Conditions to have a well-disordered dynamics in the CBC Mode of Operation

Abdessalem Abidi, Christophe Guyeux, Belgacem Bouallègue, Mohsen Machhout

Conditions to have a well-disordered dynamics in the CBC Mode of Operation

Abdessalem Abidi
Electronics and Microelectronics Lab.
University of Monastir, Tunisia
Email: abdessalemabidi9@gmail.com

Christophe Guyeux
FEMTO-ST Institute, UMR 6174 CNRS,
University of Franche-Comté, France

Belgacem Bouallègue
and Mohsen Machhout
Electronics and Microelectronics Lab.
University of Monastir, Tunisia

***Abstract*—In cryptography, Cipher Block Chaining (CBC) mode of operation presents a very popular way of encryption that is used in numerous applications. In our previous research work, we have been proven that, under some conditions, this mode of operation can exhibit a chaotic behavior according to the reputed definition of Devaney. The quantitative study of this chaotic CBC has been deepened later by evaluating both its level of sensibility and of expansivity. In this paper, our objective is now to further develop the evaluation of the CBC dynamics, by obtaining a complete topological study of this mode of operation. Such an evaluation encompasses both the qualitative property of topological mixing and its level of topological entropy, which is indeed a quantitative measure of disorder.**

I. Introduction

Block ciphers, like the Data Encryption Standard (DES) or the 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. 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 the block cipher modes of operation. There are several modes of operation and each one possesses its own characteristics and its specific security properties. In this article, we are only interested in one of these modes, namely the cipher block chaining (CBC) mode, and we will study its dynamical behavior of chaos.

The chaos theory that has been consider in this article is the Devaney's topological one and its ramifications [1]. Being reputed as one of the best mathematical definition of chaos, this theory offers a framework with qualitative and quantitative tools to evaluate the notion of unpredictability [2]. As an application of our fundamental results, It has been interested in the area of information safety and security. Specifically, the contribution belongs to the field of the cipher block chaining modes of operation.

In [3], we have been started to give mathematical proofs that emphasize the chaotic behavior of the CBC mode of operation. Thereafter, in [4], we have been stated that in addition to being chaotic as defined in Devaney's formulation, this mode is indeed largely sensible to initial errors or modification on either the Initialization Vector IV or the message to encrypt. Its expansivity has been regarded too, but this property is not satisfied as it has been established thanks to a counter example. In this new article, we have been intend to deepen the topological study of this CBC mode of operation in order to obtain a complete mathematical overview of its dynamics.

The remainder of this research work is organized as follows. In the next section, some basic definitions related to chaos and cipher block chaining mode of operation will be recalled. Previously obtained results are recalled in Section III. Sections IV and V contain the main contribution of this article: the first one evaluates the topological mixing of the CBC mode of operation, while the second one focuses on its topological entropy. This article ends with a conclusion section where the contribution is summarized and intended future work is presented.

II. Basic recalls

This section is devoted to basic definitions and terminologies in the field of topological chaos and in the one of block cipher mode of operation.

A. Devaney's Chaotic Dynamical Systems

In the remainder of this article,

m_n denotes the n^{th} block message of a sequence S while m^j stands for the $j-th$ bit of integer of the block message $m \in [\![0, 2^{\mathsf{N}} - 1]\!]$, expressed in the binary numeral system and x_i stands for the i^{th} component of a vector x.

$\mathcal{X}^{\mathbb{N}}$ is the set of all sequences whose elements belong to $\mathcal{X}$.

$f^{\circ k} = f \circ ... \circ f$ is for the k^{th} composition of a function f. $\mathbb{N}$ is the set of natural (non-negative) numbers, while $\mathbb{N}^*$ stands for the positive integers $1, 2, 3, \ldots$

Finally, the following notation is used: $[\![1; N]\!] = \{1, 2, \ldots, N\}$.

Consider a topological space $(\mathcal{X}, \tau)$, where τ represents a family of subsets of $\mathcal{X}$, and a continuous function $f : \mathcal{X} \to \mathcal{X}$ on $(\mathcal{X}, \tau)$.

