Research of the Influence of the local Transition Function on the Formation of a New Active Cell in the PRNG Based on ACA

STEPAN BILAN
Department Telecommunication technologies and automatics
State Economy and Technology University of Transport
Lukashevicha str., 19, Kiev, 03049, Ukraine.
UKRAINE
bstepan@ukr.net
MYKOLA BILAN
The municipal educational institution Mayakskaya Secondary School,
Mayak, Moldova of
REPUBLIC OF MOLDOVA
nickni@mail.ru
SERGII BILAN
Win-Interactive LLC
Vinnytsia, Ukraine.
UKRAINE
belan@svitonline.com

Abstract: - In this paper, three pseudorandom number generators are considered which are built on asynchronous cellular automata with several active cells that form additional active cells in the field of the cellular automaton. The paper describes pseudo-random number generators based on an asynchronous cellular automaton with one, two and three active cells. Such generators use cellular automata in which each active cell performs two local functions. One local function calculates the state of the cell in the next time step, and the second local function determines the active cell at the next time step. The results of testing all the generators using graphical tests are presented. The tests allow detection of generator defects for different local transition functions. The paper also considers the method of formation of new active cells by two initial active cells. New active cells are formed as a result of the combining of the initial two active cells in one cell of cellular automata. In this case, each additionally formed active cell performs another local transition function that differs from the local transition functions of the previous active cells. The use of additional active cells allows to improve the quality of work of generators based on two-dimensional asynchronous cellular automata. The high quality of the pseudo-random number generator is proved by the used graphic tests.

Key-Words: - Asynchronous cellular automata, pseudorandom number generator, tests, cell, neighborhood of cells, local transition function, active cell.

1 Introduction

At present time, there are many scientific works devoted to the application of pseudo-random number generators (PRNG) based on cellular automata (CA) [1–18]. Synchronous (SCA) and asynchronous cellular automata (ASC) of different dimension are used [2, 5, 11, 12, 17, 18]. Today, there are many solutions for implementation of the PRNG based on one-dimensional CA [3–9, 13]. These PRNGs are well studied and widely used for solving various tasks in the field of information technology. Two-dimensional CAs are also used [2, 14, 15, 17]. However, they require additional research in terms of improving the basic characteristics of PRNG.

Today the PRNGs has been developed based on CA of various configurations [1–18]. They use SCA and ACA, as well as hybrid CA (HCA). In doing so, various local functions of states and transitions are investigated that realize CA cells. They have good characteristics under certain initial states. However, PRNGs based on ACA do not always produce a high-quality pseudo-random bit sequence. They are realized on the basis of ACA with one active cell and practically do not use several active cells. The reason for this is that in each time step only one cell changes its state.

To assess such PRNG the tests were used. However, they do not always show good results. Therefore, the authors propose to use of several active cells in the area of one ACA using various local transition functions. The basic principles of functioning and results of studies of such PRNGs were presented in the report at the conference CSCC2017 (Stepan Bilan, Mykola Bilan, and Sergii Bilan. Research of the method of pseudo-random number generation based on asynchronous cellular automata with several active cells, Crete, Greece, 2017). The graphical tests were used.

In this paper, the authors suggest variants for the formation of new active cells for improving the quality of the PRNG functioning on the basis of ACA with two active cells.

2 PRNG Based on the ACA with One Active Cell

The main element of such PRNG is ACA, in which only one cell implements the local transition function (LTF) at each time step. The cell that performs the LTF at the corresponding time is active at this present time step. The remaining cells of the ACA do not change their state because they are not active. The active cell computes the ACA cell, which will be active at the next time step. The next active cell belongs to the neighborhood of the active cell at the current time (Figure 1). The next active cell can be an ACA cell that does not belong to the neighborhood of the active cell at the current time step. The mode of selecting the active cell at the next time step is set by the original LTF.

