The Research of Reversible Cellular Automata with a Finite Lattice

Alexey Chilikov, Alexey Zhukov, Alexey Verkhovsky
Information Security department
Bauman Moscow State Technical University, Moscow Institute of Physics and Technology
Moscow, Russia
chilikov@passware.com, aez_iu8@rambler.ru, alexey.verkhovsky@mail.ru

Abstract. The work contains a research about a reversibility property of cellular automata. Using computational methods, local connection functions, that provide a property of reversibility to cellular one-dimensional and two-dimensional automata of different dimensions, were explicitly obtained. Reversibility criteria were obtained for simple cases, as well as properties for which reversibility is preserved. Authors provided several directions for theoretical analysis, such as polynomial and group model and gain several results, which could be relatively easy extended and generalized. The property of cyclicity represent interest for developing a theory, similar to theory of LFSR. Reversible cellular automata with non-linear local function contains properties of cyclicity and non-linearity, which could be interesting for cryptographic applications.

Keywords — cellular automata, reversible transformations, nonlinear transformations, cryptographic primitive, algebraic models

I. Introduction

For the first time cellular automata were mentioned by John von Neumann in the 40s of the twentieth century. In 1985 Steven Wolfram described the first stream encryption algorithm on cellular automata [1]. A classical cellular automaton is an ordered set of memory cells forming some regular n-dimensional lattice. Many theoretical studies, especially concerning the theory of dynamical systems, mostly consider infinite lattice. In practice, the most widespread cellular automata of small dimension-with one-, two- and three-dimensional lattices, usually infinite. In cryptography, as shown in the review [2] – [5], one-dimensional and two-dimensional finite-lattice automata, or models based on generalized cellular automata, have so far found their application. On the basis of a two-dimensional cellular automaton, a high-performance stream cipher was obtained [6]. Based on the second model, a hash function was recently obtained [7]. A reversible cellular automaton – such that each of its states has only one antecedent. In a recent review [8] it is shown that the main results of studies of reversible cellular automata affect only automata with infinite lattice.

For cryptographic applications, it makes no sense to consider such automata. Authors have found examples of reversible cellular automata with finite lattice, as well as proposed areas of theoretical research and obtained some results.

II. Formal statement of problem

An autonomous finite automaton (1) is called a cellular automaton $C(\Omega, X_1, X_2, \ldots, X_d, \Psi_r, f)$ over a set Ω with d-dimensional lattices, which has size $X_1 \times X_2 \times \ldots \times X_d$, with a radius of locality r, a neighborhood Ψ_r local coupling function f that specifies the transition rule.

$$\mathrm{AC}(S, s_0, F), \qquad (1)$$

where S is the set of possible States of the automaton, $s_0 \in S$ is the initial state of the automaton, F is the transition function. Denote by $m_{(x_1,x_2,\ldots,x_d)}$ the lattice cell of the cellular automaton with coordinates $(x_1, x_2, \ldots, x_d)$. Denote by $m_{(x_1,x_2,\ldots,x_d),t}$ this value if we need to specify its value at the time t. Each internal state s of the automaton corresponds to the filling of its lattice. It is described by an ordered set whose components are the values of memory cells, as shown in the formula (2)

This work was supported by Russian Scientific Foundation Grant N 17-11-01377.

$$s = [\ldots, m_{(x_1, x_2, \ldots, x_d)}, \ldots], 1 \leq x_i \leq X_i, 1 \leq i \leq d \qquad (2)$$

Consider a one-dimensional cellular automaton with coefficients from $\mathbb{Z}_2$.

Cellular automaton is called a one-dimensional Boolean cellular automaton C (3) with a lattice of size X, locality radius r, neighborhood Ψ_r and the local communication function f

$$C(\mathbb{Z}_2, X, \Psi_r, f) \qquad (3)$$

described by an autonomous finite state machine AC (4):

$$AC(S, s0, F), \qquad (4)$$

Here $S = Z_2^X$ is a set of internal states, $s_0 \in S$ is an initial state, $F : S \rightarrow S$ is a transition function.

