 DOI: 10.1515/umcsinfo-2015-0004

On the semantic security of cellular automata based pseudo-random permutations using results from the Luby-Rackoff construction

Kamel Mohammed Faraoun[1]*

[1] *Computer science department, Djilalli Liabbes University*
Sidi Bel Abbés, Algeria

Abstract – This paper proposes a semantically secure construction of pseudo-random permutations using second-order reversible cellular automata. We show that the proposed construction is equivalent to the Luby-Rackoff model if it is built using non-uniform transition rules, and we prove that the construction is strongly secure if an adequate number of iterations is performed. Moreover, a corresponding symmetric block cipher is constructed and analysed experimentally in comparison with popular ciphers. Obtained results approve robustness and efficacy of the construction, while achieved performances overcome those of some existing block ciphers.

Keywords: *semantic security, reversible cellular automata, block ciphers, cryptography*

(*Received: 09.02.2015; Revised: 30.03.2015; Published: 07.05.2015*)

1 Introduction

pseudo-random permutations (PRPs) figure as a central tools in designing secure cryptographic protocols, especially those for secret-key block ciphers. The term pseudo-random permutation, refers in cryptography to a function that cannot be distinguished from a permutation selected randomly with a uniform probability from the family of all permutations defined on the function's domain, whenever using any polynomially computable distinguisher.

Modeling block cipher using PRP's constructions enables a theoretically founded security analysis of such protocols, since well specified and formalized theory has been developed during the last decades for construction, validation and security analysis of PRPs [**1, 2, 3**]. Most known and normalized block ciphers are generally built using such type of functions, especially by the means of the standardized Luby-Rackoff construction proposed initially in [**4**] that permits to build strong and secure PRPs using symmetric iterative structure named Feistel networks [**5**]. Specifically, it has been proved that using four rounds of the Feistel networks construction are sufficient to build a strongly secure PRP that remains pseudo-random even to an adversary who can gets access to its inverse permutation [**4**]. Such kind of provable security is named semantic security, and is considered as extremely strong when it is met. Precisely, if a crypto-system is semantically secure, then an adversary is not able to compute any information about a plain-text from its corresponding cipher-text. This may be posited as an adversary, given two plain-texts of equal length and their two respective cipher texts, cannot determine which cipher-text belongs to which plain-text.

Cellular automata (CAs) have been introduced first by Von Neumann and later by Wolfram [**6**] as simple model for physics, biological and computational systems. The fact that simple CAs underlying rules with elementary transitions steps can be efficiently implemented, and demonstrates complex and random-like behavior, has attracted researchers to use them for cryptographic protocols design. Since the first attempt to build a CA-based stream-cipher by Wolfram [**6**], several cryptographic variants have been explored using different classes and types of CAs. The first attempt to build a block cipher using CAs has been made by Nandi et al. [**7**] where the author implemented a crypto-system based on additive CAs with group properties. In [**8**], Kari proposed in a crypto-system with reversible CA, and Zhang presented in [**9**] a different method of encryption based on RCAs that has a larger key space. Another RCA based encryption algorithm is proposed in [**10**] that satisfies the avalanche criteria, but trades off with additional communication overhead. In [**11**], a crypto-system (CAC) is proposed, where non-linearity is achieved by intermixing affine CA with non-affine transformations. Relatively recent works on block ciphers constructions using CAs can be found in [**12, 13, 14, 15, 16**].

Many of the proposed CAs-based block ciphers have been successfully broken [**17, 18, 19**], and only some of them have been commendably tested and crypt-analysed [**20**]. Unfortunately, no formal theoretic model of such

*kamel_mh@yahoo.fr

constructions has been established, and in the best case, security analyses have been performed using empirical and statistical measurements. In previously proposed works, we have tried to build secure cellular automata based block ciphers using several techniques and approaches: we used genetic algorithm to evolve optimal ciphers with respect to the avalanche criterion in [**21**], and we designed an ad-hoc parallel model of block ciphers for digital images in [**22**] that was enhanced later in [**23**]. In contrast to the present work, no theoretic model has been used to prove security of the mentioned ciphers, and only experimental analysis has been performed to evaluate robustness and secrecy the designed solutions.

In the present work, we show that theoretic result drawn from Feistel networks and Luby-Rackoff constructions can be used to prove semantic security of a specific CAs-based PRP construction model. We establish a conditioned equivalence between Feistel networks and second-order reversible cellular automaton (RCAs), and we show that equivalence's conditions are met only when using non-uniform transition rules. The proposed PRP's RCAs-based construction is firstly shown to be semantically secure under the conditions mentioned above, then a simple block cipher scheme is derived and validated experimentally with respect to the strict avalanche criterion. The remaining of the paper is organized as follows: Section 2 gives preliminaries of pseudo-random permutations and Luby-Rackoff construction. Section 3 introduces the basic CAs elements with the second-order reversibility mechanism. Section 4 exposes the RCAs-based proposed PRP's construction with the corresponding security conditions. Section 5 illustrates an application of the proposed model to build a semantically secure block cipher and gives corresponding experimental security analysis results. Finally, conclusions are drawn in Section 6.

2 Pseudo-random permutations definitions and security conditions

In this section we introduce some basic definitions about PRPs, and their corresponding security conditions and requirements.

Definition 1. A function defined on the set of all binary blocks of length n into the same set $\Phi : \{0,1\}^n \to \{0,1\}^n$ is said to be a permutation if and only if it is a bijection (i.e. Φ^{-1} exist and is efficiently computable). A family of permutations Φ_k is defined by:

$$\begin{aligned} &\Phi_k : \{0,1\}^m \times \{0,1\}^n \\ &(k,x) \to y = \Phi(k,x), \end{aligned} \tag{1}$$

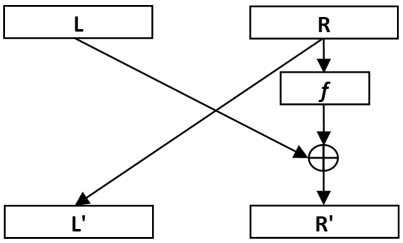

FIGURE 1. Pictorial representation of the Feistel function D_f construction.

is said to be a pseudo-random permutation family if it verify the following properties [**24**]:

(1) For any $k \in \{0,1\}^m, \Phi_k$ is a bijection from $\{0,1\}^n$ to $\{0,1\}^n$,
(2) For any $k \in \{0,1\}^m$, there exist and efficient algorithm to evaluate $\Phi_k(x)$,
(3) For all probabilistic polynomial-time distinguishers $D : |Pr\{D^{\Phi k}(1^n) = 1\} - Pr\{D_n^f(1^n) = 1\}| < \varepsilon(s)$, where $k \in \{0,1\}^n$ is chosen uniformly at random and f_n is chosen uniformly at random from the set of permutations on n-bit strings.

