( R^2_i(c^2_q,2) = s(c^2_q,2) \) for every \( c^2_q \neq c^2_i \). Use a multiset \( A_2 \) to store these replicas.

7. Repeat steps (4)–(6) in every subsequent time step \( t + 1 \) in order to assemble \( h(\cdot,t+1) \) and \( A_{t+1} \).

After computing the number of defects \( \epsilon_t \) at every consecutive time step \( t \), the rate of divergence/convergence of initially close phase space trajectories \( \lambda(t) \) of a CA \( C \) can be obtained from:

\[
\lambda(t) = \frac{1}{t} \log \left( \frac{\epsilon_t}{\epsilon_0} \right), \tag{7}
\]

with its limit value

\[
\lambda = \lim_{t \to \infty} \lambda(t), \tag{8}
\]

generally referred to as the maximum Lyapunov exponent (MLE) of \( C \). In the framework of cryptographic systems, \( \lambda(t) \) quantifies how ciphertexts, which are obtained by iteratively encrypting two close plaintexts \( P \) and \( P^* \), behave (converge/diverge) as the number of time steps grows. As indicated in papers on the LE of CAs, one can derive a theoretical upper bound on these LEs, which has shown to depend on the number of neighbours [14, 15].

Calling to mind Shannon’s idea of diffusion, which is related to the avalanche effect and states that a slight change of the plaintext gives in worst case rise an entirely different ciphertext, we are able to derive a theoretical upper bound on the MLE of cryptographic systems. For instance, consider the plaintext \( P = 10101101 \) and its perturbed version \( P^* = 10101100 \), as well as their encryption \( E_K(P) = 101011000 \) and \( E_K(P^*) = 010101111 \), respectively. In the worst case scenario, the number of differences may be at most 8, which is the length of the plaintext \( N \). This means that a defect in \( c^1_i \) at the \( t \)-th time step can at most propagate to \( N \) bits at the subsequent time step. Therefore, a mean-field approximation of the upper bound \( \lambda_m \) for the cryptographic systems becomes

\[
\lambda_m = \frac{1}{t} \log(\lambda^t) = \log(N) = \log(bn). \tag{9}
\]

Obviously, the higher the number of blocks \( b \), the higher the upper bound becomes.

Before turning to the experimental section of this paper, we illustrate in Fig. 3 the procedure by which the LE of a mode of operation \( M_{E_K} \) can be assessed. Note that we employed the same plaintext as in Fig. 2. By moving along this table’s rows, we see the plaintexts that are encrypted by repeatedly applying the mode of operation \( M_{E_K} \). Note that some replicas are repeated as soon as the system is evolved for one time step, which is in agreement with the findings reported in Fig. 3.

In order to avoid having to keep track of all pathways individually, one can optimize the algorithm by just counting every unique replica once and keeping track of its multiplicity. For example, at \( t = 2 \) the replica \( R^1_2 \) would be repeated twice, then at the subsequent time step this replica has two cell defects, which means four pathways in total at \( t = 3 \). As such, by tracking the multiplicity of every defect rather than every defect itself, the efficiency of the algorithm increases substantially.
If the cryptographic system is sensitive to the plaintext from which it is evolved, the number of defects $e_t$ increases exponentially during its evolution, such that $e_t \approx e_0$, and consequently, $\lambda > 0$. On the other hand, the system should be referred to as insensitive to the underlying plaintext if the initial defect vanishes as the number of time steps increases. Such a situation implies that $\lambda = -\infty$ owing to the discrete nature of a CA’s state space. Since cryptographic systems are designed in such a way that small changes in the plaintext give rise to substantially differing ciphertexts, it should not come as a surprise if $\lambda$ would be positive for all the modes of operation at stake in this paper. Still, the numerically assessed values of $\lambda(t)$ might differ significantly among different block ciphers and/or underlying modes of operation, such that they may still be used to discriminate between different modes of operation. This usage will be illustrated in the following section.