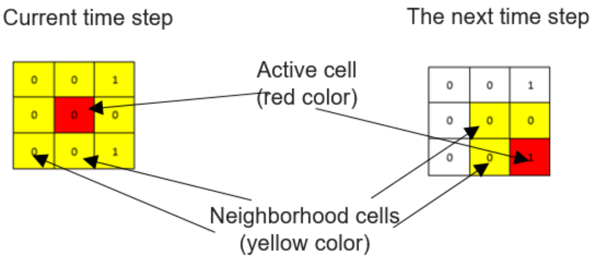

Figure 1. Example of active state transmission from cell to cell at each time step.

An active cell performs two local functions. The first local function calculates the cell of its own neighborhood, which will become active in the next time step. The second local function is the LTF. As a rule, the first local function realizes the XOR function over the signals of the neighborhood cells and the own state signal. Also, additional signals from selected ACA cells can be used at each time step. Additional signals that are LTF arguments improves PRNG properties.

The next active cell is selected according to the local transition function. If the LTF is set unsuccessfully, the PRNG generates a pseudo-random bit sequence of poor quality. The quality of the bit sequence is checked using special tests. Tests often possible to determine the defect PRNG. The used tests can determine an unsuccessful LTF for PRNG based on ACA with one active cell. Especially, the graphical test of the distribution of quantities in the bit sequence shown such results. In this case, most of the tests for PRNG with a large dimension of ACA are successful.

The hardware implementation of PRNG with one active cell is based on the implementation of one cell of the ACA. The cell of the ACA consists of two parts that realize the local function of states and the local function of the active signal transmission of one of the cells in the neighborhood of the active cell. In addition, the PRNG uses a switching circuit in its structure that implements the connection of the output of the active cell to the output of the generator at each instant of time.

The use of ACA with two active cells allows to increase the quality of the PRNG work.

3 PRNG Based on the ACA with Two Active Cells

In an ACA with one active cell, the state of only one active cell at each current time is can changed. The remaining cells do not change their state for a long time, and some cells cannot change their state during the entire time of the PRNG functioning. This situation does not always give a pseudo-random bit sequence of high quality.

To improve the work of PRNG the authors suggest to using the ACA with several active cells. Each active cell performs a separate local transition function, and at the output of the active cells, bit sequences is formed. Thus, at each current time step, two ACA cells can simultaneously change their state. However, the quality of the bit sequence being formed is strongly depend on the LTF that used for each active cell. This was shown by graphic tests that indicate the quality of all used local transition functions. An example of the PRNG functioning based on ACA with two active cells on Figure 2 is shown.

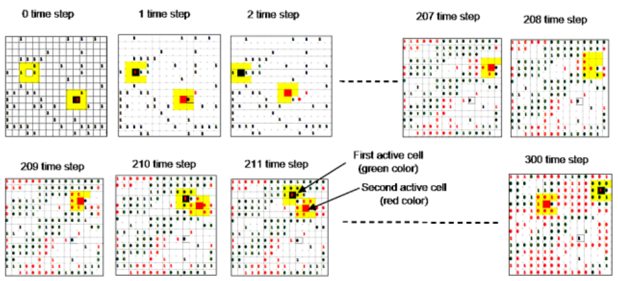

Figure 2. An example of the work of PRNG based on the ACA with two active cells.

In the example shown in Figure 2, several ACA states are represented in the 300 time steps. We see the presence of superpositions on 207 and 209 time steps. At these time steps, only one cell changes its state. However, in the presence of a superposition, two LTFs are performed and compatible active cells pass to other cells of the neighborhood at the next time step. The initial settings of the ACA are shown at 0 the time step. With other initial settings of the ACA, during the operation of the generator there may be no overlap.

The structure of PRNG based on ACA with two active cells is similar to a generator with one active cell. Only ACA is organized somewhat differently. The cell of such an ACA has a different structure since it can work in three modes.

- Standby mode,
- The mode of the first active cell,
- Mode of the second active cell.

The standby mode is characterized by the fact that the cell is set to the information state of the logical "1" or "0". In this state, the cell is located until it becomes active. In the active state, the cell can change its information state, or it may not change its own state. This depends on the local function and on the values of the arguments for the local function of the active cell.

In the second mode, the cell is active, and it functions as well as the active cell, as described in the previous section.

