Investigation of Properties of Pseudorandom Binary Sequences Generator on the Basis of Cellular Automata

Sergey OSTAPOV, Vladimir ZHIKHAREVICH, Lidiya VAL'
Chernivtsi Yuri Fed'kovich National University
2, Kotsyubinski St.,Chernivtsi,58012, Ukraine
sergey.ostapov@gmail.com

***Abstract*—The comparative analysis of descriptions of pseudorandom binary sequences which are generated using the Blum-Blum-Schub (BBS) algorithm and the one-dimensional cellular automata algorithm (CA) is carried out in this work. It is indicated that CA algorithm demonstrates better results in comparison with BBS. The analysis of CA application is performed in the stream encryption systems. The possibility of the attack based on the known plaintext and any stream part of two nearby generator channels based on CA is shown. The new class CA, which is based on pseudorandom mechanism of localization determination of interactive cells is offered for such type of attacks resistance enhancement.**

***Index Terms*—binary sequences, cellular automata, codes, cryptography, pseudorandom number generator**

I. INTRODUCTION

It is known that stream ciphers cryptoresistance is practically fully determined by the quality of key sequence generator which is laid on the information stream, randomizing it [1-2]. The important part here is not only the possibility of key sequence reproducing on a receiving site but also statistical properties of this sequence, the main of which is probably a large proximity of the generated sequence to the random one. The criterion of such proximity is, as it is generally known, the impossibility of determination with the probability, considerably greater than 0.5, what a next term of the sequence will be, «0» or «1». Deficiency of correlations in generated sequences, and also sequences of several zeros and ones, the appearance probability of which considerably exceeds 0.5 is considered not to be the less important.

The Blum-Blum-Schub (BBS) generator [3], which is considered to be a cryptographically resistant one, is taken as a standard for the comparison with the CA generator.

II. DESCRIPTION OF THE MODELS

S. Wolfram, in his research [4], suggested to use an one-dimensional cellular automata, which is an array of cells $c_1, c_2, ., c_n$, the states of which in the following instant of time is determined by the rule:

$$c_i' = c_{i-1} \oplus (c_i \vee c_{i+1}) \qquad (1)$$

as a generator of pseudorandom numbers.

The pseudorandom sequence of bits can be generated by any of the n cells of one-dimensional array (see also [2].

The BBS generator was chosen as a generator of pseudorandom binary sequences for conducting comparative analysis. The iterative process of pseudorandom sequence bits generation in this case is described by following correlations:

$$x_i = (x_{i-1})^2 \bmod n, \; s_i = x_i \bmod 2, \qquad (2)$$

where $i = 1,2,3,\mathbf{K}$, $n = p \cdot q$ is the Blum number, and $p \bmod 4 = q \bmod 4 = 3 \bmod 4$, and iteration cycle initialization arises from the rule: $x_0 = x^2 \bmod n$, where x is an initial random prime number.

The parameters of BBS generator, which are used in this research, have the following values: $p = 24907$, $q = 8831$, $x = 1129$.

III. STATISTICAL ANALYSIS

Probability of generation of binary number representation 0,1,2,...,255 was analyzed for the comparative analysis conduction of the pseudorandom binary sequences characteristic, which are generated using the BBS and CA algorithms.

In the case of the equiprobable distribution we have $p(0) = p(1) = \mathbf{K} = p(255) = 1/256 = 0{,}00390625$. The results of analysis are presented in Fig. 1 (CA – on the top, BBS – on the bottom). For both cases sequences of 10.000.000 bits were generated.

The analysis of periodic correlations is conducted: the probability of «1» appearance on each next step of the binary sequence (0), through one step (1), through two steps (2), etc. Current probabilities are equal for a truly random sequence: $p(1,T_0) = p(1,T_1) = \mathbf{K} = 0{,}5$. Results are presented in Fig. 2 (CA – on the top, BBS – on the bottom). For both algorithms sequences of 100.000.000 bits were generated. In the case of BBS algorithm the apparent periodicity for probability of «1» appearance can be seen. This periodicity is the reason of initiation of peculiar bands (Fig. 3, on the bottom) filling the screen with black and white dots, 640×480 in size.