The last property implies that the output of Φ_k cannot be distinguished from a randomly permutation selected from the set of all permutations on functions domain for any value of k. Given the output of a PRP and the output of a truly random function, no polynomial algorithm that can distinguish between the two outputs must exit. Formally, a PRP is considered secure if the advantage of any distinguishing algorithm from a truly random permutation is negligible.

A pseudo-random permutation family can then be considered as a collection of pseudo-random permutations, where a specific one may be chosen using a key. In the following, we use the term PRP to refer to any pseudo-random permutation family Φ_k. The notion of PRP is a rigorous formalization of the notion of block cipher from applied cryptography. As mentioned in section 1, the most known and used way to build secure PRPs is the standardized Luby-Rackoff construction based on Feistel networks. Related definition and security conditions are presented in the following.

Definition 2. For a function $f : \{0,1\}^n \to \{0,1\}^n$, the Feistel function $D_f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is defined like the following:

$$D_f(L,R) = (R, f(R) \oplus L), \tag{2}$$

where L and R are two n-bits blocks from $\{0,1\}^n$.

Figure 1 gives a pictorial representation of a Feistel function construction.

It is clear from the above definition that the function D_f is invertible and hence define a bijection. Formally, the inverse D_f^{-1} is defined by the composition $\phi o D_f o \phi$ when $\phi(L,R) = (R,L)$. However, the function D_f do not define a PRP by itself, since $L' = Left(D(L,R)) = R$ for any L and R. To achieve the requirement of a PRP using the Feistel functions model, we should use a composition of multiple rounds. Using m-rounds Feistel network, the output (L_m, R_m) is defines by the following :

$$\begin{aligned}(L_m, R_m) &= \\ D_f(L_{m-1}, R_{m-1}) &= \\ D_f(D_f(L_{m-2}, R_{m-2})) &= \\ D_f(D_f(\cdots(D_f(L,R))\cdots)\ .&\end{aligned} \tag{3}$$

The function D_f is iterated m times on the input (L,R) to give the desired output. This construction leads to the definition of an invertible function $D_f^{(m)}$ that can be considered as a PRP if the number of rounds is sufficient. The number of rounds necessary to ensure the security of the constructed PRP is given by the following theorem [**4**]:

Theorem 1. (Luby-Rackoff). Three rounds of the Feistel construction, each with a round function drawn independently from a pseudo-random function (PRF) family, yields a weak PRP family. Moreover, four rounds yield a semantically strong PRP family.

We conclude from the above theorem that building semantically strong and secure PRP using Feistel construction need at least the use of four rounds. Another important security condition is that the function f must be a PRF that is defined to be a not necessary invertible PRP. If instead we use a predictable function that can be distinguished from a random one, the resulting construction will be weak and vulnerable to cryptanalysis techniques. In standardized block ciphers, pseudo-random functions are generally built using substitution and permutation boxes (S-box and P-box).

Using Feistel construction, many secure and normalized block ciphers have been developed, such as DES, 3DES, Blowfish, Misty and many others. Semantic security of theses algorithms is proofed and guaranteed by the Luby-Rackoff theorem; even if some simplified versions has been successfully crypt-analysed, due to some weaknesses in the random behavior of their corresponding round functions (PRFs). In the following sections, we propose a novel RCA-based PRP construction scheme, and we show that it is semantically secure by establishing conditioned equivalence between the proposed construction and the Feistel networks one.

3 Second-order reversible cellular automata preliminaries

A cellular automaton consists of a number of cells arranged in a regular lattice, each cell has its own state that change in a discrete time step. States of the whole CA's cells are updated synchronously using a local transition rule that defines each new cell's state using its old state, and the states of the corresponding neighbors. Neighbors are specific selection of cells relatively chosen with respect to a given cell's position, and can be defined for each cell using a radius r on the lattice, giving 2r+1 different neighbor including the cell itself. The boundaries cells of the lattice are concatenated together in a cyclic form to deal with finite size automaton. If the same update rule is used for all the cells then the resulting CA is named uniform. Otherwise, if a different transition rule is used each time the cell's position change, the resulting CA is named non-uniform.

Unlike standard uniform models of uniform CAs that apply the same transition rule in each lattice's position, applying non-uniform transition rules require to change the rule's value from one lattice position to another according to a predetermined conditions (that depends generally on a supplementary feedback of information). Such models relax the normal requirement of all nodes having the same update rule [**25**], and raises an advanced level of chaotic behavior with higher sensitivity to initial configuration's alterations.

Formally, when defining the state of a cell i at the time t by q_i^t, its state at time $t+1$ (defined by q_i^{t+1}) depends only on states of corresponding neighborhood at time t, and is computed by applying a transition rule that defines the way states are updated. If the neighborhood radius is r, and if only two cell states are defined (0 or 1), then the length of each transition rule is equal to 2^{2r+1} bit, and the number of possible rules is equal to $2^{2^{2r+1}}$. The transition rule of one dimensional binary CAs is generally coded using the integer value of the corresponding binary representation, while the different CA's configurations are represented by binary blocks.

Unlike elementary cellular automata, RCAs are specific case of CAs in which every configuration has only one unique predecessor. That is, RCAs are constructed in such a way that the state of each cell prior to an update can be determined uniquely from the updated states of all the cells. Several models are known to construct cellular automata rules that are reversible. The second-order cellular automaton method invented by [**26**], in which the update rule combines states from two previous steps of the automata, permits to turn any one-dimensional binary rule into a reversible one using the fact that the state of a cell at time t depends not only on its neighborhood at time $t-1$, but also on its state at time $t-2$.

This is achieved by combining the i^{th} cell state at time t with the state of the same cell in time $t-2$ using the xor operator.

If we define the configuration of a given CA at each time step t by C^t, then we can build a second-order RCA using the following equation:

$$C^t = F(C^{t-1}) \oplus C^{t-2} \ , \tag{4}$$

where the map F denote the global transition map of the used basic CA. Such defined RCA can then be reversed trivially using the following equation:

$$C^{t-2} = F(C^{t-1}) \oplus C^t \ . \tag{5}$$

The RCAs defined using equations (4) are always reversible even if the basic used CA defined by the map F is not, so we can construct as mush RCAs as possible existing CAs.

