

Lyapunov Exponent Evaluation of the CBC Mode of Operation

Abdessalem Abidi¹, Christophe Guyeux², Jacques Demerjian³, Belagacem Bouallège¹, and Mohsen Machhout¹

¹ Electronics and Microelectronics Laboratory University of Monastir, Faculty of Sciences of Monastir, Tunisia

(E-mail: abdessalemabidi9@gmail.com)

² FEMTO-ST Institute, UMR 6174 CNRS, DISC Computer Science Department Université de Bourgogne Franche-Comté, 16, Route de Gray, 25000 Besançon, France

(E-mail: jacques.demerjian@gmail.com)

³ Lebanese University, Faculty of Sciences, LARIFA-EDST, Fanar, Lebanon

(E-mail: jacques.demerjian@gmail.com)

Abstract. The Cipher Block Chaining (CBC) mode of encryption was invented in 1976, and it is currently one of the most commonly used mode. In our previous research works, we have proven that the CBC mode of operation exhibits, under some conditions, a chaotic behavior. The dynamics of this mode has been deeply investigated later, both qualitatively and quantitatively, using the rigorous mathematical topology field of research. In this article, which is an extension of our previous work, we intend to compute a new important quantitative property concerning our chaotic CBC mode of operation, which is the Lyapunov exponent.

Keywords: Lyapunov coefficient, Cipher block chaining, mode of operation, Topological study.

1 Introduction

Blocks ciphers, like Data Encryption Standard (DES) or Advanced Encryption Standard (AES), have a very simple principle: they do not treat the original text bit by bit but they manipulate blocks of text. More precisely, the plaintext is broken into blocks of N bits. For each one, the encryption algorithm is applied to obtain an encrypted block that has the same size. Then, we put together all of these blocks, which are separately encrypted, to obtain the full encrypted message. For decryption, we proceed in the same way, but now starting from the ciphertext, in order to obtain the original one employing the decryption algorithm in place of the encryption function. So it is not sufficient to put anyhow a block cipher algorithm in a program. We can, instead, use these algorithms in various ways according to their specific needs. These ways are called block cipher modes of operation. Indeed, there are several modes and each one of them differs from others by its own characteristics, in addition to its specific security properties. In



this article, we are only interested in the Cipher Block Chaining mode and we will quantify its chaotic behavior thanks to the Lyapunov exponent. To do so, we first show that such mode of operations can be considered as dynamical systems.

Indeed, some dynamical systems are very sensitive to small changes in their initial condition. Both constants of sensitivity to initial conditions and of expansivity illustrate that [1,2]. However, these variations can quickly take enormous proportions, grow exponentially, and none of these constants can measure such a behavior. Alexander Lyapunov has examined this phenomenon and introduced an exponent that measures the rate at which these small variations can grow.

Definition 1. Let $f : R \rightarrow R$. The *Lyapunov exponent* of the system defined by $x^0 \in R$ and $x^{n+1} = f(x^n)$ is:

$$\lambda(x_0) = \lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{i=1}^n \ln |f'(x^{i-1})|.$$

Consider a dynamical system with an infinitesimal error on the initial condition x_0 . When the Lyapunov exponent is positive, this error will increase (situation of chaos), whereas it will decrease if $\lambda(x_0) \leq 0$.

Example 1. The Lyapunov exponent of the logistic map $x^0 \in [0, 1]$, $x^{n+1} = \mu x^n(1 - x^n)$ [3] becomes positive for $\mu > 3,54$, but it is always smaller than 1. The tent map [4,5] and the doubling map of the circle [6], two other well-known chaotic dynamical systems, have a Lyapunov exponent equal to $\ln(2)$.

Sometimes, instead of trying to prove directly the properties on the system itself, it is preferable to reduce the initial problem to another whose characteristics are known or seem to be accessible. Such a reduction tool is called, in the mathematical theory of chaos, the semi-conjugacy.

Definition 2. The discrete dynamical system (\mathcal{X}, f) is *topologically semi-conjugate* to the system (\mathcal{Y}, g) if it exists a function $\varphi : \mathcal{X} \rightarrow \mathcal{Y}$, both continuous and onto, such that:

$$\varphi \circ f = g \circ \varphi,$$

that is, which makes commutative the following diagram [7].