### IV. EXPERIMENTAL RESULTS AND DISCUSSION

To demonstrate the effectiveness of the above methodology, we considered two groups of block ciphers on the basis of their block length $n$. The first group encloses the 64-block ciphers, namely DES [6], IDEA [7], TEA [29] and XTEA [30], which all use a $k = 64$ key except for DES that uses a key of length of $k = 56$ bits. The second group of block ciphers is composed of 128-block ciphers with key of $k = 128$ bits: AES [12], RC6 [11], Twofish [10], Serpent [9], Seed [31] and Camellia [32].

These ten block ciphers were adapted in such a way that they took the plaintext $P$, the key $K$ and the initialization vector $\gamma$ as input variables. Moreover, these block ciphers were implemented with a predefined number of rounds, each of which consist of several inner steps in the course of an encryption process and they depend on the specific algorithm [3]. We considered eight rounds for IDEA, eighteen for DES, and thirty-two rounds for both TEA and XTEA. Further, ten rounds for AES, sixteen for both Twofish and Seed, eighteen for Camellia and thirty-two for Serpent. Finally, we implemented the modes of operation in accordance with the formalism given by Eqs. (1)–(3) for ECB, CBC and OFB, and in Table I for CFB, CTR and PCBC.

#### A. The dataset

To ensure the representativity of the computed Lyapunov exponents, we computed the average $\lambda$-values that were obtained when the CAs were evolved from different plaintexts. Hence, the $\lambda$-values reported in the remainder represent averages calculated over an ensemble $E = \{P \mid e = 1, \ldots, 200\}$ of 200 randomly generated plaintexts $P$ and their perturbed versions $P^*$, which were obtained by flipping only one bit in the first block of $P$.

Since such an ensemble was constructed for each of the concerned cryptographic systems, by mutually combining the underlying block cipher and the mode of operation, we considered a total of 60 combinations, i.e., ten block ciphers and six modes of operation. Consequently, a total of 12000 plaintexts were generated randomly.

Similarly, the key $K$ and the initialization vector $\gamma$ were generated randomly in order to avoid both key repetitions and weak keys, which is a recommendation in cryptography [33]. In the remainder, we refer to the assembly of the 200 randomly generated plaintexts, keys and initialization vectors as the cryptographic dataset per cipher and mode of operation. Given that the block ciphers encrypt a plaintext by splitting it into a number of blocks and subsequently transcribing every block, the plaintexts were generated in such a way that they were composed of the same number of $b$ blocks, irrespec-

| Time steps | Original plaintext $P$ | Perturbed version $P^*$ | # defects |
|------------|-----------------------|-------------------------|----------|
| $t = 0$    | $C_0 = \gamma = [101]$ | $C_0 = \gamma^* = [101]$ | $e_0 = 1$ |
| $P = [010, 001]$ | $P^* = [011, 001]$ |
| $t = 1$    | $C^1 = M_{E_1}(P) = [100, 000]$ | $C^1 = M_{E_1}(P^*) = [111, 010]$ | $e_1 = 3$ |
| $t = 2$    | $C^2 = M_{E_2}(C^1) = [011, 111]$ | $M_{E_2}(R_1) = [001, 101]$ | $e_2 = 5$ |
| $t = 3$    | $C^3 = M_{E_3}(C^2) = [010, 011]$ | $M_{E_3}(R_1) = [010, 011]$ | $e_3 = 2^{*2+1}+2 = 7$ |
tive of the type of block cipher. Note that this implies a plaintext containing $N = b \times 64$ bits in case of the 64-block ciphers and $N = b \times 128$ bits in case of the 128-block ciphers. Thus, in order to compare $\lambda$-values of 64- and 128-block ciphers, we normalized the numerically obtained $\lambda$ with respect to $\lambda_m$ obtained from Eq. 9.

B. Lyapunov exponents for the modes of operation

We assessed $\lambda(t)$ for the CA counterpart of each of the concerned cryptographic systems. For that purpose, the equivalent CAs were evolved for $t = 200$ time steps, which was sufficiently long because $\lambda(t)$ showed convergence in such a way that $|\lambda(t) - \lambda(t + 1)| < 1.19 \times 10^{-4}$, being the maximum discrepancy between $\lambda(t)$ and $\lambda(t+1)$ at the end of the simulation.