Definition 1 The function f is *topologically transitive* if, for any pair of nonempty open sets $\mathcal{U}, \mathcal{V} \subset \mathcal{X}$, there exists an integer $k > 0$ such that $f^{\circ k}(\mathcal{U}) \cap \mathcal{V} \neq \varnothing$.

Definition 2 An element x is a *periodic point* for f of period $n \in \mathbb{N}$, $n > 1$, if $f^{\circ n}(x) = x$ and $f^{\circ k}(x) \neq x, 1 \leq k \leq n$.

Definition 3 f is *regular* on $(\mathcal{X}, \tau)$ if the set of periodic points for f is dense in $\mathcal{X}$: for any point x in $\mathcal{X}$, any neighborhood of x contains at least one periodic point.

Definition 4 The function f has *sensitive dependence on initial conditions* on the metric space $(\mathcal{X}, d)$ if there exists $\delta > 0$ such that, for any $x \in \mathcal{X}$ and any neighborhood $\mathcal{V}$ of x, there exist $y \in \mathcal{V}$ and $n > 0$ such that the distance d between the results of their n^{th} composition, $f^{\circ n}(x)$ and $f^{\circ n}(y)$, is greater than δ:

$$d\left(f^{\circ n}(x), f^{\circ n}(y)\right) > \delta.$$

δ is called the *constant of sensitivity* of f.

Definition 5 (Devaney's formulation of chaos [1]) The function f is *chaotic* on a metric space $(\mathcal{X}, d)$ if f is regular, topologically transitive, and has sensitive dependence on initial conditions.

Banks *et al.* have proven in [5] that when f is regular and transitive on a metric space $(\mathcal{X}, d)$, then f has the property of sensitive dependence on initial conditions. This is why chaos can be formulated too in a topological space $(\mathcal{X}, \tau)$: in that situation, chaos is obtained when f is regular and topologically transitive. Note that the transitivity property is often obtained as a consequence of the strong transitivity one, which is defined below.

Definition 6 f is *strongly transitive* on $(\mathcal{X}, d)$ if, for all point $x, y \in \mathcal{X}$ and for all neighborhood $\mathcal{V}$ of x, it exists $n \in \mathbb{N}$ and $x' \in \mathcal{V}$ such that $f^{\circ n}(x') = y$.

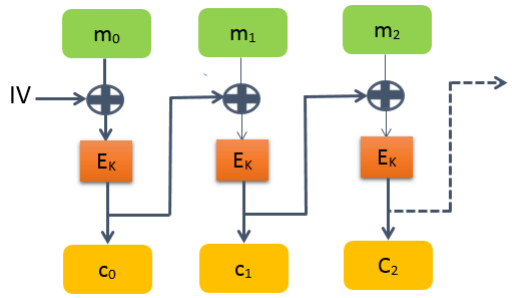
B. CBC properties

As what has been already defined, a mode of operation is an algorithm that uses a block cipher to provide an information service such as confidentiality or authenticity. The most commonly used mode of operation in recent decades is the cipher block chaining CBC. In what follows, it will be seen how this mode works in practice.

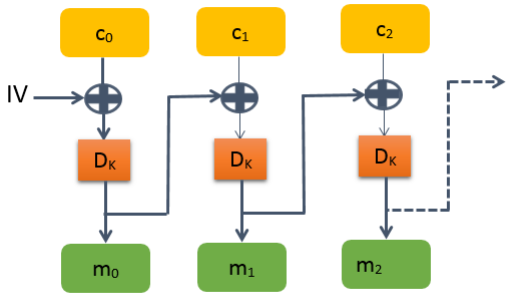
1) Initialization vector IV: Like some other modes of operation, the CBC one requires not only a plaintext but also an initialization vector (denoted as IV in what follows). An IV is an arbitrary number that must be generated for each execution of the encryption operation. For the decryption algorithm, the vector used must be the same, see Figure 1. The use of this vector prevents repetition in data encryption. So, it offers the benefit to make this operation more difficult for a hacker. Indeed, it deprives him to find patterns and break a cipher. The length of the initialization vector (the number of bits or bytes it contains) depends on the method of encryption. It is usually comparable to the length of the encryption key or block of the cipher in use.