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{f} & \mathcal{X} \\ \varphi \downarrow & & \downarrow \varphi \\ \mathcal{Y} & \xrightarrow{g} & \mathcal{Y} \end{array}$$

In this case, the system (\mathcal{Y}, g) is called a *factor* of the system (\mathcal{X}, f) .

Various dynamical behaviors are inherited by systems factors [7]. They are summarized in the following proposition:

Proposition 1. *Let (\mathcal{Y}, g) a factor of the system (\mathcal{X}, f) . Then:*

1. for all $j \leq k$, $p \in \text{Per}_k(f) \implies \varphi(p) \in \text{Per}_j(g)$, where $\text{Per}_n(h)$ stands for the set of points of period n for the iteration function h .
2. (\mathcal{X}, f) regular $\implies (\mathcal{Y}, g)$ regular,
3. (\mathcal{X}, f) transitive $\implies (\mathcal{Y}, g)$ transitive.

So if (\mathcal{X}, f) is chaotic as defined by Devaney, then (\mathcal{Y}, g) is chaotic too.

Having these materials in mind, it is now possible to measure the Lyapunov exponent of some CBC mode of operations. To do so, we will follow the canvas described hereafter. In Section 2, some basic reminders are given. The semiconjugacy allowing the exponent evaluation is described in Section 3. In the next one, the consequences of such a semi-conjugacy are outlined, and the exponent is computed. This article ends by a conclusion section where our contribution is summarized and intended future work is outlined.

2 Basic Recalls

2.1 The Cipher Block Chaining (CBC) mode

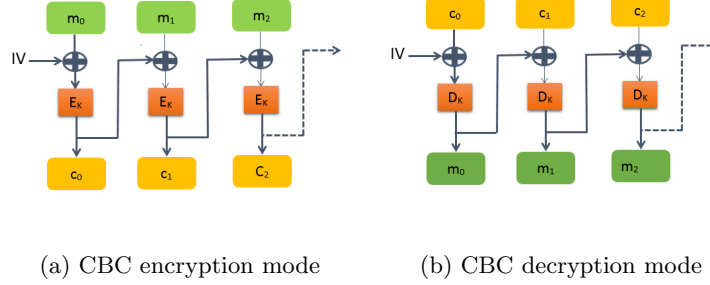
The CBC block cipher mode of operation presents a very popular way of encryption that is used in numerous applications, despite the fact that encryption in this mode can be performed only using one thread. Cipher block chaining is a block cipher mode that provides confidentiality but not message integrity in cryptography. The operating principle of this mode is to add XOR each subsequent plain-text block to a cipher-text one that was previously received, see Figure 1. Each subsequent cipher-text block depends on the previous one. Finally, the first plain-text block is added XOR to a random Initialization Vector (commonly referred to as IV). This vector has the same size as all plain-text blocks.

To decrypt cipher-text blocks, one should add XOR output data from decryption algorithm to previous cipher-text blocks. The receiver knows all cipher-text blocks just after obtaining encoded the message, thus he can decrypt the message using many threads simultaneously. If one bit of a plain-text message is damaged (for instance, because of some earlier transmission error), all subsequent cipher-text blocks will be damaged and it will be never possible to decrypt the cipher-text received from this plain-text. As opposed to that, if one cipher-text bit is damaged, only two received plain-text blocks will be damaged.

Finally, note that a message that is to be encrypted using the CBC mode, should be extended until being as long as a multiple of a single block length.

2.2 Modeling the CBC mode as a dynamical system

Our modeling follows a same canvas than what has been done for hash functions [8,1] or pseudo-random number generation [9]. Let us consider the CBC mode of operation with a keyed encryption function $\varepsilon_k : B^N \rightarrow B^N$ depending on a secret key k , where N is the size for the block cipher, and $\mathcal{D}_k : B^N \rightarrow B^N$ is the associated decryption function, which is such that $\forall k, \varepsilon_k \circ \mathcal{D}_k$ is the identity function. We define the Cartesian product $\mathcal{X} = B^N \times \mathcal{S}_N$, where:

**Fig. 1.** CBC mode of operation

- $B = \{0, 1\}$ is the set of Boolean values,
- $\mathcal{S}_N = 0, 2^N - 1^N$, the set of infinite sequences of natural integers bounded by $2^N - 1$, or the set of infinite N -bits block messages,

in such a way that \mathcal{X}_N is constituted by couples of internal states of the mode of operation together with sequences of block messages. Let us consider the initial function:

$$i : \mathcal{S}_N \longrightarrow 0, 2^N - 1$$

$$(m^i)_{i \in N} \longmapsto m^0$$

that returns the first block of a (infinite) message, and the shift function:

$$\sigma : \mathcal{S}_N \longrightarrow \mathcal{S}_N$$

$$(m^0, m^1, m^2, \dots) \longmapsto (m^1, m^2, m^3, \dots)$$

which removes the first block of a message. Let m_j be the j -th bit of integer, or block message, $m \in 0, 2^N - 1$, expressed in the binary numeral system, and when counting from the left. We define:

$$F_f : B^N \times 0, 2^N - 1 \longrightarrow B^N$$

$$(x, m) \longmapsto (x_j + f(x)_j)_{j=1..N}$$

This function returns the inputted binary vector x , whose m_j -th components x_{m_j} have been replaced by $f(x)_{m_j}$, for all $j = 1..N$ such that $m_j = 1$. In case where f is the vectorial negation, this function will correspond to one XOR between the clair text and the previous encrypted state.

Denote by f_0 the vectorial negation. So the CBC mode of operation can be rewritten in a condensed way, as follows.

$$\begin{cases} X^0 = (IV, m) \\ X^{n+1} = (\mathcal{E}_k \circ F_{f_0}(i(X_1^n), X_2^n), \sigma(X_1^n)) \end{cases} \quad (1)$$

For any given $g : 0, 2^N - 1 \times B^N \longrightarrow B^N$, we denote $G_g(X) = (g(i(X_1), X_2); \sigma(X_1))$ (when $g = \mathcal{E}_k \circ F_{f_0}$, we obtain one cypher block of the CBC, as depicted in

Figure 1). So the recurrent relation of Eq.(1) can be rewritten in a condensed way, as follows.

$$X^{n+1} = G_{\mathcal{E}_k \circ F_{f_0}}(X^n). \quad (2)$$

With such a rewriting, one iterate of the discrete dynamical system above corresponds exactly to one cypher block in the CBC mode of operation. Note that the second component of this system is a subshift of finite type, which is related to the symbolic dynamical systems known for their relation with chaos [10].

We then have defined a distance on \mathcal{X}_N as follows: $d((x, m); (\tilde{x}, \tilde{m})) = d_e(x, \tilde{x}) + d_m(m, \tilde{m})$, where [11]:

$$\begin{cases} d_e(x, \tilde{x}) = \sum_{k=1}^N \delta(x_k, \tilde{x}_k) \\ d_m(m, \tilde{m}) = \frac{9}{N} \sum_{k=1}^{\infty} \frac{\sum_{i=1}^N |m_i - \tilde{m}_i|}{10^k}. \end{cases}$$

in which $\delta(x, y) = 1$ if $x = y$, else it is 0. Using this modeling, we have been able to prove that [11],

Theorem 1. *The CBC mode of operation $G_{\mathcal{E}_k \circ F_{f_0}}$ is chaotic, as defined by Devaney [12], on the topological space (\mathcal{X}, d) . This means that $G_{\mathcal{E}_k \circ F_{f_0}}$ has on (\mathcal{X}, d) the properties of:*

- regularity: *its set of periodic points is dense in \mathcal{X}_N (for any point x in \mathcal{X}_N , any neighborhood of x contains at least one periodic point).*
- topologically transitivity: *for any pair of open sets $U, V \subset \mathcal{X}_N$, there exists an integer $k > 0$ such that $G_{\mathcal{E}_k \circ F_{f_0}}^k(U) \cap V \neq \emptyset$.*
- sensitive dependence on initial conditions: *there exists $\delta > 0$ such that, for any $x \in \mathcal{X}_N$ and any neighborhood V of x , there exist $y \in V$ and $n > 0$ such that*

$$d(G_{\mathcal{E}_k \circ F_{f_0}}^n(x), G_{\mathcal{E}_k \circ F_{f_0}}^n(y)) > \delta.$$

This result has been extended in [13], in which both expansivity and sensibility of symmetric cyphers have been regarded in the case of the CBC mode of operation. However, all these results of qualitative and quantitative disorder have been stated on an exotic phase space \mathcal{X}_N , equipped with a distance d very different from the usual Euclidian one. Our objective is now to translate them in a more usual situation, namely the real line equipped with its usual order topology. To do so, a topological semi-conjugacy must be introduced. Such a formulation will make it possible to evaluate the Lyapunov exponent of the CBC mode, as the latter will be described by a differentiable function on R .