The internal state is described by the set $s = [m_0, m_1, \ldots, m_{X-1}]$. The action of f is to apply a local communication function to the neighborhood of each cell of the cellular automaton, as shown in (5)

$$m_{x,t+1} = f, 0 \leq x < X \qquad (5)$$

Let the lattice is finite. In this case we should understand how f acts near boundaries of lattice. We consider 2 cases. In the first cells near boundary are neighbors to each other, i.e. in the one-dimensional case, the neighbor of the rightmost cell is the leftmost cell (shown at figure 1).

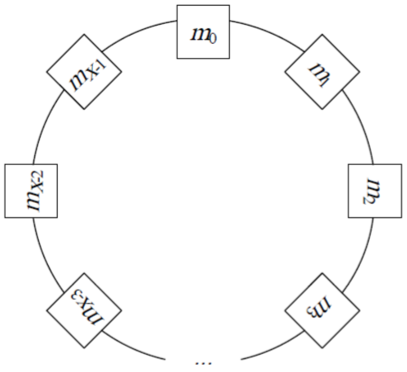

Figure 1. Identification of cells, located near with a lattice boundary, of a one-dimensional cellular automaton

In the second case we assume that beyond the boundaries of the finite lattice there are cells filled with zeros, and they do not change when the cellular automata works. We call such situations a nonzero and zero boundary, respectively. A cellular automaton is called reversible if each of its states s has the only one preceding state s' such that $F(s') = s$. Obviously this condition is equivalent to the periodicity of the cellular automaton: for each s there is t such that $F^{(t)}(s) = s$. For cryptography, there are two interesting questions: how to calculate the period efficiently and how to construct automata with maximal possible period (or almost maximal). Let a lattice be finite and a set of cell states is $\mathbb{Z}_2$. It's easy to see that the reversibility is guaranteed if a local communication function of automaton is a shift. In the two-dimensional case, the cell takes the value of its neighbor, or its inversion. That is, a function of the form (6):

$$f(x_1, \ldots, x_n) = x_i \oplus \alpha \,. \qquad (6)$$

In order to identify nontrivial local communication functions, we wrote a program in C++. This program reveals functions that provide reversibility to a cellular automaton with a given number of cells by the method of brute force. The source code and the results can be found in the repository [9].

III. AUTOMATA, OBTAINED BY BRUTE FORCE

In the course of the program, a large number of functions were obtained that provide reversibility to automata of dimension 1 and the number of cells from 7 to 23 in the case of a function of three variables, and up to 19 for equilibrium functions of 5 variables. Among them were a large number of the aforementioned shift functions as well as linear functions. Linear functions are a fairly simple case, they provide reversibility to the automaton if and only if the matrix of the corresponding linear operator acting on the vector representing the current state of the automaton is not degenerate. In addition to linear functions as well as shift functions, 542 functions with a nonlinear local communication function were obtained. Among them, the following facts are noticed: the inversion of each function providing reversibility also provides reversibility.

IV. THEORETICAL ANALYSIS

The non-obvious results prompted a detailed theoretical analysis of the reversible cellular automaton as a model. The following will list the properties that hold for cellular automata.

Property 1. *If f is a local communication function that provides reversibility for given Boolean cellular automata then $f \oplus 1$ also provides reversibility.*

Proof: We will use rule of contraries. For simplicity, consider the one-dimensional case ($d = 1$). Let be some state of the cellular automaton $s_1 = [m_0, m_1, \ldots, m_{X-1}]$. And let the transition function translate the automaton into a state

$s_2 = [n_0, n_1, \dots, n_{X-1}], m_i, n_i \in \mathbb{Z}_2$ Then $f \oplus 1$ will translate s_1 to $\overline{s_2} = [\overline{n_0}, \overline{n_1}, \dots, \overline{n_{X-1}}]$ - state with inverted coordinates. Suppose that after applying the inverted function, the state $\overline{s_2}$ has another predecessor s^*. But then in the original automaton, s^*. will be translated by f into s_2 (its own inversion), and it has only one predecessor, and that is s_1. That is, s_1 coincides with s^*. Similarly, it is proved for large dimensions.

The following 2 properties are essentially an adaptation of the classical results from [9] to the case of a finite lattice.