If the cell is in the active state of the second active cell, then it performs the same functions as the first active cell. The only difference is that at an odd time step it performs a local function similar to that performed by the first active cell at the paired time step and vice versa. This separation of active cells in even and odd time steps is carried out in order that in the case of coincidences of the two active cells, one cell does not "disappear".

The following model describes the information state of the active cell of the ACA.

$$b_i(t+1)=\begin{cases} f\left[b_{N_j}^{i}(t)\right], & if\ \ \exists b_{N_j}^{i,act1}(t)=1\ \ or\ \ \exists b_{N_j}^{i,act2}(t)=1 \\ b_i(t), & in\ \ other\ \ case \end{cases} \quad (1)$$

where $b_{N_j}^{i}(t)$ - signals on the information outputs of the cells that constitute the cell neighborhood of i-th cell at time t;

$b_{N_j}^{i,actl}(t)$ - signal at the j-th activation input of i-th cell in i-th activity mode and this signal comes from activation output of the cell that belongs to the cell neighborhood of i-th cell at time t $\left(j=\overline{1,N}\right)$;

N – the amount of neighbor cells, that makes the neighborhood of the i-th cell.

In accordance with this model, active cells change their state regardless of the mode of functioning of the active cell.

Two local transition functions were used. For the first active cell, the LTF was chosen, which been helps to determ the cell of the neighborhood of the active cell with the largest number that was determined at an odd step among the cells of the neighborhood having a logical "1" state at the current time step. At an even step, the cell with the largest number among the neighborhood cells was determined, which have a logical "0" state at the current time step. In addition, the von Neumann neighborhood and the Moore neighborhood were investigated.

For the second active cell, the same LTF was chosen as for the first active cell. However, cells with logical "1" states were analyzed at an even step, and at an odd step all cells of the neighborhood of the zero-state were analyzed, and the cell with the largest numbering among the neighborhood cells was determined.

The LTFs of the first and second active cells are realized identically, but they analyze cells with opposite binary states.

PRNG based on ACA with two active cells forms three bit sequences Q1, Q2, $Q_3 = Q_1 \oplus Q_2$. Each bit at the output of active cells is formed using the XOR function over the signals of the neighborhood cells, the eigenstate and the state of the additional cell at the current time step. An additional bit can be generated using the method presented in the works [16, 17].

The results of testing all three sequences generated by PRNG using graphical tests are shown on Figure 3 and Figure 4.

To perform the test the long sequences that have 2000000 bit in each sequence were formed. Graphical tests show bursts of amplitudes for bit sequences of each active cell. However, the third bit sequence Q3 shows good test results. At the same time, only two LTFs described earlier were realized and other local transition functions were not analyzed.

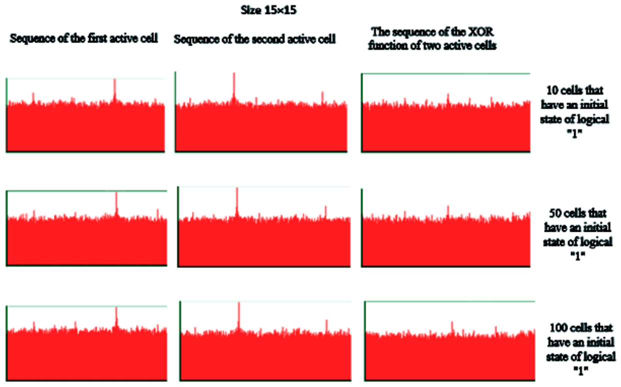

Figure 3. The results of testing of all three of bit sequences with help a graphical test of the distribution of bit sequence elements on the plane.