Instead of using one initial configuration like standard one-dimensional CA, two initial configurations are required to evolve a second-order RCA. Starting from two configurations C^0 and C^1 we obtain after m time step two configurations C^m and C^{m+1}. By running the RCA backward starting from C^m and C^{m+1} as initial configuration, we recover the two configurations C^0 and C^1 after exactly m iteration using exactly the same transition rule. Reversion is performed using the same transition rule, raising qualitatively the same behaviour of one-order CAs as pointed by Wolfram [**27**]. This makes the use of such defined RCAs very appropriate for crypto-systems building, when security of such RCAs based crypto-systems is assured by the impossibility to reconstruct initial configurations pair from any given pair of consecutive configurations without the knowledge of the transition rule used initially.

4 PRPs construction using reversible cellular automata

In the following, we present the proposed constructions of PRPs using second-order RCA. We establish a conditioned equivalence between the second-order RCA scheme and the Feistel construction, then we show that such equivalence do not hold when using uniform transition rules. In contrast, we show that a non-uniform RCA-based model can raises sufficient conditions under which the construction of semantically secure PRPs becomes feasible.

4.1 Equivalence between RCA and Feistel rounds

Let's consider in the following that a second-order RCA is defined by a transition rule T, a global transition map F_t (exclusively defined by T), and a set of possible configurations C^i for $0 \leq i \leq m$, when assuming that each configuration is an n-bits block form $\{0,1\}^n$. Let's also consider that $(C^i)_j$ denotes the j^{th} bit value of the i^{th} configuration C^i (the j^th cell state). A single iteration of such RCA on two consecutive configurations C^i and C^{i-1} gives the next configurations C^i like follows:

$$C^i = F_t(C^{i-1}) \oplus C^{i-2}, \ i > 1 \ . \tag{6}$$

To obtain a new configuration C^{i+1}, a new iteration should be performed using the two configurations C^i and C^{i-1}:

$$C^{i+1} = F_t(C^i) \oplus C^{i-1}, \ i \geq 1 \ . \tag{7}$$

By combining equations (6) and (7), we define the function G_t permitting to derive two new successive configurations from two initial ones like the following:

$$\begin{aligned} G_t : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \times \{0,1\}^n, \\ G_t(C^{i-2}, C^{i-1}) = (C^i, C^{i+1}) = \\ (F_t(C^{i-1}) \oplus C^{i-2}, F_t(C^i) \oplus C^{i-1}) \ . \end{aligned} \tag{8}$$

Starting from arbitrary two initial configurations C^0 and C^1, a second-order RCA produces any desired number of successive configuration pairs using equation (8). This equation defines entirely two iterations of an RCA using a fixed transition rule T if the RCA is uniform.

By comparing equation (8) with equation (2) from the definition 2.1, we easily conclude that if the global transition map F_t is a pseudo-random function, then the function G_t is equivalent to two successive rounds of the Feistel function D_{FT} applied on two consecutive configurations C^{i-2} and C^{i-1}:

$$\begin{aligned} D_{FT}(D_{FT}(C^{i-2}, C^{i-1})) = \\ D_{FT}(C^{i-1}, F_t(C^{i-1}) \oplus C^{i-2}) = \\ (F_t(C^{i-1}) \oplus C^{i-2}, F_t(F_t(C^{i-1} \oplus C^{i-2}) \oplus C^{i-1}) = \\ G_t(C^{i-2}, C^{i-1}) \ . \end{aligned} \tag{9}$$

Equation (9) is a proof of the following lemma that establishes equivalence between second-order RCAs and Feistel functions:

Lemma 1. Any second-order reversible cellular automata defined by a transition rule T and a global transition map F_t can be constructed using Feistel functions, such that two consecutive RCA's iterations are equivalent to two Feistel rounds, if and only if the global transition map F_t is a pseudo-random function.

AI XX, 1 (2015) 21–31 DOI: 10.1515/umcsinfo-2015-0004

Figure 2 gives a pictorial illustration of the equivalence described by the above lemma. Note that L_1 and R_1 are temporary configurations, used for intermediate computation.

It result from this equivalence that all obtained security results on the Feistel construction can be used to deduce equivalent ones for the RCA's construction. The mains consequence derived by combining results of lemma 1 with the Luby-Rackoff theorem is formulated by the following lemma:

Lemma 2. Four iterations of a second-order RCA-based construction, each with a global transition map F_t yields a semantically strong PRP family, if and only if F_t is a pseudo-random function.

The sufficient and necessary condition of equivalence drawn by the lemma 1 is that the global transition map F_t be a pseudo-random function for any possible transition rule T. We show in the following that this condition does not hold for uniform second-order RCA since the global transition map F_t is not a PRF in this case.

Let's consider a uniform second-order RCA using transition rule T with a radius size r, when T is selected randomly form $\{0,1\}^N$ and $N = 2^{2^{2r+1}}$. According to the uniform second-order RCA scheme [**25**], the global transition map F_t produces a new configuration C^{i+1} using the transition rule T, and determine each bit (C_j^{i+1}) according to its corresponding neighborhood in the configuration C^i. The value of this j^{th} bit is exactly equal to the bit of rule T at position p_j defined by the binary representation of the neighborhood. Since the neighborhood of any selected bit $(C^i)_j$ is given by the binary configuration $(C^i)_{j-r}(C^i)_{j-r+1}\dots(C^i)_{j-1}(C^i)_j(C^i)_{j+1}\dots(C^i)_{j+r-1}(C^i)_{j+r}$ the position p_j is computed by:

$$\begin{aligned} p_j = 2^0.(C^i)_{j-r} + 2^1.(C^i)_{j-r+1} + \dots \\ +2^{r-1}.(C^i)_{j-1} + 2^r.(C^i)_{j+1} + \dots \\ +2^{2r+1}.(C^i)_{j+r-1} + 2^r.(C^i)_{j+r}\ . \end{aligned} \tag{10}$$

It is clear that any given configuration C^i that has all bits equals (all zeros or all ones), gives always the same neighborhood value for any bit's position. So produced configuration $F_t(C^i)$ have all bit's values identical whenever is the used transition rule T. If we denote by 0^n and 1^n the two n-bits configurations that have all bits positions at 0 or 1 respectively, the produced configuration $F_t(C^i)$ can have only two possible values $F_t(C^i) = 0^n$ or $F_t(C^i) = 1^n$ depending on the rule's bit value at the position computed by the two possible neighborhood 0^{2r+1} or 1^{2r+1}. We deduce that the global transition map F_t cannot be considered as a PRF by itself since $F_t(0^n)$ and $F_t(1^n)$ can have only two possible values 0^n or 1^n whenever is the transition rule, which is extremely rare to be the case for a truly random PRF. According to the 2, we conclude that a uniform RCA-based PRP scheme cannot be semantically secure. However, we show in the next section that a construction using non-uniform RCA permits to turn the global transition map F_t into a PRF, making the PRP's RCA-based model totally equivalent to the Feistel one, and as a result semantically secure.

