Cryptographic properties of Boolean functions defining elementary cellular automata

J. Escuadra Burrieza[a], A. Martín del Rey[b]*, J.L. Pérez Iglesias[a], G. Rodríguez Sánchez[c], A. Queiruga Dios[d] and A. de la Villa Cuenca[e]

In this work, the algebraic properties of the local transition functions of elementary cellular automata (ECA) were analysed. Specifically, a classification of such cellular automata was done according to their algebraic degree, the balancedness, the resiliency, nonlinearity, the propagation criterion and the existence of non-zero linear structures. It is shown that there is not any ECA satisfying all properties at the same time.

1. Introduction

As is well known, Boolean functions play an important role in symmetric cryptography: for example, suitable Boolean functions are considered as combining functions of linear feedback shift registers (LFSRs for short) in stream ciphers, or as basic functions involved in S-boxes in block ciphers. The cryptographic usefulness of Boolean functions is measured by some cryptographic characteristics. The most important of these properties are the following: high algebraic degree, balancedness, high nonlinearity, resiliency, higher order propagation criteria and the non-existence of non-zero linear structures. In order to resist modern cryptanalytic attacks (based on linear approximation and differential characteristics), highly nonlinear Boolean functions with good propagation criteria and less linear structure are basically needed.

The main goal of this paper is to study the cryptographic properties of the local transition functions defining the elementary cellular automata (ECA). Roughly speaking, cellular automata are, in the simplest case, a finite collection of two-stage elementary cells arranged linearly in a lattice and locally interacting in a discrete time step. The state of each cell is synchronously updated according to a Boolean function whose variables are the states of the neighbour cells. Cellular automata have been widely used in symmetric cryptography as pseudo-random bit generators (see, e.g. [6] and the references therein), the design of secret sharing schemes [11], the design of message authentication protocols [14], etc.

A particular and interesting type of cellular automata are ECA for which the local transition function depends only on three variables: the states of the main cell and its two nearest neighbours [25]. As a consequence, it is a three-variable Boolean function and there exist $2^{2^3} = 256$ ECA. As it was mentioned before, there are several papers proposing cryptographic algorithms based on cellular automata. In fact, in some of them, ECA are used. More precisely, we can find a lot of works dealing with the statistical properties of the ECA as generators of pseudorandom bit generators for cryptographic uses (see, e.g. [7,20,21,23,24] and the references therein). Also, some applications to the design of block ciphers have been published [15,18]. However, there are very few works studying the basic cryptographic properties of the local transition functions defining ECA (note that they are three-variable Boolean functions). To our knowledge, there is only one work dealing with this problem: it is due to Martin [10] and he explores all these Boolean functions – using the Walsh transform – in order to find out correlation-immune ones for generating good pseudo-random sequences with use in stream ciphers. In this work, we extend the study of ECA to other cryptographic properties regarding not only stream ciphers but also block ciphers.

The rest of the paper is organized as follows: in section 2, the mathematical background on Boolean functions and ECA is introduced; the main cryptographic properties that a cryptographic function must satisfy are shown in Section 3; in Section 4, we test these properties for the local transition functions of ECA; finally, the conclusions and future work are presented in Section 5.

2. Mathematical preliminaries

2.1 *Boolean functions*

An n-variable Boolean function f is a function from the vectorspace $\mathbb{F}_2^n$, formed for all binary vectors of length n, to the finite field $\mathbb{F}_2 = \{0, 1\}$. The set of all n-variable Boolean functions is denoted by $\mathcal{BF}_n$ and its cardinal is $|\mathcal{BF}_n| = 2^{2^n}$. The Hamming weight of a vector $x = (x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$ is the number of its non-zero coordinates, whereas the Hamming weight of an n-variable Boolean function f is defined as

$$w_{\mathrm{H}}(f) = |\{x \in \mathbb{F}_2^n \text{ such that } f(x) \neq 0\}|,$$

that is, it is the cardinal of its support. Furthermore, the Hamming distance between two Boolean functions $f, g \in \mathcal{BF}_n$ is $d_{\mathrm{H}}(f, g) = w_{\mathrm{H}}(f \oplus g)$, where $(f \oplus g)(x) = f(x) \oplus g(x)$.