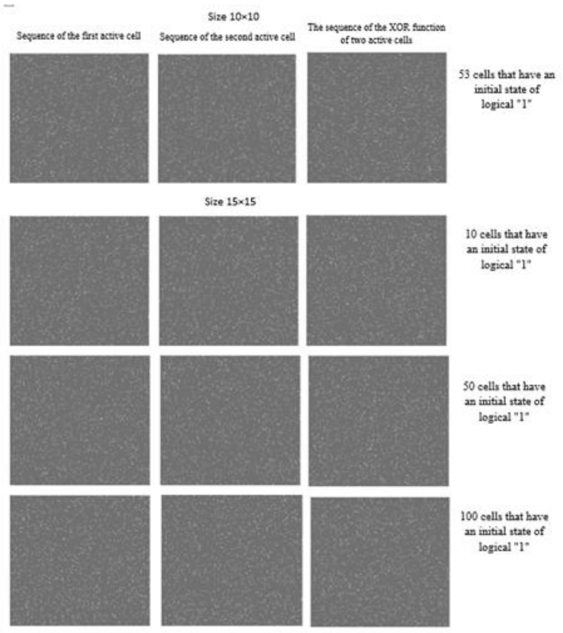

Figure 4. Diagrams of the distribution of points in the plane for bit sequences formed using the Moore neighborhood for a sequence of length of 2,000,000 bits.

ACA in various sizes were used. For large ACA dimensions, the tests showed good results. Good results were also obtained for small sizes, which was not observed for ACA with one active cell.

4 PRNG Based on ACA with a Variable Number of Active Cells

For normal operation of ACA with two active cells, both active cells must perform the same local state function. That is, these cells changed their state according to one local function of states. In addition to this, at the current time step only two active cells change their state.

If at some time step two active cells are combined in one ACA cell, then only one cell changes its state. When both active cells are combined, they can form a new active cell. This new active cell in the next time step is a cell that is located in the place of combining the two active cells.

Thus, in the next time step after combining, three active cells appear. At the next time step, the two original active cells pass to other cells, as well as the third active cell passes into another active cell according to the established LTF. At the next time steps, all three active cells came from cell to cell. If none of the active cells are combined, then at the current time step its state changes three cells of the ACA. In this case, the cell can not change its state if the result of the execution of the local state function corresponds to the value in the previous step. An example of the functioning of the initial two active cells and a new active cell are shown on Figure 5.

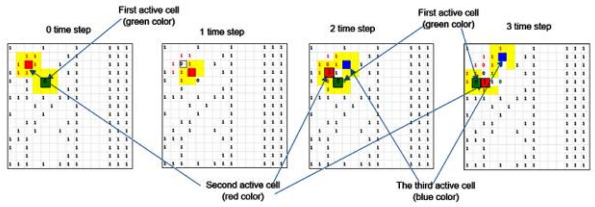
First active cell (green color)
0 time step
1 time step
2 time step
First active cell (green color)
3 time step
Second active cell (red color)
The third active cell (blue color)

Figure 5. An example of the functioning of ACA at the time of the formation of a new active cell in ACA a well as at the following time steps.

The work consider the mode of operation of ACA, when new active cells are formed only by the initial two active cells. There may be other modes for the formation of new active cells in the ACA. For example, new active cells can also form new active cells in future. In addition, new active cells can form under the condition that two active cells are combined with certain LTFs. Thus, after a certain number of time steps, all cells can change their state.

Variants are also possible when the cells go into an inactive state if they are combined on the ACA field. This mode is carried out by selecting the necessary conditions for the functioning of active cells.

In the presented example, a new formed cell performs another LTF. According to the new LTF at the next time step, the active cell is determined by the code of the first three cells of the neighborhood of the third active cell at the current time step. Numbering for active cells of the Moor neighborhood is shown on Figure 6.

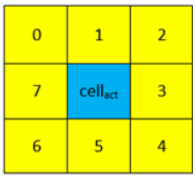

Figure 6. An example of the numbering of cells of the Moore neighborhood, which was used in the software implementation of the method for the first, second and third active cells.

The Moore neighborhood is considered. The numbering of the neighborhood cells is carried out from the left cell of the top row clockwise. If the first three cells (the 0th, 1st and 2nd neighborhood cells) of the neighborhood of the active cell represent binary code 110 (decimal 6), then at the next time step the cell of the neighborhood, which is designated by the number 6, becomes the active cell, that is presented on Figure 7 (3 time step).