4.2 Semantically secure RCA-based PRP construction

When using non-uniform second-order RCA, the transition rule can change from one configuration's bit position to another. It has been shown in pervious works [**27, 28**] that such class of cellular automata raises more complex and chaotic evolution behavior with respect to standard uniform model, and are consequently more suitable for cryptographic applications. Reversibility of the non- uniform model is always guaranteed by the second-order composition principle and only the global transition map F_R is affected by the introduced non-uniformity.

Let's consider a second-order RCA defined by a set of n different r-radius transition rule $S = \{T_1, T_2, \cdots, T_n\}$ (selected randomly from $\{0,1\}^N$ such that $N = 2^{2^{2r+1}}$), with a global transition map F_S (exclusively defined by the set S), and a set of possible configurations C^i from $\{0,1\}^n$ for $0 \le i \le m$.

Using this model, computation of a new configuration C^{i+1} from two prior ones C^{i-1} and C^i performed similarly using equation (7), while the global transition map F_S operate differently from the uniform model : to compute the j^{th} bit's value $(F_S(Ci))_j$ corresponding to the bit $(C^i)_j$ at the j^{th} position of the configuration C^i, the global transition map F_S apply the position's corresponding transition rule T_j from S on the corresponding neighbourhood extracted from the configuration C^i that is uniquely defined by the binary sequence $(C^i)_{j-r}(C^i)_{j-r+1}\cdots(C^i)_{j-1}(C^i)_j(C^i)_{j+1}\cdots(C^i)_{j+r-1}(C^i)_{j+r}$. The value of $(F_S(C^i))_j$ is exactly equal to the bit extracted from the rule T_j at the neighbourhood's dependent position p_j defined by equation (10). So bits of the new configuration C^{i+1} are computed like the following:

$$\begin{aligned} &\forall\ 0 \le j \le n-1\ : \\ &(C^i)_j = (F_S(C^i))_j \oplus (C^{i-1})_j = (T_j)_{p_j} \oplus (C^{i-1})_j\ . \end{aligned} \tag{11}$$

Let's show in the following that such global transition map F_S is a pseudo-random function. By definition, a function is considered as pseudo-random if its output cannot be distinguishable from a random function. If the global transition map F_S is a PRF, then for any given produced configuration $F_F(C^i)$, each bit value at each

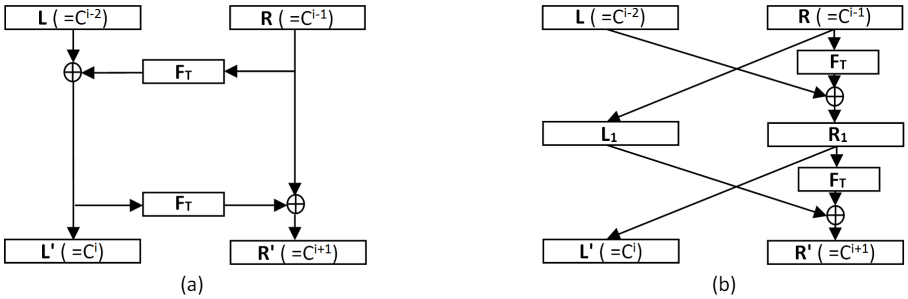

FIGURE 2. Equivalence between RCA's mechanism and Feistel functions :(a) two iterations of RCA; (b) two Feistel rounds.

position can be either 0 or 1 with same probability 1/2 (which is the definition of a randomly chosen binary string according to a uniform distribution). Hence, we must show that $Pr\{(F_S(C^i)_j)\} = 0 = Pr\{(F_S(C^i)_j)\} = 1 = \frac{1}{2} \forall\ 0 \leq j \leq n$, for any configuration C^i. In order to show that such property is verified, we firstly show that for any configuration C^i, each two bits selected at two different positions j and j' are equal with a probability $\frac{1}{2} : Pr\{(F_S(C^i)_j) = (F_S(C^i)_{j'})\} = \frac{1}{2} \forall\ 0 \leq j \leq n, \forall\ 0 \leq j' \leq n$ and $j \neq j'$.

When using a uniform model of second-order RCA, the bit's distribution of $(F_S(C^i))_j$ reflects exactly the distribution of the p_j values computed from the set of corresponding neighborhoods extracted from C^i. So the probability $Pr\{(F_S(C^i)_j) = (F_S(C^i)_{j'})\}$ for two different positions j and j' is equal to the probability $Prp_j = p_{j'}$ since the same unique rule is always used. As a result, if we choose a configuration C^i that has same bit value in all positions, we get the same neighborhood at each position j and we obtain the following:

(12)
$$\forall\ 0 \leq j \leq n,\ 0 \leq j' \leq n \ and\ j \neq j' :$$
$$Pr\{(F_S(C^i)_j) = (F_S(C^i)_{j'})\} = Pr\{p_j = p_{j'}\} = 1\ .$$

Equation (12) is the proof that uniform transition maps are not pseudo-random functions. However, in the case of non-uniform transition rules, and since a different rule is used each time the position change, we deduce the following:

(13)
$$\begin{aligned} &\forall\ 0 \leq j \leq n,\ 0 \leq j' \leq n \ and\ j \neq j' : \\ &Pr\{(F_S(C^i)_j) = (F_S(C^i)_{j'})\} = \\ &Pr\{(p_j = p_{j'})\ and\ ((T_j)_{p_j} = (T_{j'})_{p_{j'}})\} + \\ &Pr\{(p_j <> p_{j'})\ and\ ((T_j)_{p_j} = (T_{j'})_{p_{j'}})\} = \\ &Pr\{(T_j)_{p_j} = (T_{j'})_{p_{j'}}\}\ . \end{aligned}$$

Equation (13) is justified by the fact that $(F_S(C^i))_j$ and $(F_S(C^i))_{j'}$ are equal in two case: either the corresponding neighborhoods from C^i are identical and the two rule T_j and $T_{j'}$ has the same bit value in the position p_j and $p_{j'}$, or the two neighborhoods are different but the two rule T_j and $T_{j'}$ has randomly the same bit value in the two different positions p_j and $p_{j'}$ respectively. We note that even if a configuration C^i has same bit value in all positions (C^i is equal to 0^n or 1^n) and then all neighborhoods are identical ($Pr\{p_j = p_{j'}\} = 1$), the probability that $(F_S(C^i))_j$ and $(F_S(C^i))_{j'}$ be equal is independent form the neighborhoods values and corresponding positions p_j and $p_{j'}$.