The usual representation of a Boolean function f is by means of its algebraic normal form (ANF for short) which is the n-variable polynomial representation over $\mathbb{F}_2$, that is:

$$f(x_1, \dots, x_n) = \bigoplus_{\substack{1\leq k\leq n \\ 1\leq i_1, i_2, \dots, i_k \leq n}} a_{i_1 i_2 \cdots i_k} \cdot x_{i_1} \cdot x_{i_2} \cdot \cdots \cdot x_{i_k},$$

where $a_{i_1 \cdots i_k} \in \mathbb{F}_2$. The degree of the ANF is the algebraic degree of the function. The simplest Boolean functions considering their ANF are the affine functions: $f(x_1, \dots, x_n) =$

$a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n \oplus a_0$, where $a_0, a_1, \ldots, a_n \in \mathbb{F}_2$. If $a_0 = 0$, we have the linear functions and are denoted by $l_a(x)$ with $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$.

The discrete Fourier transform is the linear mapping that maps any pseudo-Boolean function $\phi\colon \mathbb{F}_2^n \to \mathbb{R}$ to the function

$$\begin{aligned} \hat{\phi}\colon \mathbb{F}_2^n &\longrightarrow \mathbb{R} \\ u &\longmapsto \hat{\phi}(u) = \sum_{x\in\mathbb{F}_2^n} (-1)^{x\bullet u}\phi(x), \end{aligned}$$

where $x \bullet u$ stands for the usual inner product. We can apply the discrete Fourier transform to a given n-variable Boolean function f, and the function obtained is denoted by $\hat{f}$. Notice that $\hat{f}(0) = w_{\mathrm{H}}(f)$ and $d_{\mathrm{H}}(f, g) = w_{\mathrm{H}}(f \oplus g) = \widehat{(f+g)}(0)$. The discrete Fourier transform can also be applied to the pseudo-Boolean function $f_\chi(x) = (-1)^{f(x)}$ (called the *sign function*) instead of f itself. Then, it yields:

$$\begin{aligned} \hat{f}\colon \mathbb{F}_2^n &\longrightarrow \mathbb{R} \\ u &\longmapsto \hat{f}(u) = \sum_{x\in\mathbb{F}_2^n} (-1)^{x\bullet u} f(x), \end{aligned}$$

and it is called the Walsh transform of f. The Walsh transform of a Boolean function has some interesting statistical properties [10] that permit to test whether such boolean function is balanced or correlation-immune.

The derivative of the n-variable Boolean function f with respect to $b \in \mathbb{F}_2^n$ is other Boolean function denoted by $D_b f$ and defined as follows:

$$\begin{aligned} D_b f\colon \mathbb{F}_2^n &\longrightarrow \mathbb{F}_2 \\ x &\longmapsto D_b f(x) = f(x) \oplus f(x \oplus b). \end{aligned}$$

The linear kernel of f is denoted by $\mathcal{LK}(f)$ and is defined as the following subspace of $\mathbb{F}_2^n$:

$$\mathcal{LK}(f) = \{b \in \mathbb{F}_2^n \text{ such that } D_b f \text{ is a constant function}\}.$$

Every element $b \in \mathcal{LK}(f)$ is called the linear structure of f.