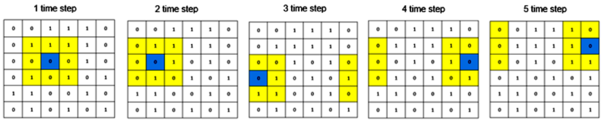

Figure 7. An example of LTF performing by a third active cell.

In this paper, an example is considered where the first and second active cells perform LTF, which are described in the previous section. These cells have a neighborhood where all neighborhood cells are numbered according to Figure 6. For such LTF the cells can only be combined in the case shown in Figure 8.

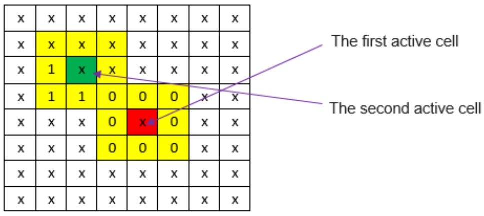

Figure 8. The combination of cells of the neighborhoods of two active cells, which may lead to their coincidence.

At the next time step, the cells are combined (Figure 9). At this time step, a new cell is formed, and at the next time step, the first and second active cells move to other positions according to the established LTFs. The new active cell is blue and moves according to the previously described LTF. She also begins to move to next active cell on the next time step. For other LTFs, the number of variants preceding the overlap may be greater. For example, for a new cell, the described LTF allows to increase the number of possible combinations for combining.

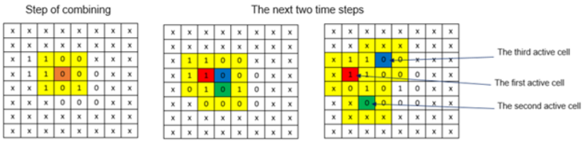

Figure 9. Example of the formation of a new active cell and their transition according to the given LTF.

The "x" characters indicate that the state can be any for these cells (0 or 1). In some cells, the states were chosen arbitrarily at the next time steps. This was necessary to select the following active cells that belong to the neighborhood of active cells on the current time step. Order of transitions are made active cells is shown.

The use of different LTFs for each active cell does not allow the cells to be absorbed when they combine their location. However, it is possible that all ACA cells become active.

Each cell of the ACA can operate in eight modes.

1. The background mode.
2. The mode of the first active cell.
3. The mode of the second active cell.
4. The mode of the third active cell.
5. The mode of the first and second active cells.
6. The mode of the first and third active cells.
7. The mode of the second and third active cells.
8. The mode of the first, second and third active cells.

In the first mode, the ACA cell is not active and does not perform local transition functions and the local state function. In this mode, the cell does not change its state.

If the cell passes into the second, third, or fourth modes, it performs a local state function and a corresponding LTF for the first, second, or third active cell.

In the fifth mode, the cell performs a local state function and two LTFs that are set for the first two active cells. Also in this mode, the cell forms the third active cell (if the fifth mode came the first time), and also the third LTF. In fact, the fifth mode goes into the eighth mode of cell operation and three LTFs are performed. After the formation of the third cell, the transition from the fifth mode to the eighth mode is not carried out. In the fifth mode, two neighborhood cells (the first and second active cells) are determined which will become active at the next time step.

In the sixth mode, the cell performs a local state function, as well as the first and third local transition function. In the seventh mode, the cell performs a local state function, as well as the second and third LTFs.

In the eighth mode, the cell performs a local state function, as well as the first, second, and third LTFs.

The paper considers an option with only three active cells. The influence of three LTFs on the quality of the work of PRNG was investigated. The third LTF used the arguments of the first two cells of the neighborhood of the active cell for the von Neumann neighborhood, and for the Moore neighborhood the signals of the first three neighborhood cells.

The operation of the ACA cell in the described modes requires a complex hardware implementation of each cell. Each cell contains four control outputs. These outputs control the switching system that connects the output of the active cell to one of the outputs of the switching system. If the cell is the first active cell, its information output is connected to the first output of the switching system. The outputs of the second and third active cells are connected to the second and third outputs of the switching system.

PRNG quality analysis is carried out using graphical tests. The results were evaluated for all formed bit sequences by all active cells and sequences generated by XOR function over the bits of active cell sequences. Figure 10 shows the results of the tests of number distribution on the plane for all sequences that are generated simultaneously for one initial state of PRNG.