2) CBC mode characteristics: In cryptography, Cipher Block Chaining is a block cipher mode that provides confidentiality but not message integrity. It offers a solution to most of the problems presented by the Electronic Code Book (ECB) mode; thanks to CBC mode, the encryption will depend not only on the plaintext, but also on all preceding blocks. More precisely, each block of plaintext is XORed immediately with the previous cipher text block before being encrypted (*i.e.*, the binary operator XOR is applied between two stated blocks). For the first block, the initialization vector acts as the previous cipher text block, see Figure 1. CBC mode possesses several advantages. In fact, the same plaintext is encrypted differently in the case of different initialization vectors. In addition, the encryption operation of each block depends on the preceding one, so any modification in the order of the cipher text block makes the decryption operation unrealizable. Furthermore, if a transmission error affects the encrypted data, for example the C_i block, so only m_i and m_{i+1} blocks will be influenced by this error while the remained blocks will be determined correctly. Conversely, the CBC mode is characterized by two main drawbacks. The first one is that encryption is sequential (*i.e.*, it cannot be parallelized). The second one is that the initial message should be padded to a multiple of the cipher block size.

In the next section, the previous results that has been detailed respectively in [3] and [4] will be summarized.



(a) CBC encryption mode



(b) CBC decryption mode

Fig. 1. CBC mode of operation

III. Previously obtained results

A. Modeling the CBC mode as a dynamical system

The modeling follows a same canvas as what has been done for hash functions [6], [7] or pseudorandom number generation [8].

Let us consider the CBC mode of operation with a keyed encryption function $\mathcal{E}_\kappa : \mathbb{B}^{\mathsf{N}} \to \mathbb{B}^{\mathsf{N}}$ depending on a secret key κ, where N is the size for the block cipher, and $\mathcal{D}_\kappa : \mathbb{B}^{\mathsf{N}} \to \mathbb{B}^{\mathsf{N}}$ is the associated decryption function, which is such that $\forall \kappa, \mathcal{E}_\kappa \circ \mathcal{D}_\kappa$ is the identity function. We define the Cartesian product $\mathcal{X} = \mathbb{B}^{\mathsf{N}} \times \mathcal{S}_{\mathsf{N}}$, where:

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

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

$$\begin{array}{rccc} \iota : & \mathcal{S}_{\mathsf{N}} & \longrightarrow & [\![0, 2^{\mathsf{N}} - 1]\!] \\ & (m_i)_{i \in \mathbb{N}} & \longmapsto & m_0 \end{array}$$

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

$$\begin{array}{rccc} \sigma : & \mathcal{S}_{\mathsf{N}} & \longrightarrow & \mathcal{S}_{\mathsf{N}} \\ & (m_0, m_1, m_2, ...) & \longmapsto & (m_1, m_2, m_3, ...) \end{array}$$

that removes the first block of a message, when counting from the left. We define:

$$\begin{array}{rccc} F_f : & \mathbb{B}^{\mathsf{N}} \times [\![0, 2^{\mathsf{N}} - 1]\!] & \longrightarrow & \mathbb{B}^{\mathsf{N}} \\ & (x, m) & \longmapsto & \left(x_j m^j + f(x)_j \overline{m^j} \right)_{j=1..\mathsf{N}} \end{array}.$$

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 $j = 1..\mathsf{N}$ such that $m^j = 0$. In case where f is the vectorial negation, this function will correspond to one XOR between the plaintext and the previous encrypted state. The CBC mode of operation can be rewritten as the following dynamical system:

$$\left\{ \begin{array}{ll} X^0 = & (IV, m) \\ X^{n+1} = & \left(\mathcal{E}_\kappa \circ F_{f_0}\left(\iota(X_1^n), X_2^n\right), \sigma(X_1^n)\right) \end{array} \right. \quad (1)$$

For any given $g : [\![0, 2^{\mathsf{N}} - 1]\!] \times \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$, we denote $G_g(X) = (g(\iota(X_1), X_2); \sigma(X_1))$ (when $g = \mathcal{E}_\kappa \circ F_{f_0}$, we obtain one cipher block of the CBC, as depicted in Figure 1). The recurrent relation of Eq.(1) can be rewritten in a condensed way, as follows.