3 A Topological Semi-conjugacy

3.1 The phase space is an interval of the real line

Toward a topological semi-conjugacy We show, by using a topological semi-conjugacy, that CBC mode can be described on a real interval. In what follows

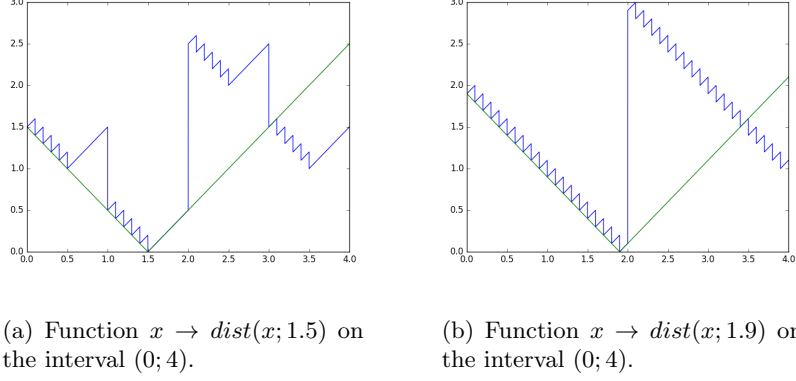


Fig. 2. Comparison between D (in blue) and the Euclidean distance (in green).

and for easy understanding, we will assume that $\mathbf{N} = 10$. However, an equivalent formulation of the following can be easily obtained by replacing the base 10 by any base \mathbf{N} .

Definition 3. The function $\varphi : \mathcal{S}_{10} \times B^{10} \rightarrow [0, 2^{10}[$ is defined by:

$$\begin{aligned} \varphi : \quad \mathcal{X}_{10} = \mathcal{S}_{10} \times B^{10} &\longrightarrow [0, 2^{10}[\\ ((S_0, S_1, \dots); (E_0, \dots, E_9)) &\longmapsto \varphi((S, E)) \end{aligned}$$

where $(S, E) = ((S_0, S_1, \dots); (E_0, \dots, E_9))$, and $\varphi((S, E))$ is the real number:

- whose integral part e is $\sum_{k=0}^9 2^{9-k} E_k$, that is, the binary digits of e are $E_0 E_1 \dots E_9$.
- whose decimal part s is equal to $s = 0, S_0 S_1 S_2 \dots = \sum_{k=1}^{+\infty} 10^{-k} S^{k-1}$.

φ realizes the association between a point of \mathcal{X}_{10} and a real number into $[0, 2^{10}[$. We must now translate the CBC process $G_{\mathcal{E}_k \circ F_{f_0}}$ on this real interval. To do so, two intermediate functions over $[0, 2^{10}[$ must be introduced:

Definition 4. Let $x \in [0, 2^{10}[$ and:

- e_0, \dots, e_9 the binary digits of the integral part of x : $[x] = \sum_{k=0}^9 2^{9-k} e_k$.
- $(s_k)_{k \in \mathbb{N}}$ the digits of x , where the chosen decimal decomposition of x is the one that does not have an infinite number of 9: $x = [x] + \sum_{k=0}^{+\infty} s_k 10^{-k-1}$.

e and s are thus defined as follows:

$$\begin{aligned} e : [0, 2^{10}[&\longrightarrow B^{10} \\ x &\longmapsto (e_0, \dots, e_9) \end{aligned}$$

and

$$\begin{aligned} s : [0, 2^{10}[&\longrightarrow [0, 9^N \\ x &\longmapsto (s_k)_{k \in N} \end{aligned}$$

We are now able to define the function g , whose goal is to translate the CBC mode $G_{\mathcal{E}_k \circ F_{f_0}}$ on an interval of R .