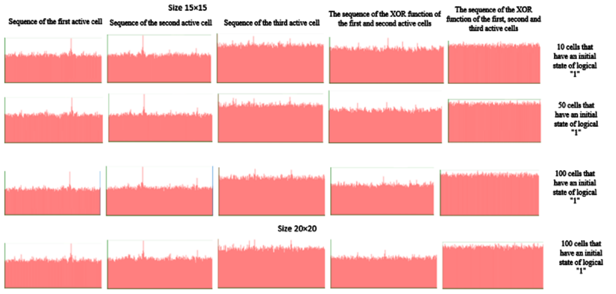

Figure 10. The results of using the graphical test of distribution of elements of bit sequences on the plane.

Four formed bit sequences were analyzed for each initial state of the generator. The first three bit sequences were formed by the first, second and third active cells. A fourth bit sequence is obtained by performing an XOR function for all bits of the first and second bit sequences that are generated by the first and second active cells. A fifth bit sequence is obtained by performing a XOR function for all bits of the first and second bit sequences that are formed by the first, second, and third active cells. In this case, the third bit sequence always contains a smaller number of bits than in the first two sequences since it starts to form later after the first combining of the first two active cells. The greatest length of the third bit sequence can be obtained if the initial state of the first two active cells is used according to Figure 8. The results are presented for ACA sizes of 15 × 15 and 20 × 20 cells, as well as for a different number of cells that at the initial moment have a logical "1" state.

The resulting histograms show that the LTF of third cell gives a better sequence, and the fourth and fifth resulting bit sequences have a good distribution.

The quality of the obtained bit sequences is also confirmed by a graphical test of the distribution of numbers on the plane as shown in Figure 11. Results for the same bit sequences are presented (Figure 10).

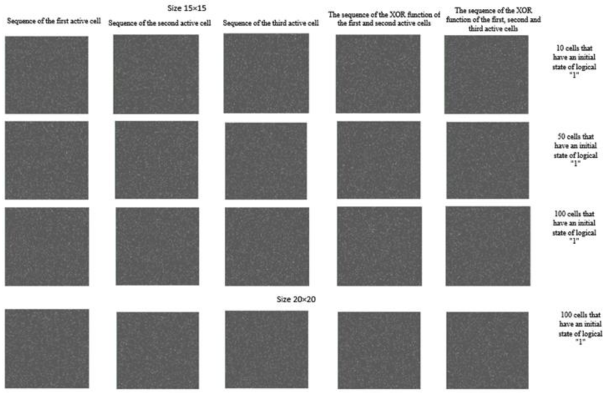

Figure 11. Diagrams of the distribution of points in the plane for bit sequences formed using the Moore neighborhood for a sequence of length of 2,000,000 bits.

This graphical test showed good results for all bit sequences.

5 Conclusion

The use of two active cells in the organization of ACA makes it possible to improve the properties of the generated pseudorandom bit sequences. The analysis of ACA with active cells that performed various LTFs was carried out. It is shown that a large influence on the quality of the bit sequence is provided by the using LTF. Graphical tests showed that the LTF of the third active cell produces a pseudo-random bit sequence of higher quality. In addition, graphic tests showed that the most effective is the neighborhood of Moore. It gives a positive result for small size of ACA when using graphical tests. The use of XOR functions for bit sequences formed by two and three active cells gives better results, which is proved in graphical tests. Also the length of the repeat period of the pseudo-random bit sequence is increased.

References:

[1] Bruce Schneier. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*, Wiley Computer Publishing, John Wiley & Sons, Inc,. 784, 1996.

[2] S. Bilan, M. Bilan, S. Bilan, Novel pseudorandom sequence of numbers generator based cellular automata. *Information Technology and Security*, Vol. 3(1), 2015, pp. 38-50.

[3] Wolfram S., Cellular automata. *Los Alamos Science,* Vol. 9, 1983, pp. 2-21.

[4] Wolfram S., Cryptography with cellular automata. *Lecture Notes in Computer Science,* Vol. 218, 1986, pp. 429-432.