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

With such a rewriting, one iterate of the discrete dynamical system above corresponds exactly to one cipher block in the CBC mode of operation. Note that the second component of this system is a subshift of finite type that is related to the symbolic dynamical systems known for their relation with chaos [9]. Now, a distance on $\mathcal{X}$ as follows: $d((x, m); (\check{x}, \check{m})) = d_e(x, \check{x}) + d_m(m, \check{m})$ is defined, where:

$$\left\{ \begin{array}{ll} d_e(x, \check{x}) & = \sum_{k=1}^{\mathsf{N}} |x_k - \check{x}_k| \\ \\ d_m(m, \check{m}) & = \dfrac{9}{\mathsf{N}} \displaystyle\sum_{k=1}^{\infty} \dfrac{\sum_{i=1}^{\mathsf{N}} \left|m^i - \check{m}^i\right|}{10^k}. \end{array} \right.$$

This distance has been introduced to satisfy the following requirements:

- The integral part between two points X, Y of the topological space $\mathcal{X}$ corresponds to the number of

binary components that are different between the two internal states X_1 and Y_1.
- The k-th digit in the decimal part of the distance between X and Y is equal to 0 if and only if the k-th blocks of messages X_2 and Y_2 are equal. This desire is at the origin of the normalization factor $\frac{9}{\mathsf{N}}$.

B. Proofs of chaos

As mentioned in Definition 5, a function f is *chaotic* on $(\mathcal{X}, \tau)$ if f is regular and topologically transitive. It has been beagan in [10] by stating some propositions that are primarily required in order to proof the chaotic behavior of the CBC mode of operation.

Proposition 1 *Let $g = \mathcal{E}_\kappa \circ F_{f_0}$, where $\mathcal{E}_\kappa$ is a given keyed block cipher and $f_0 : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$, $(x_1, ..., x_{\mathsf{N}}) \longmapsto (\overline{x_1}, ..., \overline{x_{\mathsf{N}}})$ is the Boolean vectorial negation. The directed graph $\mathcal{G}_g$ is considered, where:*

- *vertices are all the N-bit words.*
- *there is an edge $m \in [\![0, 2^{\mathsf{N}} - 1]\!]$ from x to $\check{x}$ if and only if $g(m, x) = \check{x}$.*

If $\mathcal{G}_g$ is strongly connected, then G_g is strongly transitive.

Then it has been proven that,

Proposition 2 *If $\mathcal{G}_g$ is strongly connected, then G_g is regular.*

According to Propositions 1 and 2, It can be conclude that, depending on g, if the directed graph $\mathcal{G}_g$ is strongly connected, then the CBC mode of operation is chaotic according to Devaney, as established in our previous research work [3]. In this article and for illustration purpose, we have been also given some examples of encryption functions making this mode a chaotic one.

In the next section, some quantitative measures of chaos that have already been proven in previous research work will be recalled.

C. Quantitatives measures

In [4], these two following propositions have been respectively developed .

Proposition 3 *The CBC mode of operation is sensible to the initial condition, and its constant of sensibility is larger than the length N of the block size.*

Proposition 4 *The CBC mode of operation is not expansive.*

To sum up, CBC mode of operation is sensible to the initial conditions but it is not expansive.

IV. Topological mixing

The topological mixing is a strong version of transitivity.

Definition 7 A discrete dynamical system is said *topologically mixing* if and only if, for any couple of disjoint open set $\mathcal{U}, \mathcal{V} \neq \varnothing$, there exists an integer $n_0 \in \mathbb{N}$ such that, for all $n > n_0$, $f^{\circ n}(\mathcal{U}) \cap \mathcal{V} \neq \varnothing$.