Furthermore, the consistency of the $\lambda$-values across the members of the different ensembles is also demonstrated in Fig. 5(a), which depicts the frequency distribution of the standard deviation $\sigma_\lambda$ (base 10 logarithm) of $\lambda_{200}$ calculated for the 60 cryptographic systems at stake. This histogram shows the similarity of $\lambda$ across the different plaintexts, as the standard deviation that comes along with the average MLE for the different cryptographic systems is obviously small.

![Histogram of standard deviation](image)

**FIG. 5:** (a) Frequency distribution of the standard deviation $\sigma_\lambda$ (base 10 logarithm) of $\lambda_{200}$ calculated over the 60 combinations of cryptographic systems. (b) Frequency distribution of $\Delta = \max\{\{eP | e = 1, \ldots, 200\} \} - \min\{\{eP | e = 1, \ldots, 200\}\}$.  

Fig. 5(b) shows a histogram of the discrepancies between the maximum and minimum observed MLE among the members of the ensemble $E$, denoted by $\Delta = \max\{\{eP | e = 1, \ldots, 200\} \} - \min\{\{eP | e = 1, \ldots, 200\}\}$. The $\Delta$-values obtained for the investigated datasets lie between $3.99 \times 10^{-5}$ and $4.79 \times 10^{-3}$. The maximum and minimum $\Delta$ correspond, respectively, to the pairs of modes of operation with underlying block cipher: IDEA-OFB and Serpent-CFB. All together, these small discrepancies demonstrate once more that the $\lambda$-values are highly consistent across the different plaintexts within the ensemble $E$, such that we may draw conclusions on their average values.

For simplicity, we mainly restrict our attention to IDEA and AES as representative members of the families of 64- and 128-block ciphers (see Fig. 6), respectively, since similar results were obtained for the other block ciphers in the same families (see Fig. 7). These figures depict the LE curves for all the modes of operation versus the number of time steps—note that the standard deviation of each curve is not shown since they are very small. Taking into account Eq. (9), the upper bound for the 64-block ciphers is $\lambda_m = \log(N) = \log(320) \approx 5.76832$, while it is $\lambda_m = \log(640) \approx 6.64147$ for the 128-block ciphers were employed to normalize the $\lambda$-values, respectively.

![Lyapunov exponent curves](image)

**FIG. 6:** Lyapunov exponent versus the number of time steps for different modes of operation, being ECB, CBC, OFB, CFB, CTR and PCBC, using the (a) IDEA 64-block cipher and (b) AES 128-block cipher. The curves represent the average LE $\lambda$ over 200 initial plaintexts during $t = 200$ times steps, which are normalized with respect to $\lambda_m$ obtained from Eq. (9).

From both figures, it is quite easy to discriminate between the modes of operation, except for the overlapping curves of CTR and OFB. It is interesting to have a closer look at how their corresponding LE increases almost exponentially during the first few time steps. This behaviour can be explained by reconsidering the equations in Table I. Indeed, CTR uses an inner pseudo-random number generator and OFB uses a new initialization vec-
tor at every time step, such that the number of defective cells will not only increase due to discrepancies naturally emerging between the plaintexts, but also due to the additional defects introduced through these random processes. In contrast, CFB displays the opposite effect, i.e., its curve decays exponentially.

Further, the Lyapunov exponents of ECB and PCBC are constant, since the number of defective cells grows proportionally through time. For instance, this behaviour can be explained by considering that ECB contains \( \lambda_{200} = 3.46565 \pm 1.35 \times 10^{-3} \) with the IDEA block cipher, which means that the number of defects \( \epsilon_t = e^{(\lambda_{200})} = 31.99728 \pm 4.32 \times 10^{-2} \) equals approximately \( n/2 \), being almost 50% of the block length. The same behaviour occurs for the AES block cipher, where \( e^{(\lambda_{200})} = 63.994055 \pm 4.29 \times 10^{-2} \).