[5] Wolfram S., Random Sequence Generation by Cellular Automata, *Advances in Applied Mathematics*, vol. 7, 1986, pp. 429 – 432.

[6] C. Fraile Ruboi, L., Hernandez Encinas, S. Hoya White, A. Martin del Rey, Rodrigues Sancher., The use of Linear Hybrid Cellular Automata as Pseudorandom bit Generators in Cryptography. *Neural Parallel & Scientific Comp. 12(2),* 2004, pp. 175-192.

[7] Bruno Martin, Patrick Sole, Pseudo-random Sequences Generated by Cellular Automata, *International Conference on Ralations, Orders and Graphs: Interaction with Computer Scince*, May 2008, Mandia, Tunisia, Nouha editions, 2008, pp. 401-410.

[8] K. Cattell, J. C. Muzio, Synthesis of one-dimensional linear hybrid cellular automata, *IEEE Trans. On Computer-aided design of integrated circuits and systems,* 15(3), 1996, pp. 325-335.

[9] K. Bhattachrjee, D. Paul, S. Das. Pseudorandom Pattern Generation Using 3-State Cellular Automata. In: EI Yacoubi S., Was J., Bandini S. (eds). *Cellular Automatar. ACRI 2016. Lect. Not. in Comp. Scien. 9863,* 2016, pp. 3-13.

[10] G. Sh. Sirakoulis. Parallel Application of Hybrid DNA Cellular Automata for Pseudorandom Number Generation. *JCA*. Vol. 11(1), 2016, pp. 63-89.

[11] B. Martin, P. Sole, Pseudo-random Sequences Generated by Cellular Automata". International Conference on Ralations, Orders and Graphs: *Interaction with Computer Scince, May 2008, Mandia, Tunisia, Nouha editions*, 2008, pp. 401-410.

[12] S. Bilan, M. Bilan, R. Motornyuk, A. Bilan, S. Bilan, Research and Analysis of the Pseudorandom Number Generators Implemented on Cellular Automata, *WSEAS TRANS. on SYS.*, Vol. 15, 2016, pp. 275 - 281.

[13] S.J. Cho, U. S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, S.H. Heo., New syntheesis of one-dimensional 90/150 liner hybrid group CA, *IEEE Transactions on comput-aided design of integrated circuits and systems*, 25(9), 2007, pp. 1720-1724.

[14] Suhinin B.M., High generators of pseudorandom sequences based on cellular automata, *Applied discrete mathematics*, № 2, 2010, pp. 34 – 41.

[15] Suhinin B.M., Development of generators of pseudorandom binary sequences based on cellular automata, *Science and education*, № 9, 2010, pp. 1 – 21.

[16] David H. K. Hoe, Jonathan M. Comer, Juan C. Cerda, Chris D. Martinez, Mukul V. Shirvaikar, Cellular Automata-Based Parallel Random Number Generators Using FPGAs. *International Journal of Reconfigurable Computing,* Vol. 2012, 2012, pp. 1-13, Article ID 219028

[17] S. Bilan, M. Bilan, R. Motornyuk, A. Bilan, S. Bilan, Designing of the Pseudorandom Number Generators on the Basis of Two-Dimensional Cellular Automata, *Applied Physics, System Science and Computers. Proceedings of the 1st International Conference on Applied Physics, System Science and Computers (APSAC2016), September 28–30, Dubrovnik, Croatia. Lecture Notes in Electrical Engineering*. Vol. 428. Springer International Publishing AG 2018, pp. 137-143.

[18] S. Bilan, O. Levchuk. Research of pseudorandom number generator based on asynchronous cellular automaton. *Collection of scientific works of SETUT Series "Transport systems and technologies",* Vol. 30, 2017. pp. 184-190.

[19] Marsaglia G., Random number generators. *Journal of Modern Applied Statistical Methods,* Vol. 2, 2003, pp. 2-13.

[20] Chugunkov E.V., *Methods and tools to evaluate the quality of pseudo-random sequence generators, focused on solving problems of information security*, Textbook. M.: NEYAU MIFI, 236, 2012.