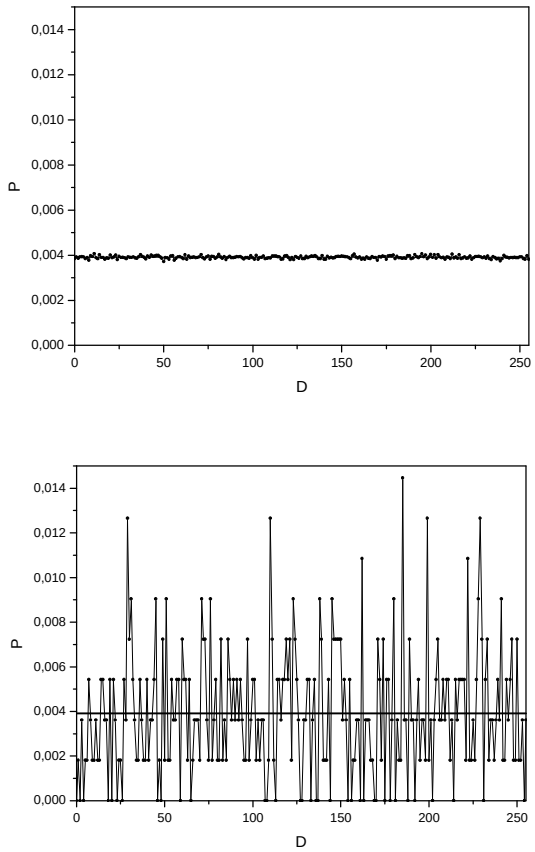

Figure 1. Results of the comparative analysis conduction of the pseudorandom binary sequences characteristic.

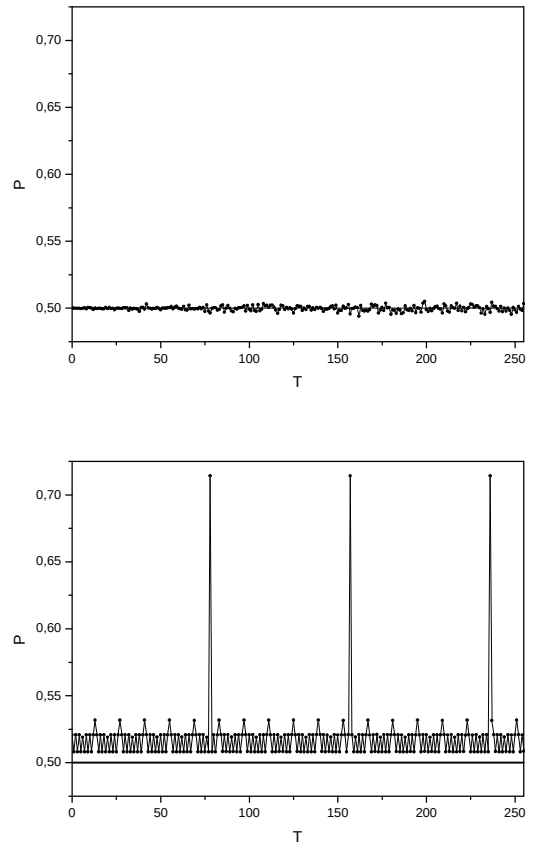

Figure 2. Results of the analysis of periodic correlations.