2.2 *Elementary cellular automata*

ECA are finite state machines formed by m memory units called cells that are arranged linearly. Each cell assume a state from the finite state set $\mathbb{F}_2$ at every step of time. The state of the ith cell at time t is denoted by $s_i^t \in \mathbb{F}_2$ and it changes synchronously in discrete steps of time according to a local transition function f. This function is a three-variable Boolean function whose variables are the previous states of the main cell and its two adjacent cells, that is:

$$\begin{aligned} f\colon \mathbb{F}_2^3 &\longrightarrow \mathbb{F}_2 \\ (s_{i-1}^t, s_i^t, s_{i+1}^t) &\longmapsto s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t) \end{aligned}$$

for every $1 \leq i \leq m$. As a consequence, there exists $2^{2^3} = 256$ ECA, each of which can be indexed by a rule number that is computed as follows [25]:

$$\alpha_0 \cdot 2^0 + \alpha_1 \cdot 2^1 + \alpha_2 \cdot 2^2 + \alpha_3 \cdot 2^3 + \alpha_4 \cdot 2^4 + \alpha_5 \cdot 2^5 + \alpha_6 \cdot 2^6 + \alpha_7 \cdot 2^7,$$

where the truth table of the Boolean function f is:

s_{i-1}^t	s_i^t	s_{i+1}^t	$\longmapsto$	s_i^{t+1}
0	0	0	$\longmapsto$	α_0
0	0	1	$\longmapsto$	α_1
0	1	0	$\longmapsto$	α_2
0	1	1	$\longmapsto$	α_3
1	0	0	$\longmapsto$	α_4
1	0	1	$\longmapsto$	α_5
1	1	0	$\longmapsto$	α_6
1	1	1	$\longmapsto$	α_7

For example, the rule number of the ECA whose local transition function is

$$s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t) = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t,$$

$150 = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 0 \cdot 2^6 + 1 \cdot 2^7$, since its truth table is the following:

s_{i-1}^t	s_i^t	s_{i+1}^t	$\longmapsto$	s_i^{t+1}
0	0	0	$\longmapsto$	$0 \oplus 0 \oplus 0 = 0$
0	0	1	$\longmapsto$	$0 \oplus 0 \oplus 1 = 1$
0	1	0	$\longmapsto$	$0 \oplus 1 \oplus 0 = 1$
0	1	1	$\longmapsto$	$0 \oplus 1 \oplus 1 = 0$
1	0	0	$\longmapsto$	$1 \oplus 0 \oplus 0 = 1$
1	0	1	$\longmapsto$	$1 \oplus 0 \oplus 1 = 0$
1	1	0	$\longmapsto$	$1 \oplus 1 \oplus 0 = 0$
1	1	1	$\longmapsto$	$1 \oplus 1 \oplus 1 = 1$

As the number of cells of an ECA is finite, some boundary conditions must be stated in order to preserve the well-defined evolution. Usually one can take into account three types of boundary conditions: periodic boundary conditions ($s_i^t = s_j^t$ if $i \equiv j \pmod{m}$ for every t), null

Table 1. Rule numbers and ANF of affine ECA.

Rule number	ANF
0	$s_i^{t+1} = 0$
15	$s_i^{t+1} = 1 \oplus s_{i-1}^t$
51	$s_i^{t+1} = 1 \oplus s_i^t$
60	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t$
85	$s_i^{t+1} = 1 \oplus s_{i+1}^t$
90	$s_i^{t+1} = s_{i-1}^t \oplus s_{i+1}^t$
102	$s_i^{t+1} = s_i^t \oplus s_{i+1}^t$
105	$s_i^{t+1} = 1 \oplus s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$
150	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$
153	$s_i^{t+1} = 1 \oplus s_i^t \oplus s_{i+1}^t$
165	$s_i^{t+1} = 1 \oplus s_{i-1}^t \oplus s_{i+1}^t$
170	$s_i^{t+1} = s_{i+1}^t$
195	$s_i^{t+1} = 1 \oplus s_{i-1}^t \oplus s_i^t$
204	$s_i^{t+1} = s_i^t$
240	$s_i^{t+1} = s_{i-1}^t$
255	$s_i^{t+1} = 1$

boundary conditions ($s_i^t = 0$ for every t if $i < 1$ or $i > m$) and intermediate boundary conditions ($s_{1-k}^t = s_{1+k}^t$ and $s_{n+k}^t = s_{n-k}^t$ for every t and $1 \leq k \leq m$).

The ECA whose local transition function is an affine Boolean function is shown in Table 1.