The original values of the exponents and standard deviation found at the end of the simulation are summarized in Table [II]. Furthermore, we can discriminate between modes of operation in families of block ciphers not only

FIG. 7: Lyapunov exponent versus the number of time steps for different modes of operation, being ECB, CBC, OFB, CFB, CTR and PCBC using 64-block ciphers: DES, TEA and XTEA, and 128-block ciphers: RC6, Twofish, Seed, Serpent and Camellia with \( b = 5 \) blocks and \( n = 64 \) bits. The curves represent the average LE \( \lambda \) over 200 initial plaintexts during \( t = 200 \) time steps, which are normalized with respect to \( \lambda_m \) obtained from Eq. [9].
by visual inspection of the graphs, but also by means of statistical tests to demonstrate it. Paired t-tests revealed that there are statistically significant differences between ECB, CBC, CFB and PCBC mutually at the 5% significance level. However, no statistically significant difference was found between CTR and OFB. These observations were found in both families of 64- and 128-block ciphers, which also allows the proposed method to discriminate between modes of operation of different families, for instance, IDEA-CTR can be distinguished from AES-CTR.

Moreover, by means of the washer method [39], we analyzed statistically whether a curve (for one of the ensemble’s members) for a given mode falls within the envelope of curves obtained for the entire ensemble for another mode of operation. This procedure was repeated for all the curves within the given mode of operation at the 5% significance level, which indicated that at most 6.4% and 11.1% of the observations of the 64- and 128-block ciphers constituted outliers. These outliers exist at the beginning of the simulation. We can also notice that the CFB curve behaves completely different from the other ones (non overlapping and not too close), which means that the CFB falls outside of the range of the LE for the other modes of operation.

C. Analysis of the LE of cryptographic systems

In this section, we will examine and discuss the preceding results in more detail.

a. Initial conditions $P$ and $P^*$

Recalling that an assessment of the Lyapunov exponent involves tracking the CA evolution from two initial configurations for which it holds that $h(x,0) = P \oplus P^*$ and given the fact that we are dealing with Booleans, the smallest possible perturbation in such a setting implies flipping the right-most bit of the plaintext. However, we observed that the position of the flipped bit does not affect the numerical value of the Lyapunov exponent, which can be understood by recalling the theoretical upper bound on the Lyapunov exponent of cryptographic systems. Indeed, the encryption of the plaintext with a bit flipped at an arbitrary $x$ position at the first plaintext block $(1 \leq x \leq n)$ may, in the worst case, affect all the bits of the ciphertext.

b. Cryptographic signatures

From Figs. 6–7 it should be noticed that the normalized $\lambda$-values do not attain 1, because none of the cryptographic systems at stake is attaining the worst case scenario mentioned in Section III. This can be explained by the fact that this is an ideal and desirable “scenario” for cryptographic systems and that the block ciphers at stake have their limitations. Furthermore, we found an unexpected phenomenon with regard to the families of 64- and 128-block ciphers. A closer look at the curves tied up with these families shows that, in fact, we can also differentiate between block cipher families.

c. Number of blocks

In order to investigate the importance of the number of blocks $b$, we computed the Lyapunov exponents for the same cryptographic systems but with $2, 4, 8, \ldots, 20$ blocks. In Fig. 8 one can see the LE curves for each mode of operation using the IDEA block cipher as a function of $b$. From this figure it is clear that each curve is somehow lifted upwards with the number of blocks $b$.

---

TABLE II: MLE $\lambda_{200}$ and standard deviation ($\times 10^{-3}$) for the (a) 64- and (b) 128-block ciphers.

(a)

| $\lambda_{200}$ | IDEA | DES | TEA | XTEA |
|-----------------|------|-----|-----|------|
| ECB             | 3.46565 ± 1.35 | 3.46570 ± 1.27 | 3.46554 ± 1.23 | 3.46564 ± 1.25 |
| OFB             | 5.04796 ± 4.00  | 5.04800 ± 3.89  | 5.04817 ± 3.87  | 5.04816 ± 3.68  |
| CBC             | 3.55597 ± 0.96  | 3.55598 ± 0.93  | 3.55596 ± 0.81  | 3.55598 ± 0.88  |
| CTR             | 5.04817 ± 3.55  | 5.04818 ± 3.81  | 5.04853 ± 4.14  | 5.04787 ± 4.15  |
| CFB             | 0.15925 ± 0.07  | 0.15925 ± 0.07  | 0.15926 ± 0.06  | 0.15925 ± 0.07  |
| PCBC            | 5.07496 ± 1.91  | 5.07465 ± 2.01  | 5.07467 ± 1.91  | 5.07451 ± 1.87  |