Definition 5. $g : [0, 2^{10}[\longrightarrow [0, 2^{10}[$ is defined by:

$$\begin{aligned} g : [0, 2^{10}[&\longrightarrow [0, 2^{10}[\\ x &\longmapsto g(x) \end{aligned}$$

where $g(x)$ is the real number of $[0, 2^{10}[$ defined bellow:

- its integral part is the number, encrypted by ε_k , whose binary decomposition equal to e'_0, \dots, e'_9 , with:

$$e'_i = \begin{cases} e(x)_i & \text{if } m_i^0 = 0 \\ e(x)_i + 1 \pmod{2} & \text{if } m_i^0 = 1 \end{cases}$$

- whose decimal part is $m_0^1, \dots, m_9^1, m_0^2, \dots, m_9^2, m_0^3, \dots, m_9^3, \dots$

In other words, if $x = \sum_{k=0}^9 2^{9-k} e_k + \sum_{k=0}^{+\infty} s^k 10^{-k-1}$, then:

$$g(x) = \sum_{k=0}^9 2^{9-k} \varepsilon_k(e_k + \delta(k, s_0) \pmod{2}) + \sum_{k=0}^{+\infty} s^{k+1} 10^{-k-1}.$$

Defining a metric on $[0, 2^{10}[$ Numerous metrics can be defined on the set $[0, 2^{10}[$, the most usual one being the Euclidean distance $\Delta(x, y) = \sqrt{y^2 - x^2}$. This Euclidean distance does not reproduce exactly the notion of proximity induced by our first distance d on \mathcal{X} . Indeed d is finer than Δ . This is the reason why we have to introduce the following metric:

Definition 6. Let $x, y \in [0, 2^{10}[$. D denotes the function from $[0, 2^{10}[^2$ to R^+ defined by: $D(x, y) = D_e(e(x), e(y)) + D_s(s(x), s(y))$, where:

$$D_e(E, \tilde{E}) = \sum_{k=0}^9 \delta(E_k, \tilde{E}_k), \quad \text{and} \quad D_s(S, \tilde{S}) = \sum_{k=1}^{\infty} \frac{|s_k - \tilde{s}^k|}{10^k}.$$

Proposition 2. D is a distance on $[0, 2^{10}[$.

Proof. The three axioms defining a distance must be checked.

- $D \geq 0$, because everything is positive in its definition. If $D(x, y) = 0$, then $D_e(x, y) = 0$, so the integral parts of x and y are equal (they have the same binary decomposition). Additionally, $D_s(x, y) = 0$, then $\forall k \in N^*, s(x)^k = s(y)^k$. In other words, x and y have the same k -th decimal digit, $\forall k \in N^*$. And so $x = y$.

- $D(x, y) = D(y, x)$.
- Finally, the triangular inequality is obtained due to the fact that both δ and $|x - y|$ satisfy it.

The convergence of sequences according to D is not the same than the usual convergence related to the Euclidean metric. For instance, if $x^n \rightarrow x$ according to D , then necessarily the integral part of each x^n is equal to the integral part of x (at least after a given threshold), and the decimal part of x^n corresponds to the one of x “as far as required”. To illustrate this fact, a comparison between D and the Euclidean distance is given in Figure 2. These illustrations show that D is richer and more refined than the Euclidean distance, and thus is more precise.

The semi-conjugacy It is now possible to define a topological semi-conjugacy between \mathcal{X}_N and an interval of R which makes possible to translate the action of the CBC encryption on a message in the form of a recurrent sequence on the interval $[0, 2^{10}[$.

Theorem 2. *CBC mode on the phase space \mathcal{X}_N are simple iterations on R , which is illustrated by the semi-conjugacy of the diagram below:*

$$\begin{array}{ccc} (S_{10} \times B^{10}, d) & \xrightarrow{G_{\varepsilon_k \circ F_{f_0}}} & (S_{10} \times B^{10}, d) \\ \varphi \downarrow & & \downarrow \varphi \\ ([0, 2^{10}[, D) & \xrightarrow{g} & ([0, 2^{10}[, D) \end{array}$$

Proof. φ has been constructed in order to be continuous and onto.

In other words, \mathcal{X}_N is approximately equal to $[0, 2^N[$.

Comparing the metrics of $[0, 2^N[$ The two propositions below allow us to compare our two distances on $[0, 2^N[$:

Proposition 3. *The identity function $Id: ([0, 2^N[, \Delta) \rightarrow ([0, 2^N[, D)$ is not continuous.*

Proof. The sequence $x^n = 1, 999 \dots 999$ constituted by n 9’s as digits, is such that:

- $\Delta(x^n, 2) \rightarrow 0$.
- But $D(x^n, 2) \geq 1$, so $D(x^n, 2)$ does not converge to 0.