The vector $C^t = (s_1^t, s_2^t, \ldots, s_m^t) \in \mathbb{F}_2^m$ is called configuration of the ECA at time t. The whole evolution of a particular ECA can be comprised in its global transition function:

$$\begin{aligned} \Phi\colon \mathbb{F}_2^m &\longrightarrow \mathbb{F}_2^m \\ C^t &\longmapsto \Phi(C^t) = C^{t+1}. \end{aligned}$$

3. Cryptographic properties

In order to resist the modern cryptanalytic attacks, highly nonlinear Boolean functions with good propagation criteria and less linear structure are needed [1–3,12]. The cryptanalytic attacks on each cryptosystem lead to criteria that the implemented cryptographic Boolean functions must satisfy. More precisely, the resistance of the cryptographic algorithms to the cryptanalytic attacks can be quantified through some fundamental properties (related to confusion and diffusion) on the Boolean functions involved in them. As a consequence, the design of this cryptographic functions needs to consider various characteristics simultaneously.

In this sense, the most important cryptographic criteria for Boolean functions are the following [13,16,19]: algebraic degree, the balancedness, the resiliency, the nonlinearity, the propagation criterion (PC) and the non-existence of non-zero linear structures. Obviously, all of these characteristics cannot be optimum at the same time and consequently trade-offs must be taken into account. In what follows, we describe the mentioned properties.

3.1 *The algebraic degree*

Cryptographic n-variable Boolean functions must have high algebraic degrees since otherwise the cryptographic protocols can be successfully cryptanalysed [8,9,17]. Nevertheless, we have to take into account that the n-variable Boolean functions with algebraic degrees n or $n-1$ do not optimally achieve other cryptographic properties such as nonlinearity or resiliency.

3.2 *Balancedness*

Cryptographic Boolean functions must be balanced, that is, their outputs must be uniformly distributed over $\mathbb{F}_2$. This properties allows one to avoid statistical dependence between the input and the output that can be used in some types of cryptanalytic attacks.

3.3 *Resiliency*

There is an additional condition to balancedness with special importance in the case of the design of stream ciphers: the m-resiliency. An n-variable Boolean function f is said to be m-resilient if it is a balanced function when we keep constant $0 < m \leq n$ variables. If a Boolean function is not m-resilient then there exists a correlation between the output of the function and (at most) m coordinates of its input (correlation attack). Xiao and Massey [26] characterized the resiliency by means of the Walsh transform.

THEOREM 3.1 *An n-variable Boolean function f is m-resilient if and only if it is balanced and $\hat{f}(u) = 0$ for all $u \in \mathbb{F}_2^n$ such that $0 < w_{\mathrm{H}}(u) \leq m$.*

3.4 *The nonlinearity*

Cryptographic Boolean functions must lie at large Hamming distance to all affine Boolean functions. The nonlinearity of an n-variable Boolean function f is defined as

$$\mathcal{NL}(f) = \min_{a \in \mathbb{F}_2^n}\{d_{\mathrm{H}}(f, l_a)\};$$

in this sense, a Boolean function will be considered as highly nonlinear if its nonlinearity is near 2^n. It is shown that $\mathcal{NL}(f) \leq 2^{n-1} - 2^{n/2-1}$, and if the equality holds, f is called Bent function. Note that if n is odd, the last inequality for $\mathcal{NL}(f)$ cannot be an equality and in this case $\mathcal{NL}(f) \leq 2^{n-1} - 2^{(n-1)/2}$.

The Bent functions that are not balanced are not suitable for cryptographic purposes. As a consequence, it is necessary to study the n-variable Boolean functions that have large but not optimal nonlinearities, say between $2^{n-1} - 2^{(n-1)/2}$ and $2^{n-1} - 2^{n/2-1}$, among which some balanced functions exist.