(b)

| $\lambda_{200}$ | AES | RC6 | Twofish | Seed | Serpent | Camellia |
|-----------------|-----|-----|---------|------|---------|----------|
| ECB             | 4.15879 ± 0.67 | 4.15885 ± 0.75 | 4.15876 ± 0.68 | 4.15887 ± 0.7 | 4.15887 ± 0.75 | 4.15884 ± 0.76 |
| OFB             | 5.73875 ± 2.82 | 5.73879 ± 2.96 | 5.73869 ± 2.86 | 5.73860 ± 2.84 | 5.73840 ± 2.82 | 5.73885 ± 3.02 |
| CBC             | 4.24921 ± 0.52 | 4.24913 ± 0.56 | 4.24920 ± 0.56 | 4.24915 ± 0.51 | 4.24919 ± 0.56 | 4.24920 ± 0.55 |
| CTR             | 5.73891 ± 2.83 | 5.73876 ± 2.70 | 5.73882 ± 2.79 | 5.73904 ± 2.78 | 5.73866 ± 2.74 | 5.73871 ± 2.81 |
| CFB             | 0.17311 ± 0.05 | 0.17311 ± 0.05 | 0.17311 ± 0.05 | 0.17311 ± 0.05 | 0.17311 ± 0.05 | 0.17311 ± 0.05 |
| PCBC            | 5.76812 ± 1.31 | 5.76815 ± 1.27 | 5.76792 ± 1.37 | 5.76816 ± 1.40 | 5.76792 ± 1.38 | 5.76806 ± 1.30 |
From Eq. (9), it is expected to get higher $\lambda$-values when the length of the plaintext increases. In fact, this occurs for all the modes of operation at stake, except for ECB. In particular, this indicates that irrespective of the number of blocks $b$ of the plaintext, the ECB’s number of defects will attain approximately $n/2$, which demonstrates that the first block is the only one affected by the initial conditions, while the other blocks do not spread defects. Furthermore, we obtained the same results with both groups of 64- and 128-block ciphers and the six modes of operation.

d. **Empirical MLE** In Section III we provided some mathematical foundations to obtain the theoretical upper bound $\lambda_m$ for cryptographic systems. However, the lack of an analytical upper bound for a specific mode of operation is an important limitation remaining. Perhaps, this limitation may seem contradicive to cryptography aims, because it indicates to find an analytical way to obtain the essence of a cryptographic system that is designed to avoid this gap.

Here, we opted for an alternative approach, i.e., an empirical estimation of the upper bound for the modes of operation as a function of the number of blocks, based on a multiple regression analysis, to gain a deeper insight into the behaviour of the LE curves. In Fig. 9 we show the MLE $\lambda$ obtained as a function of $b$ for the IDEA and the corresponding regression curves (see also Fig. 10 for the AES block cipher). The coefficients of determination also demonstrate the strong influence by the number of blocks $b$. 

---

**FIG. 8: Comparison of the LE for different modes of operation with 2, 4, 8, ..., 20 blocks using IDEA. Each plot contains curves which represent the average LE $\lambda$ over 200 initial plaintexts during $t = 200$ time steps of the IDEA 64-block cipher.**
FIG. 9: An empirical analysis of the upper bound for the modes of operation based on IDEA $\lambda_{200}$ with different number of blocks ($R^2 = 0.99$).
FIG. 10: An empirical analysis of the upper bound for the modes of operation based on AES $\lambda_{200}$ with different number of blocks ($R^2 = 0.99$).

c. **Computational considerations** Although the algorithm has been enhanced with different strategies to avoid tracking each individual defect, somehow the computational cost of the proposed methodology is very high, since the computational time dramatically increases as the number of blocks of the plaintext $P$ grows.