Since the rules T_j are selected randomly, the probability that a cell at any position p_j is equal to zero or one is $\frac{1}{2}$: $Pr\{(T_j)_{p_j} = 0\} = Pr\{(T_j)_{p_j} = 1\} = \frac{1}{2}\ \forall\ 0 \leq j \leq n$. So the probability that two different positions p_j and $p_{j'}$ from two different rules T_j and $T_{j'}$ be equal can be computed like the following:

(14)
$$\begin{aligned} &\forall\ 0 \leq j \leq n\ , 0 \leq j' \leq n \ and\ j \neq j' : \\ &Pr\{(T_j)_{p_j} = (T_{j'})_{p_{j'}}\} = Pr\{((T_j)_{p_j} = 0)\ and\ ((T_{j'})_{p_{j'}} = 0)\} + \\ &Pr\{\{((T_j)_{p_j} = 1)\ and\ ((T_{j'})_{p_{j'}} = 1)\}\} = \\ &(Pr\{(T_j)_{p_j} = 0\} \cdot Pr\{(T_{j'})_{p_{j'}} = 0\}) + \\ &(Pr\{(T_j)_{p_j} = 1\} \cdot Pr\{(T_{j'})_{p_{j'}} = 1\})\ , \\ &Pr\{(T_j)_{p_j} = (T_{j'})_{p_{j'}}\} = 1/2 \cdot 1/2 + 1/2 \cdot 1/2 = 1/2\ . \end{aligned}$$

By combining equations (13) and (14), we conclude that for any given produced configuration C^i , two random bits positions are equal with a probability 1/2:

(15)
$$\begin{aligned} &\forall\ i, \forall\ 0 \leq j \leq n\ , 0 \leq j' \leq n \ and\ j \neq j' : \\ &Pr\{(F_S(C^i))_j = 0\} = Pr\{(F_S(C^i))_j = 1\} = 1/2\ . \end{aligned}$$

Let's suppose that $\forall\ 0 \leq j \leq n$, $Pr\{(F_S(C^i))_j = 0\} = \alpha$, and then show that α is equal to 1/2. If we consider the following:

$$
\begin{aligned}
Pr\{F_S(C^i)_j = F_S(C^i)_{j'}\} = \\
Pr\{((F_S(C^i)_j = 0)\ and\ (F_S(C^i)_{j'} = 0))\ or \\
((F_S(C^i)_j = 1)\ and\ (F_S(C^i)_{j'} = 1))\} = \\
Pr\{((F_S(C^i)_j = 0)\ and\ (F_S(C^i)_{j'} = 0))\} + \\
Pr\{((F_S(C^i)_j = 1)\ and \\
(F_S(C^i)_{j'} = 1))\} = \\
Pr\{F_S(C^i)_j = 0\} \cdot Pr\{F_S(C^i)_{j'} = 0\} + \\
Pr\{F_S(C^i)_j = 1\} \cdot Pr\{F_S(C^i)_{j'} = 1\} = \\
\alpha \cdot \alpha + (1-\alpha) \cdot (1-\alpha) = \alpha^2 + (1-\alpha)^2 ,
\end{aligned} \tag{16}
$$

then, by combining equation (17) and equation (16), we conclude that:

$$
\begin{aligned}
\alpha^2 + (1-\alpha)^2 = 1/2 \Rightarrow \\
2\alpha^2 - 2\alpha + 1/2 = 0 \Rightarrow \\
2(\alpha - 1/2)^2 = 0 \Rightarrow \alpha = 1/2 .
\end{aligned} \tag{17}
$$

As a result, equation (16) is always verified. Consequently, the global transition map F_S is a pseudo-random function. According to equation (16), the output of F_S is indistinguishable from a randomly selected bit string, even when the configuration C^i is equal to 0^n or 1^n.

Now since F_S is shown to be a pseudo-random function, and using results from Lemma 1 and Lemma 2, we conclude the following theorem about security of non-uniform RCA-based PRPs construction model:

Theorem 2. A non-uniform second-order RCA defined by a set of randomly selected transition rules $S = \{T_1, T_2, \ldots, T_n\}$ and a global transition map F_S is equivalent to a Feistel construction, such that two iterations of such RCA are equivalent to two Feistel rounds. A construction with four non-uniform RCA's iterations, each with a global transition map F_S, yields a semantically strong PRP family.

The above theorem defines a novel PRPs construction scheme using non-uniform RCA, and establishes the corresponding security conditions. In the following section, we propose the construction of a symmetric block cipher using this construction, which is as a result semantically secure. Several statistical experiments are also performed on the proposed scheme to show its robustness and efficacy with respect to some popular ones.

5 Cryptographic application of the proposed PRP construction

In the following, we use the proposed non-uniform RCA-based PRP's construction to build a symmetric block cipher. The cipher uses a 128-bit secret key K selected randomly from $\{0,1\}^{128}$ to encipher a 128-bit plain-block PB into a ciphered one CB. Even if only four iterations are sufficient to achieve semantic security according to the Theorem 2, we use sixteen successive iterations (equivalent to sixteen Feistel round) to ensure further robustness of the designed block cipher.

5.1 Details of the proposed Block cipher

According to the proposed non-uniform RCA-based PRP's construction, enciphering plain-blocks of size $2n$ require a set S of n randomly selected rules to build the global transition map F_S. Furthermore, the global transition map F_S should change from a ciphering iteration to another in order to ensure strong security of the cipher. To achieve the mentioned requirements, a key scheduling mechanism is used to derive sub-keys for different iterations (rounds) such that each iteration i for $1 \leq i \leq 16$ uses a different sub-key K_i. At each iteration, the rule's set S is constructed from the corresponding secret sub-key K_i using a pseudo-random numbers generation scheme that is not necessarily secure, since security of the proposed block cipher relay only on randomness distribution of the rules neither on the predictability of their sequence.