The sequential characterization of the continuity allows us to conclude the proposition.

A contrario:

Proposition 4. *$Id: ([0, 2^N[, D) \rightarrow ([0, 2^N[, \Delta)$ is continuous.*

Proof. On the one hand, if $D(x^n, x) \rightarrow 0$, then $D_e(x^n, x) = 0$ at least after a given rank, because D_e produces only integers. So, after a given rank, the whole integral parts of x^n are equal to the one of x .

On the other hand, $D_s(x^n, x) \rightarrow 0$, so $\forall k \in \mathbb{N}^*, \exists N_k \in \mathbb{N}, n \geq N_k \Rightarrow D_s(x^n, x) \leq 10^{-k}$. Which means that for all k , it exists a rank N_k after which all the x^n 's have the same k first digits, which are the ones of x . We can deduce from all these aspects that $\Delta(x^n, x) \rightarrow 0$, which leads to the claimed result.

We can conclude from the previous propositions that the introduced metric is more precise than the Euclidean distance. In other words:

Proposition 5. *The distance D is finer than the Euclidean distance Δ .*

This proposition can be reformulated as follows:

- The topology generated by Δ is inside the one generated by D .
- D has more open sets than Δ .
- Figuratively, D allows a better observation, leading to more details than Δ .
- Finally, it is harder to converge with the topology τ_D generated by D , than with the one generated by Δ , and denoted τ_Δ .

Impact of the topology To alleviate notations, let us denote by \mathcal{X}_τ the topological space (\mathcal{X}, τ) , and by $\mathcal{V}_\tau(x)$ the set of all neighborhoods of x when considering the τ topology. When there is no ambiguity, we will simply use the notation $\mathcal{V}(x)$.

Theorem 3. *Let $\mathcal{X}_\mathbb{N}$ be a set, and τ, τ' two topologies on $\mathcal{X}_\mathbb{N}$ such that τ' is finer than τ . Let $f : \mathcal{X} \rightarrow \mathcal{X}_\mathbb{N}$ be a function continuous for both τ and τ' .*

If $(\mathcal{X}_{\tau'}, f)$ is chaotic according to Devaney, then (\mathcal{X}_τ, f) is chaotic too.

Proof. Let us firstly introduce the transitivity of (\mathcal{X}_τ, f) .

Let ω_1, ω_2 be two open sets of τ . Then $\omega_1, \omega_2 \in \tau'$, as τ' is finer than τ . But f is τ' -transitive, so we can deduce that $\exists n \in \mathbb{N}, \omega_1 \cap f^{(n)}(\omega_2) = \emptyset$. As a consequence, f is τ -transitive.

Let us now establish the regularity of (\mathcal{X}_τ, f) , i.e., for all $x \in \mathcal{X}_\mathbb{N}$, and for all τ -neighborhood V of x , a periodic point for f can be found in V .

Let $x \in \mathcal{X}_\mathbb{N}$ and $V \in \mathcal{V}_\tau(x)$ a τ -neighborhood of x . By definition of the neighborhood notion, $\exists \omega \in \tau, x \in \omega \subset V$.

But $\tau \subset \tau'$, so $\omega \in \tau'$, and as a consequence, $V \in \mathcal{V}_{\tau'}(x)$. As $(\mathcal{X}_{\tau'}, f)$ is regular, it exists a periodic point for f in V , and the regularity of (\mathcal{X}_τ, f) is proven.

3.2 CBC mode described as a real function

We will now show that the g function is a piecewise linear one: it is linear on each interval having the form $\left[\frac{n}{10}, \frac{n+1}{10} \right]$, $n \in 0; 2^{10} \times 10$ and its slope is equal to 10.

Proposition 6. *CBC mode g defined on R have derivatives of all orders on $[0, 2^{10}]$, except on the 10241 points in I defined by $\left\{ \frac{n}{10} \mid n \in 0; 2^{10} \times 10 \right\}$.*

Furthermore, on each interval of the form $\left[\frac{n}{10}, \frac{n+1}{10} \right]$, with $n \in 0; 2^{10} \times 10$, g is a linear function, having a slope equal to 10: $\forall x \notin I, g'(x) = 10$.