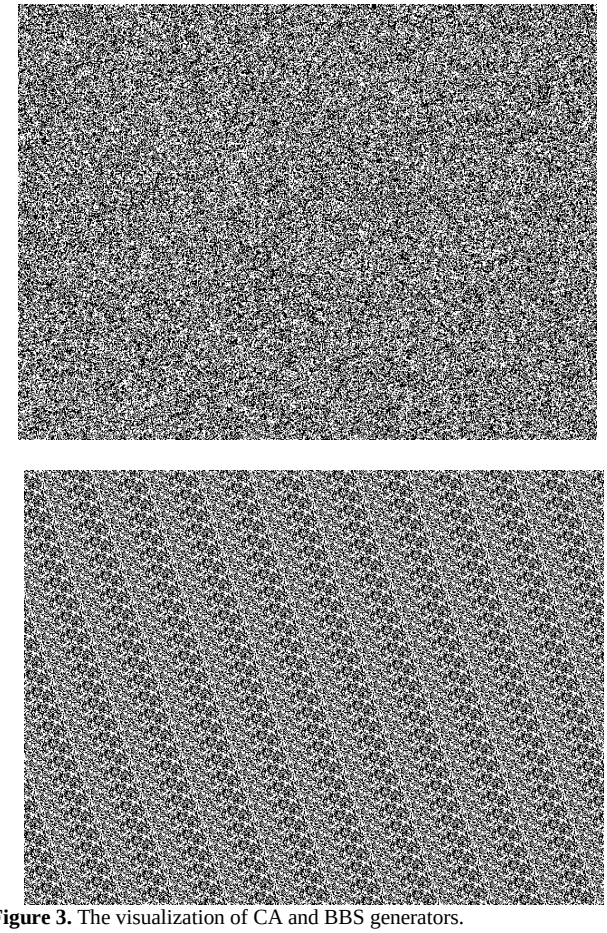

Figure 3. The visualization of CA and BBS generators.

IV. CRYPTOGRAPHIC ANALYSIS

Despite rather high degree of approximation to the «white noise» parameters, and therefore perspectives of the CA application in the cryptographic systems, the authors [5-7] mark the deficiency in CA that is successful cracking with known plain text. Indeed, relying on the main feature of CA, – the locality of cells interaction (each cell interacts just with the surrounding neighbours), it is possible to construct the stream ciphers decoding systems. For example, if except plaintext the area of bits sequence, generated by an adjacent cell (Fig. 4, upper part) is known, than the process of adjacent invisible bits values finding (Fig. 4, lower part) can arise from the following rule:

$$c_{i-1} = c_i' \oplus (c_i \vee c_{i+1}) \qquad (3)$$

Thus, we can get the set of the initial states of all cells array.

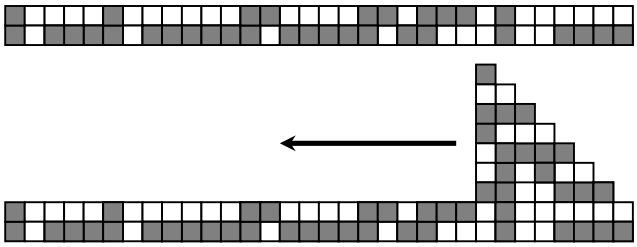

Figure 4. The rule of adjacent invisible bits values finding.

For the decline of such an attack probability we can offer a new CA class, based on the pseudorandom mechanism of interactive cells localization finding.

According to the invariable rule of cells state determination in next instant of time (1), it is suggested to form the numbers (addresses) of interactive cells from the adjacent cells set of bits (Fig. 5). In this case the rule of interaction can be written as:

$$c_i' = c_{a_1} \oplus \left(c_i \vee c_{a_2}\right), \quad (4)$$

where $a_1 = \left(i - 3 - \sum_{k=0}^{(\log_2 n)-1} c_{i-3-k} \cdot 2^k \right) \bmod n$,

$a_2 = \left(i + 3 + \sum_{k=0}^{(\log_2 n)-1} c_{i+3+k} \cdot 2^k \right) \bmod n$ – addresses of cells, which interacted with i^{th} cell, n – general amount of cells.