V. CONCLUSIONS

There is a strong relationship between cryptographic systems and discrete dynamical systems. In this work we have outlined an approach to envisage a cryptographic system as an equivalent one-dimensional CA in order to assess its stability characteristics by computing the Lyapunov exponent of the cryptographic system. The proposed method was capable of distinguishing six cryptographic modes of operation, namely ECB, CBC, OFB, CFB, CTR and PCBC using two families of block ciphers DES, IDEA, TEA and XTEA of 64 bits, as well as AES, RC6, Twofish, Seed, Serpent and Camellia of 128 bits. Moreover, the proposed method is also capable of distinguishing between the two families of 64- and 128-block ciphers. The results showed that the Lyapunov exponent evolution pattern is maintained for each mode.
of operation and this is independent of the block cipher used.

We also provided a mathematical basis to obtain the theoretical upper bound \( \lambda_u \) for the cryptographic systems. However, further work is required to theoretically analyze the upper bound on the LE for each of the modes of operation. Here we only used an empirical assessment to fit the curves. Finally, our results suggest that even modern and contemporary algorithms yield patterns that should be explored. Thus, our theoretical framework may offer a novel alternative to explore the weakness of these cryptographic systems and may ultimately lead to a classification of these systems according to their strength.

ACKNOWLEDGEMENTS

J. M. acknowledges support from FAPESP (The State of São Paulo Research Foundation) (2011/05461-0). O. M. B. acknowledges support from CNPq (Grant #307797/2014-7 and #484312/2013-8) and FAPESP (Grant # 2011/01523-1). This work has benefited from the cooperation agreement that has been established between Universidade de São Paulo and Ghent University.