Proposition 5 *$(\mathcal{X}, G_g)$ is topologically mixing.*

This result is an immediate consequence of the lemma below.

Lemma 1 *For any open ball $\mathcal{B} = \mathcal{B}((x, m), \varepsilon)$ of $\mathcal{X}$, an index n can be found such that $G_g^{\circ n}(\mathcal{B}) = \mathcal{X}$.*

Proof Let $\mathcal{B}$ be an open ball whose radius ε can be considered as strictly lower than 1, $\varepsilon < 1$.

All the elements of $\mathcal{B}$ have the same state x, and due to the definition of the chosen metric, they are such that an integer $k\,(= -\lfloor \log_{10}(\varepsilon) \rfloor)$ satisfies:

- all the strategies of $\mathcal{B}$ have the same k first block messages,
- after the index k, all values are possible.

Then, after k iterations, the new state of the system is $G_g^{\circ k}(x, m)_1$ and all the strategies are possibles (any point of the form $(G_g^{\circ k}(x, m)_1, \hat{\mathfrak{m}})$, with any $\hat{\mathfrak{m}} \in \mathcal{S}$, is reachable from $\mathcal{B}$).

Let $(x', m') \in \mathcal{X}$. We will prove that it can be reached by starting from $\mathcal{B}$. Indeed, let us consider the point $(\check{x}, \check{m})$ of $\mathcal{B}$ defined by:

- $\check{x} = x$
- $\forall i \leqslant k, \check{m}_i = m_i$,
- $\check{m}_{k+1} = G_g^{\circ k}((x, m))_1 \oplus \mathcal{D}_\kappa(x')$,
- $\forall i \geqslant k + 2, \check{m}_i = m'_{i-k-2}$.

This latter is such that:

$$\begin{aligned} G_g^{\circ k+1}((\check{x}, \check{m}))_1 &= G_g(G_g^{\circ k}((x, m))_1, \check{m}_{k+1})_1 \\ &= G_g(G_g^{\circ k}((x, m))_1, G_g^{\circ k}((x, m))_1 \oplus \mathcal{D}_\kappa(x'))_1 \\ &= \mathcal{E}_\kappa\left(G_g^{\circ k}((x, m))_1 \oplus \left(G_g^{\circ k}((x, m))_1 \oplus \mathcal{D}_\kappa(x')\right)\right) \\ &= \mathcal{E}_\kappa\left(\left(G_g^{\circ k}((x, m))_1 \oplus G_g^{\circ k}((x, m))_1\right) \oplus \mathcal{D}_\kappa(x')\right) \\ &= \mathcal{E}_\kappa\left(\mathcal{D}_\kappa(x')\right) \\ &= x' \end{aligned}$$

and $G_g^{\circ k+1}(\check{x}, \check{m})_2 = m'$.

This shows that (x', m') has been reached starting from $\mathcal{B}$. This fact concludes the proof of the lemma and of the proposition claimed previously.

V. Topological entropy

Another important tool to measure the chaotic behavior of a dynamical system is the topological entropy, which is defined only for compact topological spaces.

Before studying the entropy of CBC mode of operation, Then, $(\mathcal{X},\ d)$ is compact must be checked.

A. Compactness study

In this section, $(\mathcal{X}, d)$ is a compact topological space will be proven, in order to study its topological entropy later. Firstly, as $(\mathcal{X}, d)$ is a metric space, it is separated. It is however possible to give a direct proof of this result:

Proposition 6 *$(\mathcal{X}, d)$ is a separated space.*

PROOF Let $(x, w) \neq (\hat{\mathrm{x}}, \hat{\mathrm{w}})$ two points of $\mathcal{X}$.