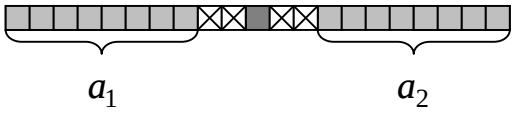

Figure 5. The formation of interactive cells numbers.

In the case when the initial CA state is the equiprobable equally distributed set of bits, than the state of some cell in the next instant of time will be defined pseudorandomly. In Fig. 6 the processes of CA changing through time with the single initial state are shown (Fig. 6, a CA behavior described by (1) is on the top; CA, described by (4) – on the bottom). Evidently at introduction of distributed nonlocal interactions mechanism, the system of cells behaves more chaotically, that inevitably leads to a greater cryptographic resistance of such an encryption method.

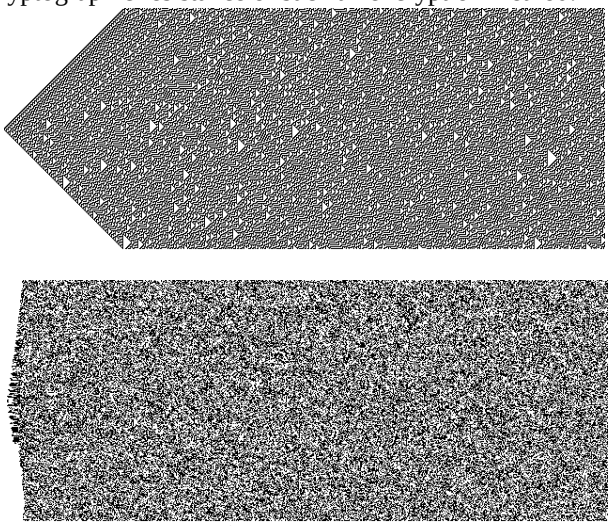

Figure 6. The processes of CA changing through time with the single initial state.

The perspective of CA application as program generators of pseudorandom numbers can be considered another proof of the validity of modification introduced by us. As it is generally known, the nature of traditional cellular automata is such, that the maximal velocity and efficiency is achieved during the algorithm realization by hardware, e.g. on the basis of n-discharged feedback registers. During the generation of pseudorandom sequences using the (4), it is possible to select not only from one certain cell of one-dimensional array, but, e.g., from every second one, without losing cryptographic resistance of stream ciphers, obtained in such a way. In this case speed of programmed generation of pseudorandom bits increases by $n/2$ times.

V. CONCLUSION

Based on the results of the research we can conclude about the perspectives of cellular automata application as a generator of pseudorandom binary sequences. It is indicated that CA algorithm in the best way satisfies the parameters of equiprobability of «0» and «1» appearance in comparison with BBS. In addition, for the cryptographic resistance increase the method of traditional CA modification by introducing the pseudorandom mechanism of determining the interactive cells localization is offered. This innovation, as well as the high velocity of such a process, enables CA algorithm application as program pseudorandom numbers generators.

REFERENCES

[1] W. Stallings. Cryptography and Network Security (4th edition), Hardcover, 2005, 564 p.

[2] D. R. Stinson. Cryptography: Theory and Practice. Hardcover, 2005. 436 p.

[3] B.Schneier. *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996, 816 p.

[4] S. Wolfram. Random sequence generation by cellular automata // Advances in Applied Mathematics, v.7, 1986, pp. 123-164.

[5] J. C. H. Castro, P. I. Viñuela, Evolutionary computation in computer security and cryptography, New Generation Computing, 2005, v.23 n.3, p.193-199.

[6] W. Meier and O. Staffelbach. Analysis of pseudorandom sequence generated by cellular automata // Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag, 1991, pp. 186-199.

[7] Feng Bao, Cryptanalysis of a Partially Known Cellular Automata Cryptosystem, IEEE Transactions on Computers, 2004, v.53 n.11, p.1493-1497.