Property 2. *A map over a vector space is a cellular automaton if and only if it commutes with a cyclic shift operator.*

Proof: For one-dimensional cellular automata with a nonzero boundary, there is a fact, which is also true for automata with an infinite lattice, namely, commutativity with a shift operation. That is, if $F: \mathbb{Z}_2{}^n \to \mathbb{Z}_2{}^n$ is the function of the cellular automaton, and $Sh(z), z \in \mathbb{Z}_2{}^n$ is the function of the cyclic shift vector z, then $F(Sh(z)) = Sh(F(z))$. This statement is quite obvious, because when applying the cyclic shift, the content of the neighborhood of each cell will not change, and therefore its value will not change when applying the transformation of the cellular automaton. The converse is also true, if a map over a vector space commutes with a shift operator, then this map is a cellular automaton with a nonzero boundary. To do this, we show that shift invariance means the homogeneity of the transformation. Let f_i be a boolean function showing the change of the i-th coordinate of an n-bit vector when the function F acts on it, depending on the value of neighboring coordinates. Since we work with binary vectors, we can get it explicitly by applying F to each set of neighboring coordinates (and itself). Having received a column of values, we write the function f through Zhegalkin polynom:

$$f_k = \oplus_{v=(v_0,v_1,\dots,v_{n-1})} \alpha_v x_0^{v_0} * x_1^{v_1} * \dots * x_k^{v_k} * \dots * x_{n-1}^{v_n-1} \quad (7)$$

Since the value after the shift does not change for any such coordinates, and the values of all neighboring cells do not change, then the function does not change during the shift. For example, if you shift by l, the coordinate value is $k + l$ (8):

$$f_{l+k} = \oplus_{v=(v_0,v_1,\dots,v_{n-1})} \alpha_v x_l^{v_0} * x_{l+1}^{v_1} * \dots * x_{l+k}^{v_k} * \dots * x_{l-1}^{v_n-1} \quad (8)$$

Thus, for any coordinate we have the same function depending on the neighboring coordinates of the vector, which means that this map is a cellular automaton. It is worth noting that the function may not be local – it may well depend on all the values of all cells of the lattice. The influence of the parameters of the local communication function on the distribution of values was studied in [10].

Property 3. *For a reversible binary one-dimensional cellular automaton with a nonzero boundary, there is an inverse cellular automaton.*

We write the commutativity condition with shift in terms of functions:

$$F \circ Sh = Sh \circ F \quad (9)$$

Applying right and left F^{-1}, we get:

$$F^{-1} \circ F \circ Sh \circ F^{-1} = F^{-1} \circ Sh \circ F \circ F^{-1} =$$

$$= F^{-1} \circ Sh = Sh \circ F^{-1} \quad (10)$$

That is, the inverse map also commutes with shifts, and therefore is a cellular automaton.

Theorem 1. *A substitutional polynomial written using a normal basis will have coefficients from the field F_2.*

By normal bases we mean such that each element z of the field F_{2^n} is represented as below:

$$z = z_1 * \theta + z_2 * \theta^2 + \dots + z_n * \theta^{2^{n-1}}$$

The shift condition in this case is written as

$$Sh(z) = z^2. \quad (11)$$

An reversible cellular automaton is a substitution, so we write for it a substitution polynomial in the normal basis:

$$F = \sum_i \alpha_i * z^i \quad (12)$$

Then the condition of commutativity with shift will be written as:

$$F(z^2) = \left(F(z)\right)^2 \tag{13}$$

Combining with (14), we obtain:

$$\sum_i \alpha_i * z^{2i} = \left(\sum_i \alpha_i * z^i\right)^2 = \sum_i \alpha_i^2 * z^{2i}, \tag{14}$$

So $\alpha_i = {\alpha_i}^2$ and $\alpha_i \in F_2$.

This approach allows us to work with cellular automata as mappings over the extension field, which are also representable as polynomials. More about the properties of such a construction is written in [10].