[1] C. Shannon, A mathematical theory of communication, Tech. rep., Bell System Technical Journal (1949).
[2] W. Stallings, Cryptography and network security: Principles and Practice, 5th Edition, Prentice Hall, 2002.
[3] A. Menezes, S. Vanstone, P. V. Oorschot, Handbook of applied cryptography, CRC Press, Inc., 1996.
[4] S. Singh, The code book: the evolution of secrecy from Mary, Queen of Scots, to quantum cryptography, Doubleday, NY, USA, 1999.
[5] A. Hodges, Alan Turing: the enigma, Walker & Company, 2000.
[6] National Institute of Standards and Technology, FIPS PUB 46-3 data encryption standard (DES), Pub-NIST, 1999.
[7] J. Massey, X. Lai, Device for the conversion of a digital block and use of same, US5214703 A, 25. (May 1993).
[8] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, Report on the development of the advanced encryption standard (AES), Tech. rep., National Institute of Standards and Technology (2000).
[9] R. Anderson, E. Biham, L. Knudsen, A candidate block cipher for the advanced encryption standard, URL http://www.cl.cam.ac.uk/~rja14/serpent.html (1998).
[10] B. Schneier, Twofish, URL http://www.schneier.com/twofish.html (1998). doi:http://www.schneier.com/twofish.html
[11] R. Rivest, M. Robshaw, R. Sidney, Y. L. Yin, The rc6 block cipher, Tech. rep., RSA Laboratories and M.I.T. Laboratory for Computer Science (1998). doi:http://people.csail.mit.edu/rivest/Rc6.pdf.
[12] National Institute of Standards and Technology, FIPS PUB 197 advanced encryption standard, Pub-NIST, 2001.
[13] M. Dworkin, Recommendation for block cipher modes of operation, Tech. rep., National Institute of Standards and Technology (2001).
[14] J. Baetens, B. De Baets, Phenomenological study of irregular cellular automata based on Lyapunov exponents and Jacobians, Chaos 20 (3) (2010) 033112.
[15] F. Bagnoli, R. Rechtman, S. Ruffo, Damage spreading and Lyapunov exponents in cellular automata, Phys. Lett. A 172 (1992) 34–38.
[16] J. Amigó, L. Kocarev, J. Szczepanski, Discrete Lyapunov exponent and resistance to differential cryptanalysis, IEEE Transactions on Circuits and Systems–II: Express Briefs 54 (10) (2007) 882–886.
[17] G. Jakimoski, K. Subbalakshmi, Discrete Lyapunov exponent and differential cryptanalysis, IEEE Transactions on Circuits and Systems–II: Express Briefs 54 (6) (2007) 499–501.
[18] J. Machicado, A. Marco, O. M. Bruno, Lyapunov exponent: a qualitative ranking of block cipher mode of operation, in: T. Gilbert, M. Kirkilionis, G. Nicolas (Eds.), Proceedings of the European conference on Complex systems, Springer Proceedings in Complexity, Springer International Publishing, Bruxelles, Belgium, 2012, pp. 979–985.
[19] N. Nagaraj, One-time pad as a nonlinear dynamical system, Communications in Nonlinear Science and Numerical Simulation 17 (2012) 4029–4036.
[20] J.-P. Eckmann, D. Ruelle, Ergodic theory of chaos and strange attractors, Reviews of Modern Physics 57 (1985) 617–656.
[21] C. Robinson, Dynamical systems: stability, symbolic dynamics, and chaos, CRC Press, Boca Raton, United States, 1998.
[22] G. Álvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, International Journal of Bifurcation and Chaos 16 (2006) 2129–2151.
[23] J. Amigó, J. Szczepanski, L. Kocarev, Discrete chaos and cryptography, in: International Symposium on Nonlinear Theory and its Applications (NOLTA2005), 2005, pp. 461–464.
[24] J. Blackledge, N. Ptitsyn, Encryption using deterministic chaos, ISAST Transactions on Electronics and Signal Processing 4 (2010) 6–17.
[25] R. Schmitz, Public key cryptography: a dynamical systems perspective, in: Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE ’08, Esterel, France, 2008, pp. 209–212.
[26] J. Machicado, A. Marco, O. M. Bruno, Chaotic encryption method based on life-like cellular automata, Expert Systems with Applications 39 (2012) 12626–12635.
[27] A. Marco, A. Martínez, O. Bruno, Fast, parallel and secure cryptography algorithm using Lorenz’s attractor, International Journal of Modern Physics C 21 (2010) 265–
[28] W. Stallings, NIST block cipher modes of operation for confidentiality, Cryptologia 34 (2) (2010) 163–175.
[29] D. Wheeler, R. Needham, TEA, a tiny encryption algorithm, in: Lecture Notes in Computer Science (Leuven, Belgium: Fast Software Encryption: Second International Workshop), Vol. 1008, 1994, pp. 363–366.
[30] R. Needham, D. Wheeler, Extended tiny encryption algorithm, Tech. rep., Computer Laboratory Cambridge University, Cambridge, UK (1997).
[31] Korea Information Security Agency, A design and analysis of 128-bit symmetric block cipher (SEED), http://tools.ietf.org/pdf/rfc4009.pdf (1999).
[32] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, Camellia: a 128-bit block cipher suitable for multiple platforms - design and analysis, in: Proceedings of the 7th Annual International Workshop on Selected Areas in Cryptography, SAC ’00, Springer-Verlag, London, UK, 2000, pp. 39–56.
[33] M. Courbage, B. Kamiński, Space-time directional Lyapunov exponents for cellular automata, Journal of Statistical Physics 124 (2006) 1499–1509.
[34] C. Langton, Computation at the edge of chaos, Physica D 42 (1990) 12–37.
[35] S. Wolfram, Universality and complexity in cellular automata, Physica D 10 (1–2) (1984) 1–35.
[36] C. Li, G. Chen, Estimating the Lyapunov exponents of discrete systems, Chaos 14 (2) (2004) 343–346.
[37] B. Luque, R. Solé, Lyapunov exponents in random Boolean networks, Physica A: Statistical Mechanics and its Applications 284 (1-4) (2000) 33–45.
[38] W. Barker, E. Barker, Recommendation for the triple data encryption algorithm (TDEA) block cipher, Tech. rep., National Institute of Standards and Technology (2012).
[39] A. Venturini, Time series outlier detection: a new non parametric methodology (washer), Statistica 71 (2011) 329–344.