In the present work, we used transition rules with radius $r = 3$, so each rule is a 128-bit random block from $\{0,1\}^{128}$. During the i^{th} iteration, the secret sub-key K_i is used to produce 64 different transition rule $T_1, T_2, \ldots, T_{64}$ by the mean of a very simple and fast mechanism: each rule T_j is equal to a left-cyclic rotation of K_i by an amount of j position. Such produced rules are randomly distributed in $\{0,1\}^{128}$ so they meet the security requirements of the proposed construction. Note that any other key expansion scheme can be used to perform rules derivation process if it ensures a random distribution, and the only motivation of the used one is speed and simplicity.

The set of sub-keys K_i for $1 \leq i \leq 16$ can be generated using any key scheduling mechanism similar to those used by several block ciphers, and it is sufficient that a non-linear relation exist between the derived sub-keys. In the proposed block cipher, the derived sub-keys are generated with an elementary cellular automaton that use rule 30 having good random-like behavior according to the results obtained by of Wolfram [**15**]. The key K is used as initial configuration, and then resulting consecutive configurations obtained by applying the rule 30 in a cycle boundary conditions mode are used as sub-keys K_i.

Figure 3 illustrate pictorial description of the proposed block cipher with its different components. The deciphering scheme act exactly like the enciphering one, except that the sub-keys are used in reverse order: if the sub-keys $K_1, K_2, \ldots, K_{16}$ are used for iterations $1, 2, \ldots, 16$ of encryption then the sequence $K_{16}, K_{15} \ldots, K_1$ is used for iterations $1, 2, \ldots, 16$ of decryption.

The proposed block cipher is semantically secure according to theoretic results reported above. Moreover, we performed an experimental analysis in terms of speed and security. Different experimental results are presented in what follows.

5.2 Experimental Security analysis and results

A secure block cipher has to ensure certain number of statistical properties related to its robustness against common cryptanalysis techniques such as linear and differential ones. Non-linearity is one of such required properties that as randomness, has not a complete unique definition, but can be measured in a number of ways. We achieve a good approximation of such property by measuring a very specific mathematical property named avalanche effect [**29**]. This property tries, to some extent, to reflect the intuitive idea of high non-linearity: very small difference in the input produces always high changes in the output, hence an avalanche of changes.

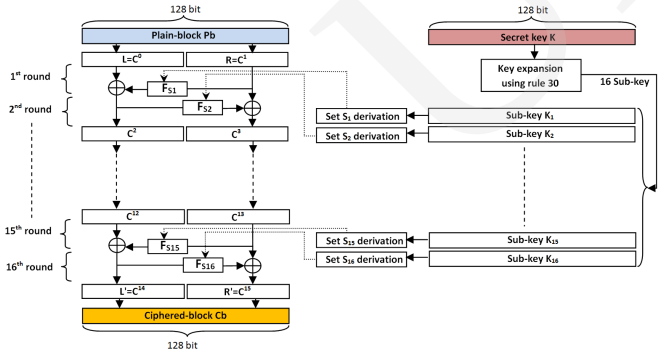

FIGURE 3. Pictorial description of the proposed block cipher.

Mathematically, let's consider the block cipher as a function (that is a pseudo-random permutation) $\Psi_K : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ with m the length of the key and n the length of plain-blocks. The Ψ_K function has the avalanche effect if the following is satisfied:

$$\forall\, K \in \{0,1\}^m,\ \forall\, x, y \in \{0,1\}^n\ : \quad H(x,y) = 1 \Rightarrow Average(H(\Psi_K(x), \Psi_K(y))) = 1/2\ , \tag{18}$$

where H denotes the Hamming distance between two n-bits blocks. According to equation (19), a minimum random input change (one single bit) should produces a maximum output change (half of the bits), on average. This definition reflects also the general concept of independence between input and output. An ideal Ψ_K will define a perfect random function and then have a perfect avalanche effect. Another more accurate and demanding non-linearity measurement is the so called strict avalanche criterion [**29**] which, in particular, implies the avalanche effect, and that is described mathematically by:

$$\forall\, K \in \{0,1\}^m,\ \forall\, x, y \in \{0,1\}^n\ : \quad H(x,y) = 1 \Rightarrow H(\Psi_K(x), \Psi_K(y)) \approx B(1/2, n)\ , \tag{19}$$

where $B(1/2, n)$ denotes a binomial distribution of parameters $1/2$ and n. A block cipher defined by a function Ψ_K satisfies the strict avalanche criterion if the bit-difference between two ciphered blocks corresponding of two plain blocks that differ only on one bit follows a binomial distribution $B(1/2, n)$.

This can be verified by measuring the amount of proximity between theoretic binomial distribution and experimental distribution computed for the block cipher using a sufficiently large samples set. Such measurement can be easily performed using χ^2 goodness-of-fit tests.

In order to compute the experimental distribution of $H(\Psi_K(x), \Psi_K(y))$ corresponding to the proposed block cipher, we use a set of 10^5 randomly generated plain-blocks P_i with a set of 10^5 randomly generated secret key K_i. For each, pair (P_i, K_i), we first encipher P_i using K_i, then we flip each one of 128 bit of the plain-block to obtain P'_i and we encipher again to compute the hamming distance $H(\Psi_K(P_i), \Psi_K(P'_i))$. The set of obtained Hamming distances for all used samples is used to build an array D of 128 value, such that each value $D[i]$ represents the number of obtained hamming distances that are equal to i. By dividing the elements of this array by the total number of experiment's samples equal to $10^5 \cdot 10^5 \cdot 128 = 128 \cdot 10^{10}$, we obtain finally the desired experimental distribution. The chi-square test is performed by computing the χ^2 value:

$$\chi^2 = \Sigma_{i=1}^{128} \frac{(O_i - E_i)^2}{E_i}\ , \tag{20}$$

where O_i is the obtained experimental value of the distance and E_i is the theoretic expected one.

Using the probability $\alpha = 0.01$ as critical threshold, the hypothesis of equivalence between the two distributions is accepted if the χ^2 value is less than the quantile $\chi_{127,0.01} = 166.99$. After several experiments, the computed averaged χ^2 value is equal to 0.0023, that is negligible with respect to the quantile value. Hence the null hypothesis is accepted and the hamming distribution of

the proposed block cipher is following a binomial distribution $B(1/2, 128)$. As a result, the block cipher is satisfying the strict avalanche criterion. Table 1 lists different χ^2 values obtained when experimenting some standard popular 128-bit block ciphers using the procedure described above.