Definition 1. Let’s determine a graph by the following rule. Let be a finite group G, and each vertex of the graph is bijectively mapped to some element of the group. Let also be fixed some subset $\hat{G} = \{g_1, \dots, g_n\}$ (not necessarily a subgroup), and the following property holds: the edge number i leading to the vertex h comes from the vertex hg_i. on the graph thus described, one can specify a cellular automaton (both homogeneous and inhomogeneous). We will call such an automaton a group automaton, and a group G a carrier automaton. The connection function will take the form $f_g(x_1, \dots, x_n)$, and the equation describing the operation of the automaton will have the form:

$$m_g(t) = f_g\left(m_{gg_1}(t-1), \dots, m_{gg_n}(t-1)\right) \tag{15}$$

A quasi-group automaton can be defined similarly by replacing the word "group" with "quasi-group". Recall that in a quasigroup, the associativity property is not necessarily, unlike a group. This definition can be very useful for studying the periodicity properties of the cellular automaton. In addition, the considered classical automata can be considered as automata whose carrier is a cyclic group, which naturally leads to the idea of generalizing the developed theory by transferring it to a wider class of groups (for example, finite Abelian).

V. Conclusion

Reversible cellular automata are a fairly simple described transformation. They can provide the properties of nonlinearity and dispersion (the value of the cell on the next cycle affects the entire neighborhood). These properties are very useful for construction of symmetric cryptosystems. In addition, [13] and [14] show ways to construct asymmetric cryptosystems based on reversible cellular automata. The theoretical basis of cellular automata with finite lattice is not yet fully developed. Authors have taken steps in this direction. Obtained results may well serve as the beginning of the construction of a theory similar to the theory of linear feedback shift registers (LFSR).

References

[1] Wolfram S. Cryptography with cellular automata // Lecture Notes in Computer Science. 1986. Vol. 218. P. 429–432.

[2] Klyucharev P. Methods of designing cryptographic hash-functions based on iteration of the uniform cellular automat. Voprosy kiberbezopasnosti [Cybersecurity issues], 2017. No 1 (19), pp. 45-50. DOI: 10.21681/2311-3456-2017-1-45-50.

[3] Zhukov A.E. Kletochnye avtomaty v kriptografii. Chast’ 1, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 3 (21). P. 70-76. DOI: 10.21581/2311-3456-2017-2-70-76.

[4] Zhukov A.E. Kletochnye avtomaty v kriptografii. Chast’ 1, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017, No 4 (22) – 2017 P. 47-66. DOI: 10.21681/2311-3456-2017-4-47-66

[5] Zotov Ya. Usage of cellular automaton in symmetric-key algorithm. Voprosy kiberbezopasnosti [Cybersecurity issues], 2015. No 3 (11) , pp. 43-45.

[6] Suhinin B.M. Vysokoskorostnye generatory psevdosluchajnyh posledovatel’nostej na osnove kletochnyh avtomatov, Prikladnaya diskretnaya matematika. – 2010. – No2. – S. 34–41.

[7] Klyucharev P.G. Metod postroeniya kriptograficheskikh khesh-funktsiy na osnove iteratsiy obobshchennogo kletochnogo avtomata, Voprosy kiberbezopasnosti [Cybersecurity issues]. 2017. N 1 (19). P. 45-50.

[8] Kari, J.: Reversible Cellular Automata: From Fundamental Classical Results to Recent Developments.: New Generation Computing 36, 145–172 (2018)

[9] Bitbucket: repository https://bitbucket.org/KleshIvanovich/bruterca/src/master/

[10] Suhinin B.M. O vliyanii parametrov lokal’noj funkcii svyazi na raspredelenie znachenij yacheek dvoichnyh kletochnyh avtomatov, Obedinennyj nauchnyj zhurnal. – 2010. – No. 8. – S. 39–41.

[11] Hedlund, G.A.: Endomorphisms and automorphisms of the shift dynamical systems. Math. Syst. Theory 3(4), 320–375 (1969)

[12] *Lidl* R., Niederreiter H. (1997), Finite Fields (2nd ed.), Cambridge University Press, ISBN 0-521-39231-4

[13] Puhua Guan.: Cellular Automaton Public-Key Cryptosystem. Complex Systems 1 51- 57 (1987)

[14] Xing Zhang, Rongxing Lu, Hong Zhang, and Chungen Xu: A New Public Key Encryption Scheme based on Layered Cellular Automata. KSII Transactions on internet and information systems. Vol. 8, No. 10 (2014)