3.5 *The propagation criterion*

In order to assure well-diffusion properties, Boolean functions must satisfy the PC. This criterion was introduced by Preneel *et al.* [16] and it is based on the properties of the derivatives of Boolean functions that gives the behaviour of such functions when some variables of the input are complemented. The n-variable Boolean function f satisfies the PC with respect to $B \subset \mathbb{F}_2^n$ if for every $b \in B$ the derivative function, $D_b f$, is balanced. Moreover, the Boolean function f satisfies PC(k) if it satisfies PC with respect to the set

$$W(k) = \{b \in \mathbb{F}_2^n - \{0\} \text{ such that } w_{\mathrm{H}}(b) \leq k\}.$$

The strict avalanche criterion (SAC) was introduced by Webster and Tavares [22] for the design of the Boolean functions involved in S-boxes. A Boolean function f satisfies SAC if changing any one of the n bits in the input x results in the output of the function being changed for exactly half of the 2^{n-1} vectors x with the changed input bit. In fact, SAC was generalized into the propagation criterion being its particular case for $k = 1$.

3.6 *Non-existence of non-zero linear structure*

Nonlinear n-variable Boolean functions with applications in cryptography (specially in block ciphers) should have no non-zero linear structures [5].

4. Analysis of the cryptographic properties of ECA

In this section we will test the cryptographic properties of local transition functions of ECA, and the results obtained will be analysed.

4.1 *Testing the properties*

4.1.1 *The algebraic degree*

The ECA whose local transition function is of algebraic degree 0 are two: the cellular automata defined by rule numbers 0 and 255. The ECA with algebraic degree 1 are the affine ECA except for 0 and 255. The ECA whose algebraic degree is 2 are:

3, 5, 6, 9, 10, 12, 17, 18, 20, 23, 24, 27, 29, 30, 33, 34, 36, 39, 40, 43, 45, 46, 48, 53, 54, 57, 58, 63, 65, 66, 68, 71, 72, 75, 77, 78, 80, 83, 86, 89, 92, 95, 96, 99, 101, 106, 108, 111, 113, 114, 116, 119, 120, 123, 125, 126, 129, 130, 132, 135, 136, 139, 141, 142, 144, 147, 149, 154, 156, 159, 160, 163, 166, 169, 172, 175, 177, 178, 183, 184, 187, 189, 190, 192, 197, 198, 201, 202, 207, 209, 210, 212, 215, 216, 219, 221, 222, 225, 226, 228, 231, 232, 235, 237, 238, 243, 245, 246, 249, 250, 252.

Finally, the ECA whose local transition function is a three-variable Boolean function of degree 3 are:

1, 2, 4, 7, 8, 11, 13, 14, 16, 19, 21, 22, 25, 26, 28, 31, 32, 35, 37, 38, 41, 42, 44, 47, 49, 50, 52, 55, 56, 59, 61, 62, 64, 67, 69, 70, 73, 74, 76, 79, 81, 82, 84, 87, 88, 91, 93, 94, 97, 98, 100, 103, 104, 107, 109, 110, 112, 115, 117, 118, 121, 122, 124, 127, 128, 131, 133, 134, 137, 138, 140, 143, 145, 146, 148, 151, 152, 155, 157, 158, 161, 162, 164, 167, 168, 171, 173, 174, 176, 179, 181, 182, 185, 186, 188, 191, 193, 194, 196, 199, 200, 203, 205, 206, 208, 211, 213, 214, 217, 218, 220, 223, 224, 227, 229, 230, 233, 234, 236, 239, 241, 242, 244, 247, 248, 251, 253, 254.

4.1.2 *Balancedness*

A three-variable Boolean function is balanced when the number of 1s and 0s of its truth table is the same and equals to 4. A simple computation shows that the ECA whose local transition function is a balanced three-variable Boolean function are those defined by the following rule numbers:

15, 23, 27, 29, 30, 39, 43, 45, 46, 51, 53, 54, 57, 58, 60, 71, 75, 77, 78, 83, 85, 86, 89, 90, 92, 99, 101, 102, 105, 106, 108, 113, 114, 116, 120, 135, 139, 141, 142, 147, 149, 150, 153, 154, 156, 163, 165, 166, 169, 170, 172, 177, 178, 180, 184, 195, 197, 198, 201, 202, 204, 209, 210, 212, 216, 225, 226, 228, 232, 240.