Figure 4 illustrate a plot of the obtained experimental distribution compared to the theoretic curve of the binomial $B(1/2, 128)$, and to those of other experimented block ciphers.

In order to check the sensitivity of the proposed block cipher to small secret key variations, the experiment procedure described above is also performed using a set of randomly selected keys K_i, while distribution of the output's Hamming distances with respect to elementary key-bits flipping is computed. Such distribution is expected to be binomial $B(1/2, 128)$ if the block cipher is highly sensitive to secret key variations. Using the chi-square test, we show that proposed block cipher satisfy the avalanche criterion with respect to elementary key variations. Results of keys sensitivity testing are listed in table 1, when figure 5 illustrates the plot of the corresponding experimental distribution. Results of Table 1 show that the proposed cipher provides good variation's sensitivity to both plain-blocks and secret key. While the strict avalanche criterion is not a sufficient security condition, it is however a necessary one that ensures robustness against differential and linear cryptanalysis methods. We agree the proposed approach have to be submitted to further cryptanalysis techniques, which is the works we are planning for perspectives.

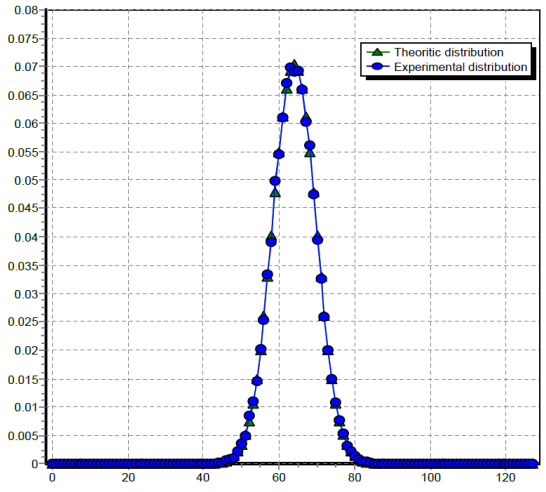

FIGURE 5. Distribution of output's sensitivity to secret key variations versus theoretic binomial distribution $B(1/2, 128)$.

Block Cipher	Operating Mode	Block Size	Key Size	Speed (MB/sec)
AES	CBC	128	128	109
Cast 256	CTR	128	256	37
Mars	CTR	128	128	47
Towfish	CTR	128	128	26
RC6	CTR	128	2048	101
SHA-CAL2	CTR	160	512	53
Camellia	CTR	128	256	37
IDEA	CTR	64	128	35
Proposed	**CBC**	**128**	**128**	**103**

TABLE 2. Ecryption speed performance's resutls with comparison to popular block ciphers [**30**].

5.3 Speed Analysis and comparison

The proposed construction can be implemented easily and efficiently in both hardware and software. Even if the inherent parallelisme of CAs is more suitable for hardware, we have realised a very fast and compact software implementation of the proposed block cipher using pure assembly and MMX instructions sets permitting the use of 128-bit CPU's registers. The simple key mixing and rules derivation schemes described in section 5.1 are favorable for a fast and reduced instruction implementation permitting to achieve high speed encryption/decryption rates. Table 2 summarize obtained performance's results for the proposed block cipher in comparison with some popular ones implemented by the Crypto++ 5.6.0 Banchmarks [**30**].

It is clear that proposed approach provides very hight performances with respect to others due to the parallelized nature of CA's and to the optimality of the designed model with respect to assembly MMX instructions.

6 Conclusions

In this work, we propose a PRP's construction model using reversible second order cellular automata. Using results from Feistel networks construction, we show that proposed construction semantically secure if non-uniform transition rules are used. Based on this construction, a simple and fast semantically secure block cipher is proposed and benchmarked with respect to the strict avalanche criterion. Obtained results show that the block cipher is highly sensitive to small variations of both plain blocks and secret key, since corresponding variations distribution computed using Hamming distance follow a binomial distribution $B(1/2, 128)$. When compared to popular ciphers, performances analysis reveals that proposed one achieve high and competitive encryption/decryption rates with equivalent security requirements. The main contribution of this work is the establishment of possible theoretic framework for study,

		Proposed	AES	Cast 256	Square	Mars	Towfish	RC6
Sensitivity to plain-text variations	χ^2 statistic	0.00231	0.0007	0.00425	0.008	0.00356	0.0102	0.00123
	Average Hamming Distance	0.0017	0.0012	0.0036	0.0021	0.00057	0.00049	0.0008
Sensitivity to the key variations	χ^2 statistic	0.0017	0.0012	0.0036	0.0021	0.00057	0.00049	0.0008
	Average Hamming Distance	64.0138	63.991	63.398	63.98	63.399	63.372	64.108

TABLE 1. Statistical experiments results performed with respect to the strict avalanche criterion.

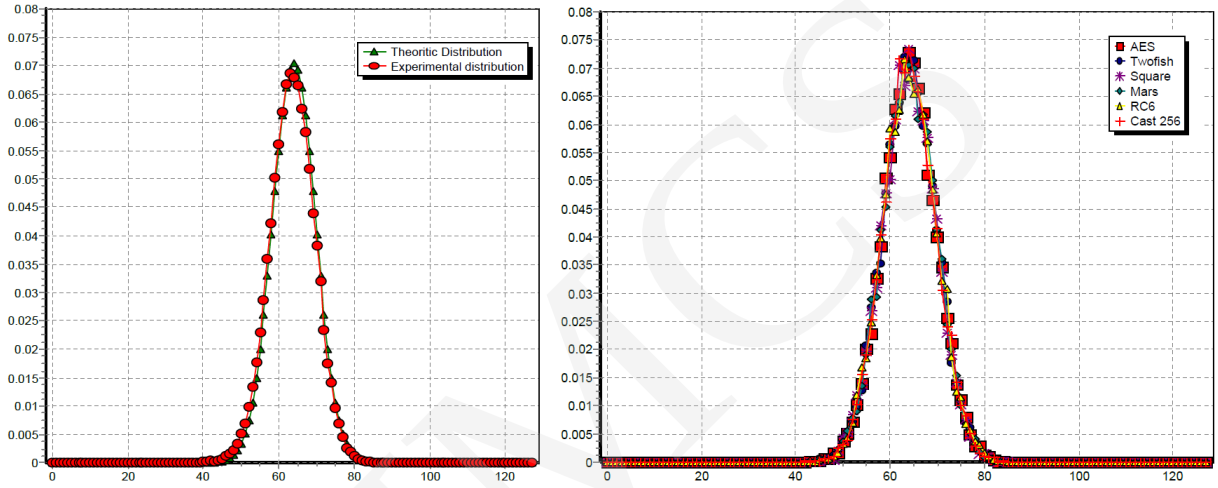

FIGURE 4. Distribution of output's sensitivity to plain-text variations: (a) theoretic distribution versus experimental distribution of the proposed block cipher, (b) experimental distribution of some popular block ciphers.

analysis and evaluation of CA's based block ciphers, until now evaluated using only statistical experiments.