1) If $x \neq \hat{\mathrm{x}}$, then the intersection between the two balls $\mathcal{B}\left((x, w), \frac{1}{2}\right)$ and $\mathcal{B}\left((\hat{\mathrm{x}}, \hat{\mathrm{w}}), \frac{1}{2}\right)$ is empty.
2) Else, it exists $k \in \mathbb{N}$ such that $w_k \neq \hat{\mathrm{w}}_k$, then the balls $\mathcal{B}\left((x, w), 10^{-(k+1)}\right)$ and $\mathcal{B}\left((\hat{\mathrm{x}}, \hat{\mathrm{w}}), 10^{-(k+1)}\right)$ can be chosen.

Now, the compactness of the metric space $(\mathcal{X}, d)$ by using the sequential characterization of compactness will be proven.

Proposition 7 *$(\mathcal{X}, d)$ is a compact space.*

PROOF Let $X = ((x_n, m_n))_{n\in\mathbb{N}}$ be a sequence of $\mathcal{X}$.

There is at least one Boolean vector that appears an infinite number of times in the first components of this sequence, as $\mathbb{B}^{\mathsf{N}}$ is finite. Let $\tilde{x}$ the lowest of them and I the (infinite) subsequence of X constituted by all the block messages having their first component equal to $\tilde{x}$.

The first block messages $(w_n)_0$ of the sequences $w_n \in [\![0, 2^{\mathsf{N}} - 1]\!]^{\mathbb{N}}$ (that are the second components of each couple in the infinite sequence I_0) all belong in the finite set $[\![0, 2^{\mathsf{N}} - 1]\!]$, and so at least one word of this finite set appears an infinite number of times in $((w_n)_0)_{n\in\mathbb{N}}$. Let $\omega_0 \in [\![0, 2^{\mathsf{N}} - 1]\!]$ be the lowest value occurring an infinite number of times in I, and n_0 the index of its first occurrence, such that $x_{n_0} = \tilde{x}$, $(w_{n_0})_0 = \omega_0$.

Similarly, the subsequence I_1 of X constituted by the block messages (x_n, w_n) such that $x_n = \tilde{x}$ and $(w_n)_0 = \omega_0$ is infinite, while all the $(w_n)_1$ belong in $[\![0, 2^{\mathsf{N}} - 1]\!]$. So at least one element of $[\![0, 2^{\mathsf{N}} - 1]\!]$ appears an infinite number of times in the second block messages of the second components $(w_n)_1$ of I_1. Let ω_1 be the lowest value in $[\![0, 2^{\mathsf{N}} - 1]\!]$ occurring an infinite number of times at this position, and n_1 the index in X of its first occurrence.

A subsequence $I_2 = (x_n, w_n)$ of X can be defined again such that $\forall n, x_n = \tilde{x}$, $(w_n)_0 = \omega_0$, and $(w_n)_1 = \omega_1$, and a similar argument leads to the definition of ω_2, the lowest value in $[\![0, 2^{\mathsf{N}} - 1]\!]$ appearing an infinite number of times in the third block messages of the sequences $w_n \in [\![0, 2^{\mathsf{N}} - 1]\!]^{\mathbb{N}}$ of I_3. This process can be continued infinitely.

Finally the point $l = \left(\tilde{x}, (w_{n_k})_k\right)$ of $\mathcal{X}$ is defined; the subsequence (x_{n_k}, w_{n_k}) of X converges to l. As for all sequences in $\mathcal{X}$ a subsequence that converges in $\mathcal{X}$ can be extracted. So, the compactness of $\mathcal{X}$ can be concluded.

B. Topological entropy

Let (X, d) be a compact metric space and $f : X \to X$ be a continuous map. For each natural number n, a new metric d_n is defined on X by

$$d_n(x, y) = \max\{d(f^{\circ i}(x), f^{\circ i}(y)) : 0 \leq i < n\}.$$

Given any $\varepsilon > 0$ and $n \geqslant 1$, two points of X are ε-close with respect to this new metric if their first n iterates are ε-close (according to d).

This metric allows one to distinguish in a neighborhood of an orbit the points that move away from each other during the iteration from the points that travel together. A subset E of X is said to be (n, ε)-separated if each pair of distinct points of E is at least ε apart in the metric d_n.