4.1.3 *Resiliency*

Only the local transition functions of some affine ECA are m-resilient. Speficically, the ECA with rule numbers 60, 90, 102, 105, 150, 153, 165, 195 are 1-resilient, whereas the ECA with rule numbers 105 and 150 are 2-resilient. There is not 3-resilient ECA.

4.1.4 *The nonlinearity*

For three-variable Boolean functions, it is $\mathcal{NL}(f) \leq 2^2 - 2^1 = 2$. It is easy to check that the ECA whose nonlinearity is 0 are the affine ECA; the ECA with nonlinearity equals to 1 are

1, 2, 4, 7, 8, 11, 13, 14, 16, 19, 21, 22, 25, 26, 28, 31, 32, 35, 37, 38, 41, 42, 44, 47, 49, 50, 52, 55, 56, 59, 61, 62, 64, 67, 69, 70, 73, 74, 76, 79, 81, 82, 84, 87, 88, 91, 93, 94, 97, 98, 100, 103, 104, 107, 109, 110, 112, 115, 117, 118, 121, 122, 124, 127, 128, 131, 133, 134, 137, 138, 140, 143, 145, 146, 148, 151, 152, 155, 157, 158, 161, 162, 164, 167, 168, 171, 173, 174, 176, 179, 181, 182, 185, 186, 188, 191, 193, 194, 196, 199, 200, 203, 205, 206, 208, 211, 213, 214, 217, 218, 220, 223, 224, 227, 229, 230, 233, 234, 236, 239, 241, 242, 244, 247, 248, 251, 253, 254.

Finally, the ECA with the possible maximum nonlinearity ($\mathcal{NL}(f) = 2$) are those defined by the following rule numbers:

> 3, 5, 6, 9, 10, 12, 17, 18, 20, 23, 24, 27, 29, 30, 33, 34, 36, 39, 40, 43, 45, 46, 48, 53, 54, 57, 58, 63, 65, 66, 68, 71, 72, 75, 77, 78, 80, 83, 86, 89, 92, 95, 96, 99, 101, 106, 108, 111, 113, 114, 116, 119, 120, 123, 125, 126, 129, 130, 132, 135, 136, 139, 141, 142, 144, 147, 149, 154, 156, 159, 160, 163, 166, 169, 172, 175, 177, 178, 180, 183, 184, 187, 189, 190, 192, 197, 198, 201, 202, 207, 209, 210, 212, 215, 216, 219, 221, 222, 225, 226, 228, 231, 232, 235, 237, 238, 243, 245, 246, 249, 250, 252.

4.1.5 *The PC and the extended propagation criterion*

The ECA that satisfies PC(1) (and, consequently, satisfying the SAC) are:

> 6, 9, 18, 20, 23, 24, 27, 29, 33, 36, 39, 40, 43, 46, 53, 58, 65, 66, 71, 72, 77, 78, 83, 92, 96, 111, 113, 114, 116, 123, 125, 126, 129, 130, 132, 139, 141, 142, 144, 159, 163, 172, 177, 178, 183, 184, 189, 190, 197, 202, 209, 212, 215, 216, 219, 222, 226, 228, 231, 232, 235, 237, 246, 249,

whereas the PC(2) is satisfied by the ECA with rule numbers: 23, 24, 36, 43, 66, 77, 113, 126, 129, 142, 178, 189, 212, 219, 231, 232. There is not any ECA satisfying PC(3).