Proof. Let $I_n = \left[\frac{n}{10}, \frac{n+1}{10} \right]$, with $n \in 0; 2^{10} \times 10$. All the points of I_n have the same integral part e and the same decimal part s_0 : on the set I_n , functions $e(x)$ and $x \mapsto s(x)^0$ of Definition 4 only depend on n . So all the images $g(x)$ of these points x :

- Have the same integral part, which is $\varepsilon_k(e)$, except probably the bit number s_0 . In other words, this integer has approximately the same binary decomposition than $\varepsilon_k(e)$, the sole exception being the digit s_0 (this number is then either $\varepsilon_k(e + 2^{10-s_0})$ or $\varepsilon_k(e - 2^{10-s_0})$, depending on the parity of s_0 , *i.e.*, it is equal to $\varepsilon_k(e + (-1)^{s_0} \times 2^{10-s_0})$).
- A shift to the left has been applied to the decimal part y , losing by doing so the common first digit s_0 . In other words, y has been mapped into $10 \times y - s_0$.

To sum up, the action of g on the points of I is as follows: first, make a multiplication by 10, and second, add the same constant to each term, which is $\frac{1}{10} (\varepsilon_k(e + (-1)^{s_0} \times 2^{10-s_0})) - s_0$.

Remark 1. CBC mode is then an element of the large family of functions that are both chaotic and piecewise linear (like the tent map [4,5]).

We are now able to evaluate the Lyapunov exponent of our chaotic CBC mode, which is now described by the iterations on R of the g function introduced in Definition 5.

4 Disorder generated by CBC formulated on R

4.1 Devaney's chaos on the real line

We have established in [11] that the CBC mode of operation $(G_{\mathcal{E}_k \circ F_{f_0}}, \mathcal{X}_d)$ satisfies the Devaney's definition of chaos. From the semi-conjugacy, we can deduce that it is the case too for the mode of operation on R with the order topology, as:

- $(G_{\mathcal{E}_k \circ F_{f_0}}, \mathcal{X}_d)$ and $(g, [0, 2^{10}[_D)$ are semi-conjugated by φ ,
- $\varphi(g, [0, 2^{10}[_D)$ is a chaotic system according to Devaney, because the semi-conjugacy preserves such a character [7].
- But the topology generated by D is finer than the one generated by the euclidean distance Δ – which is the order topology [5].
- According to Theorem 3, we can deduce that the CBC mode of operation g is chaotic, as defined by Devaney, for the usual order topology on R .

We can formulate this result as follows.

Theorem 4. *The CBC mode of operation g on R satisfies the Devaney's chaos property, when R is equipped with its usual topology (the order one).*

Indeed this result is weaker than Theorem 1, that established the chaos of iterates on a finer topology. This can be explained in the following figurative manner. By using tools that are usual in the discrete dynamical system field,

we can only observe disorder in the iterations of the CBC mode of operation (Theorem 4). And even if we considered an higher resolution, and more powerful tools than the ones that are commonly used, we still fail in finding order in such a chaos (Theorem 1).

Result of Theorem 4 is still precious. Indeed, we have started to formulate the mode of operation on a set different from the one commonly considered (\mathcal{X}_N instead of R), to be as close as possible to the computer machine (dealing with bounded integer), and so to prevent from losing disorder properties when switching from theory to computer program. It is to be feared that this introduction of discrete iterations can only be paid by the obtention of disorders of lower quality. In other words, perhaps we moved from a situation of a good disorder lost when computed on finite state machines, to a disorder preserved but of poor quality. Theorem 4 shows exactly the contrary of this claim.

4.2 Evaluation of the Lyapunov Exponent

Let $\mathcal{L} = \{x^0 \in [0, 2^{10}[\mid \forall n \in N, x^n \notin I\}$, where I is the set of points in the real interval where g is not differentiable (as it is explained in Proposition 6). We have the following result.

Theorem 5. *Let us consider the CBC mode of operation with block size of N . Then, $\forall x^0 \in \mathcal{L}$, its Lyapunov exponent is equal to $\lambda(x^0) = \ln(N)$.*

Proof. The function g is piecewise linear, with a slop of 10, as $g'(x) = 10$ where g is differentiable. Then $\forall x \in \mathcal{L}$, $\lambda(x) = \lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{i=1}^n \ln |g'(x^{i-1})| = \lim_{n \rightarrow +\infty} \frac{1}{n} \sum_{i=1}^n \ln |10| = \lim_{n \rightarrow +\infty} \frac{1}{n} n \ln |10| = \ln 10$.