Definition 8 Let $H(n, \varepsilon)$ be the maximum cardinality of a (n, ε)-separated set, the *topological entropy* of the map f is defined by (see *e.g.*, [11] or [12])

$$h(f) = \lim_{\epsilon\to 0}\left(\limsup_{n\to\infty}\frac{1}{n}\log H(n, \varepsilon)\right).$$

There is the result,

Theorem 1 *Entropy of $(\mathcal{X}, G_g)$ is infinite.*

PROOF Let $\mathrm{x}, \check{\mathrm{x}} \in \mathbb{B}^{\mathsf{N}}$ such that $\exists i_0 \in [\![1, N]\!], \mathrm{x}_{i_0} \neq \check{\mathrm{x}}_{i_0}$. Then, $\forall \mathrm{w}, \check{\mathrm{w}} \in \mathcal{S}_{\mathsf{N}}$,

$$d((\mathrm{x}, \mathrm{w}); (\check{\mathrm{x}}, \check{\mathrm{w}})) \geqslant 1$$

But the cardinal c of $\mathcal{S}_{\mathsf{N}}$ is infinite, then $\forall n \in \mathbb{N}, c > e^{n^2}$.

So for all $n \in \mathbb{N}$, the maximal number $H(n, 1)$ of $(n, 1)-$separated points is greater than or equal to e^{n^2}, and then

$$h_{top}(G_g, 1) = \overline{lim}\frac{1}{n}log\left(H(n, 1)\right) > \overline{lim}\frac{1}{n}log\left(e^{n^2}\right) = \overline{lim}\,(n) = +\infty.$$

But $h_{top}(G_g, \varepsilon)$ is an increasing function when ε is decreasing, then

$$h_{top}\left(G_g\right) = \lim_{\varepsilon\to 0} h_{top}(G_g, \varepsilon) > h_{top}(G_g, 1) = +\infty,$$

which concludes the evaluation of the topological entropy of G_g.

VI. Conclusion and future work

In this article, the topological study of the CBC mode of operation has been deepened by evaluating its property of topological mixing. Additionally, a quantitative evaluation has been performed by measuring the level of its topological entropy.

In future work, we will be interesting to show how this characterization of disorder can improve the encryption mode in terms of diffusion and confusion. We will then more specifically focus on the hardware implementation of such modes, and we will check whether adding some properties of disorder will help to face side channel attacks.

References

[1] R. L. Devaney. *An Introduction to Chaotic Dynamical Systems*. Addison-Wesley, Redwood City, CA, 2nd edition, 1989.

[2] Jacques M Bahi, Raphaël Couturier, Christophe Guyeux, and Pierre-Cyrille Héam. Efficient and cryptographically secure generation of chaotic pseudorandom numbers on gpu. *arXiv preprint arXiv:1112.5239*, 2011.

[3] A. Abidi, Q. Wang, B. Bouallegue, M. Machhout, and C. Guyeux. Proving chaotic behavior of cbc mode of operation. *International Journal of Bifurcation and Chaos*, 26(07):1650113, 2016.

[4] A. Abidi, Q. Wang, B. Bouallegue, M. Machhout, and C. 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, 2016.

[5] J. Banks, J. Brooks, G. Cairns, and P. Stacey. On devaney's definition of chaos. *Amer. Math. Monthly*, 99:332–334, 1992.

[6] Jacques Bahi and Christophe Guyeux. Hash functions using chaotic iterations. *Journal of Algorithms and Computational Technology*, 4(2):167–181, 2010.

[7] 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.

[8] 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.

[9] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, 1995.

[10] *Anonymous2016*.

[11] R. L. Adler, A. G. Konheim, and M. H. McAndrew. Topological entropy. *Trans. Amer. Math. Soc.*, 114:309–319, 1965.

[12] R. Bowen. Entropy for group endomorphisms and homogeneous spaces. *Trans. Amer. Math. Soc.*, 153:401–414, 1971.