References

[1] Zheng, Yuliang, Matsumoto, Tsutomu, et Imai, Hideki. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In : Advances in Cryptology—CRYPTO'89 Proceedings. Springer New York, 1990. p. 461-480.

[2] Mmaurer, Ueli et Pietrzak, Krzysztof. The security of many-round Luby-Rackoff pseudo-random permutations. In : Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003. p. 544- 561.

[3] Patarin, Jacques. Security of random Feistel schemes with 5 or more rounds. In : Advances in Cryptology– CRYPTO 2004. Springer Berlin Heidelberg, 2004. p. 106-122.

[4] Luby, Michael et Rackoff, Charles. How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing, 1988, vol. 17, no 2, p. 373-386.

[5] Feistel, Horst. Cryptography and computer privacy. Scientific american, 1973, vol. 228, p. 15-23.

[6] Wolfram, Stephen. Cryptography with cellular automata. In : Advances in Cryptology—CRYPTO'85 Proceedings. Springer Berlin Heidelberg, 1986. p. 429-432.

[7] Nandi, S., Kar, B. K., et Pal Chaudhuri, P. Theory and applications of cellular automata in cryptography. Computers, IEEE Transactions on, 1994, vol. 43, no 12, p. 1346-1357.

[8] Kari, Jarkko. Crypto-systems based on reversible cellular automata. Manuscript, August, 1992.

[9] Zhang, Chang N. et Li, Hua. Reconfigurable pipelined cellular automata array for cryptography. In : Communications, Circuits and Systems and West Sino Expositions, IEEE 2002 International Conference on. IEEE, 2002. p. 1213-1217.

[10] Seredyński, Marcin, Pienkosz, Krzysztof, et Bouvry, Pascal. Reversible cellular automata based encryption. In : Network and Parallel Computing. Springer Berlin Heidelberg, 2004. p. 411-418.

[11] Sen, Subhayan, Shaw, Chandrama, Chowdhuri, Dipanwita Roy, et al.Cellular automata based crypto-system (CAC). In : Information and Communications Security. Springer Berlin Heidelberg, 2002. p. 303-314.

[12] Ray, Abhishek et Das, Debasis. Encryption algorithm for block ciphers based on programmable cellular automata. In : Information Processing and Management. Springer Berlin Heidelberg, 2010. p. 269-275.

[13] Tripathy, Somanath et Nandi, Sukumar. LCASE: Lightweight Cellular Automata-based Symmetric-key Encryption. IJ Network Security, 2009, vol. 8, no 3, p. 243-252.

[14] Kumaravel, A. et Meetei, Oinam Nickson. An application of non-uniform cellular automata for efficient cryptography. In :

Information & Communication Technologies (ICT), 2013 IEEE Conference on. IEEE, 2013. p. 1200-1205.

[15] Anghelescu, Petre. Security of telemedical applications over the internet using programmable cellular automata. International Journal of Intelligent Computing Research, IJICR, 2012, vol. 3, no 1/2, p. 245-251.

[16] Abdo, A. A., Lian, Shiguo, Ismail, I. A., et al. A cryptosystem based on elementary cellular automata. Communications in Nonlinear Science and Numerical Simulation, 2013, vol. 18, no 1, p. 136-147.

[17] Sung, Jaechul, Hong, Deukjo, et Hong, Seokhie. Cryptanalysis of an involutional block cipher using cellular automata. Information Processing Letters, 2007, vol. 104, no 5, p. 183-185.

[18] Liu, Jingmei, Cheng, Xiangguo, et Wang, Xinmei. Cryptanalysis of a cellular automata crypto-system. In : Computational Intelligence and Security. Springer Berlin Heidelberg, 2005. p. 49-54.

[19] Li, Chengqing et Lo, Kwok-Tung. Cryptanalysis of an image encryption scheme using cellular automata substitution and scan. In : Advances in Multimedia Information Processing-PCM 2010. Springer Berlin Heidelberg, 2010. p. 601-610.

[20] Szaban, Mirosław et Seredyński, Franciszek. Searching for efficient cellular automata based keys applied in symmetric key cryptography. Annales UMCS Sectio AI Informatica, 2015, vol. 7, p. 49-60.

[21] Faraoun, Kamel Mohamed. A genetic strategy to design cellular automata based block ciphers. Expert Systems with Applications, 2014, vol. 41, no 17, p. 7958-7967.

[22] Mohamed, Faraoun Kamel. A parallel block-based encryption schema for digital images using reversible cellular automata. Engineering Science and Technology, an International Journal, 2014, vol. 17, no 2, p. 85–94.

[23] Faraoun, Kamel Mohamed. Fast encryption of RGB color digital images using a tweakable cellular automaton based schema. Optics & Laser Technology, 2014, vol. 64, p. 145-155.

[24] Katz, Jonathan et Lindell, Yehuda. Introduction to modern cryptography. CRC Press, 2014.

[25] Cattaneo, Gianpiero, Dennunzio, Alberto, Formenti, Enrico, et al. Non-uniform cellular automata. In: Language and Automata Theory and Applications. Springer Berlin Heidelberg, 2009. p. 302-313.

[26] Toffoli, Tommaso et Margolus, Norman H. Invertible cellular automata: A review. Physica D: Nonlinear Phenomena, 1990, vol. 45, no 1, p. 229-253.

[27] Wolfram, Stephen. A new kind of science. Champaign : Wolfram media, pp. 437–440, 2002.

[28] Cattaneo, Gianpiero, Dennunzio, Alberto, Formenti, Enrico, et al. Non-uniform cellular automata. In : Language and Automata Theory and Applications. Springer Berlin Heidelberg, 2009. p. 302-313.

[29] Cattaneo, Gianpiero, Dennunzio, Alberto, Formenti, Enrico, et al. Non-uniform cellular automata. In : Language and Automata Theory and Applications. Springer Berlin Heidelberg, 2009. p. 302-313.

[30] W.Dai, Crypto++ 5.6.0 Benchmarks. http://www.cryptopp.com/benchmarks.html.