4.1.6 *Non-existence of non-zero linear structure*

The nonlinear ECA without non-zero linear structures are those defined by the following rule numbers:

> 1, 2, 4, 7, 8, 11, 13, 14, 16, 19, 21, 22, 25, 26, 28, 31, 32, 35, 37, 38, 41, 42, 44, 47, 49, 50, 52, 55, 56, 59, 61, 62, 64, 67, 69, 70, 73, 74, 76, 79, 81, 82, 84, 87, 88, 91, 93, 94, 97, 98, 100, 103, 104, 107, 109, 110, 112, 115, 117, 118, 121, 122, 124, 127, 128, 131, 133, 134, 137, 138, 140, 143, 145, 146, 148, 151, 152, 155, 157, 158, 161, 162, 164, 167, 168, 171, 173, 174, 176, 179, 181, 182, 185, 186, 188, 191, 193, 194, 196, 199, 200, 203, 205, 206, 208, 211, 213, 214, 217, 218, 220, 223, 224, 227, 229, 230, 233, 234, 236, 239, 241, 242, 244, 247, 248, 251, 253, 254.

4.2 *Discussion*

Taking into account the results shown in the last subsection, it is easy to check that there do not exist ECA satisfying the following properties at the same time:

- Algebraic degree of the local transition functions of the ECA: between 0 and 3.
- Balancedness.
- Non-existence of non-zero linear structures.
- Nonlinearity of the local transition functions of ECA: between 0 and 2.
- Resiliency: local transition functions 1-resilients and 2-resilients.
- Propagation criterion: PC(1) and PC(2).

Consequently, it is shown that ECA cannot be used directly in the design of S-boxes or as combining functions for LFSRs outputs. Basically, it is due to the number of variables of local transition functions of ECA, which is only 3: note that in this case the Boolean functions with algebraic degrees $n = 3$ and $n - 1 = 2$ do not satisfy optimally the nonlinearity conditions, and the functions of algebraic degree $n - 2 = 1$ are affine ECA! Nevertheless, it is also true that ECA can be used in the design of other cryptographic protocols as is mentioned in section 1, since other mathematical properties, such as statistical properties or reversibility properties, are required for its use in such protocols. Note that this properties often depends not on the local transition function but on the global transition function of the ECA (it is well known that the reversibility of ECA depends on its number of cells m, [4]).

5. Conclusions and further work

In this work, the cryptographic properties of Boolean functions that rules the evolution of the 256 ECA were studied. Specifically, the following characteristics of local transition functions were tested: algebraic degree, balancedness, resiliency, nonlinearity, propagation criterion, and non-existence of non-zero linear structures.

The main conclusion obtained from the results is that ECA cannot be used directly in the design of S-boxes (in block ciphers) or in the design of combining functions of the outputs of LFSRs (in stream ciphers).

Further work is aimed at studying these properties with cellular automata whose neighbourhood's cardinal is greater than 3.

Acknowledgements

We wish to thank the referees for their valuable comments. This work has been supported by Ministerio de Ciencia e Innovación (Spain) under grant MTM2008-02773.

References

[1] C.M. Adams, *On immunity against Biham and Shamir's 'differential cryptanalysis'*, Inform. Proc. Lett. 41 (1992), pp. 77–80.

[2] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptol. 4(1) (1991), pp. 3–72.

[3] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, Berlin, 1993.

[4] P.P. Chaudhuri, D.R. Chowdhury, S. Nandi, and S. Chattopadhyay, *Additive Cellular Automata. Theory and Applications. Volume 1*, IEEE Computer Society Press, Los Alamitos, CA, 1997.

[5] J.H. Evertse, *Linear structures in block ciphers*, in *Advances in Cryptology*, Proceedings of Eurocrypt'87, Lecture Notes in Computer Science, vol. 304, D. Chaum and W.L. Price, eds., Springer, Berlin/Heidelberg, 1988, pp. 249–266.

[6] A. Fúster and P. Caballero, *On the use of cellular automata in symmetric cryptography*, Acta Appl. Math. 93(2) (2006), pp. 215–236.

[7] A. Fúster and D. de la Guía, *Cellular automata applications to the linearization of stream cipher generators*, Proceedings of ACRI 2004, Lecture Notes in Computer Science, vol. 3305, Springer, Berlin/Heidelberg, 2004, pp. 612–621.

[8] L.R. Knudsen, *Truncated and higher order differentials*, *Proceedings of 2nd FSE*, Lecture Notes in Computer Science, vol. 1008, Springer, Berlin/Heidelberg, 1995, pp. 196–211.