Remark 2. The set of initial vectors for which this exponent is not defined is countable. This is indeed the initial conditions such that an iteration value will be a number having the form $\frac{n}{10}$, with $n \in N$. We can reach such a real number only by starting iterations on a *decimal number*, as this latter must have a finite fractional part.

Remark 3. For a system having N cells, we will find, mutatis, an infinite uncountable set of initial conditions $x^0 \in [0; 2^N[$ such that $\lambda(x^0) = \ln(N)$.

So, it is possible to make the Lyapunov exponent of our CBC mode as large as possible, depending on the size of the block message.

5 Conclusion and Future work

We have available now a new quantitative property concerning the CBC mode of operation: its Lyapunov exponent is equal to $\ln(N)$, where N is the size of the block message. This exponent allows to quantify how the ignorance on the exact initial vector increases after several iterations of the mode of operation. It illustrates the disorder generated by iterations of such a process, reinforcing its chaotic nature.

Using the semi-conjugacy described here, it will be possible in a future work to compare the topological behavior of various modes of operation on \mathcal{X}_N and on R . This semi-conjugacy can be used to investigate various interesting directions, as to have a new understanding of the modes of operations while considering them as iterations on the real line. Their dynamics can be better understood thanks to the use of mathematical analysis tools. Finally, elements of comparison with usual iteration ways can be provided too, as we will consider the same iteration set, namely the real line.

References

1. Christophe Guyeux and Jacques Bahi. A topological study of chaotic iterations. application to hash functions. In *CIPS, Computational Intelligence for Privacy and Security*, volume 394 of *Studies in Computational Intelligence*, pages 51–73. Springer, 2012. Revised and extended journal version of an IJCNN best paper.
2. J. M. Bahi and C. Guyeux. Topological chaos and chaotic iterations, application to hash functions. In *WCCI'10, IEEE World Congress on Computational Intelligence*, pages 1–7, Barcelona, Spain, July 2010. Best paper award.
3. David Arroyo, Gonzalo Alvarez, and Veronica Fernandez. On the inadequacy of the logistic map for cryptographic applications. *arXiv preprint arXiv:0805.4355*, 2008.
4. Yong Wang, Kwok-Wo Wong, Xiaofeng Liao, and Tao Xiang. A block cipher with dynamic s-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation*, 14(7):3089–3099, 2009.
5. Christophe Guyeux. *Le désordre des itérations chaotiques - Applications aux réseaux de capteurs, à la dissimulation d'information, et aux fonctions de hachage*. Éditions Universitaires Européennes, 2012. ISBN 978-3-8417-9417-8. 362 pages. Publication de la thèse de doctorat.
6. David Richeson and Jim Wiseman. Chain recurrence rates and topological entropy. *Topology and its Applications*, 156(2):251–261, 2008.
7. Enrico Formenti. *Automates cellulaires et chaos : de la vision topologique la vision algorithmique*. PhD thesis, École Normale Supérieure de Lyon, 1998.
8. Jacques Bahi and Christophe Guyeux. Hash functions using chaotic iterations. *Journal of Algorithms and Computational Technology*, 4(2):167–181, 2010.
9. Jacques Bahi, Xiaole Fang, Christophe Guyeux, and Qianxue Wang. Evaluating quality of chaotic pseudo-random generators. application to information hiding. *IJAS, International Journal On Advances in Security*, 4(1-2):118–130, 2011.
10. Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, 1995.
11. Abdessalem Abidi, Qianxue Wang, Belgacem Bouallegue, Mohsen Machhout, and Christophe Guyeux. Proving chaotic behavior of cbc mode of operation. *International Journal of Bifurcation and Chaos*, 26(07):1650113, 2016.
12. R. L. Devaney. *An Introduction to Chaotic Dynamical Systems*. Addison-Wesley, Redwood City, CA, 2nd edition, 1989.
13. Abdessalem Abidi, Qianxue Wang, Belgacem Bouallegue, Mohsen Machhout, and Christophe Guyeux. Quantitative evaluation of chaotic cbc mode of operation. In *Advanced Technologies for Signal and Image Processing (ATSIP), 2016 2nd International Conference on*, pages 88–92. IEEE, 2016.