[9] X. Lai, *Higher order derivatives and differential cryptanalysis*, in *Communications and Cryptology*, R.E. Blahut, D.J. Costello, Jr., U. Maurer, and T. Mittelholzer, eds., Kluwer Academic Publishers, Berlin, 1994, pp. 227–233.

[10] B. Martin, *A Walsh exploration of elementary CA rules*, J. Cellular Automata 3(2) (2008), pp. 145–156.

[11] A. Martín del Rey and G. Rodríguez Sánchez, *Sharing secrets using elementary cellular automata*, Int. J. Mod. Phys. C 18 (2007), pp. 1707–1716.

[12] M. Matsui, *On correlation between the order of S-boxes and the strength of DES*, in *Advances in Cryptology*, Proceedings of Asiacrypt'94, Lecture Notes in Computer Science, vol. 950, J. Pieprzyk and R. Safavi-Nauti, eds., Springer, Berlin/Heidelberg, 1995, pp. 366–375.

[13] W. Meier and O. Staffelbach, *Nonlinearity criteria for cryptographic functions*, in *Advances in Cryptology*, Proceedings of Eurocrypt'89, Lecture Notes in Computer Science, vol. 434, J.-J. Quisquater and J. Vandewalle, eds., Springer, Berlin/Heidelberg, 1990, pp. 549–562.

[14] M. Mukherjee, N. Ganguly, and P.P. Chaudhuri, *Cellular automata based authentication*, in Proceedings of ACRI 2002, Lecture Notes in Computer Science, vol. 2493, 2002, pp. 259–269.

[15] S. Nandi, B.K. Kar, and P. Pal Chaudhuri, *Theory and applications of cellular automata in cryptography*, IEEE Trans. Comput. 43(12) (1994), pp. 1346–1357.

[16] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandevalle, *Propagation characteristic of boolean functions*, in *Advances in Cryptology*, Proceedings of Eurocrypt'90, Lecture Notes in Computer Science 473 (1991), pp. 161–173.

[17] R.A. Rueppel and O.J. Staffelbach, *Products of linear recurring sequences with maximum complexity*, IEEE Trans. Inform. Theory 33(1) (1987), pp. 124–131.

[18] M. Seredynski and P. Bouvry, *Block encryption using reversible cellular automata*, Proceedings of ACRI 2004, Lecture Notes in Computer Science, vol. 3305, 2004, pp. 785–792.

[19] T. Siegenthaler, *Correlation-immunity of nonlinear combining functions for cryptographic applications*, IEEE Trans. Inform. Theory 30(5) (1984), pp. 776–780.

[20] S. K. Tan and S.-U. Guan, *Evolving cellular automata to generate nonlinear sequences with desirable properties*, Appl. Soft Comput. 7(3) (2007), pp. 1131–1134.

[21] M. Tomassini and M. Perrenoud, *Cryptography with cellular automata*, Appl. Software Comput. 1 (2001), pp. 151–160.

[22] A.F. Webster and S.E. Tavares, *On the design of S-boxes*, in *Advances in Cryptology*, Proceedings of Crypto'85, Lecture Notes in Computer Science, vol. 219, H.C. Williams, ed., Springer, Berlin/Heidelberg, 1985, pp. 523–534.

[23] S. Wolfram, *Random sequence generation by cellular automata*, Adv. Appl. Math. 7 (1986), pp. 123–169.

[24] S. Wolfram, *Cryptography with cellular automata*, in *Advances in Cryptology*, Proceedings of Crypto'85, Lecture Notes in Computer Science, vol. 218, H.C. Williams, ed., Springer, Berlin/Heidelberg, 1986, pp. 429–432.

[25] S. Wolfram, *A New Kind of Science*, Wolfram Media Inc, Champaign, IL, 2002.

[26] G.Z. Xiao and J.L. Massey, *A spectral characterization of correlation-immune combining functions*, IEEE Trans. Inform. Theory 34(3) (1988), pp. 569–571.