Cryptoresistant Generator of Binary Key Sequences 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* — In this paper the cryptoresistant generator of pseudorandom binary consecution is developed and implemented on the basis of unidimensional cellular automata. The determined algorithm of regular bit selection, which can be easily reproduced on a receiving side, is offered. The statistical analysis of the obtained results is conducted by the package of NIST-STS.**

***Index Terms* — binary sequences, cellular automata, initial state, pseudorandom number generator, idle cycles**

I. INTRODUCTION

Today, because of the information transmitted open networks sudden development information security is of particular relevance. To protect such information stream ciphers are used, the main component of which is a key sequence generator. Such generators should be simple and quick, to be used for audio and video information.

There are many binary key stream generators, but despite a sufficient degree of reliability, they want better performance. Therefore, the development of simple quick and reliable pseudorandom binary sequences generators become urgent.

II. CALCULATIONS AND RESULTS

The aim of this work is to develop a key binary sequence generator which would satisfy the following requirements:

1. Generated sequence should pass statistical tests for randomness;
2. The sequence should be easily reproduced on the receiving side;
3. The generator quickness should be sufficient for streaming encryption.

As a binary sequence generator an one-dimensional cellular automata, which is in array of cells $c_1, c_2, ..., c_n$, the states of which in the following instant of time is determined by the rule:

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

is used.

The pseudorandom sequence of bits can be generated by any of the 256 cells of one-dimensional array or using a bits combination.

On the first stage of the development [3] the probability of generation of binary number representation $0,1,2,...,255$ was analyzed. In the case of the equiprobable distribution we have $p(0) = p(1) = ... = p(255) = 1/256 = 0{,}00390625$.

The results of analysis are presented in Fig. 1. The sequence of 10.000.000 bits was 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:. $p(1, T_0) = p(1, T_1) = ... = 0.5$ Results are presented in Fig. 2. The sequence of 100.000.000 bits was generated.

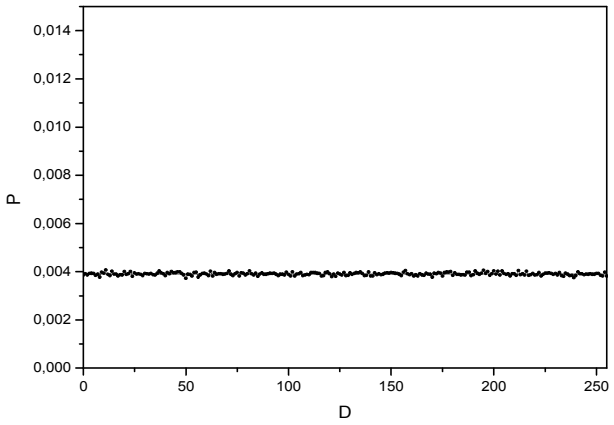

Figure 1. Results of the «0» and «1» distribution in the sequences.

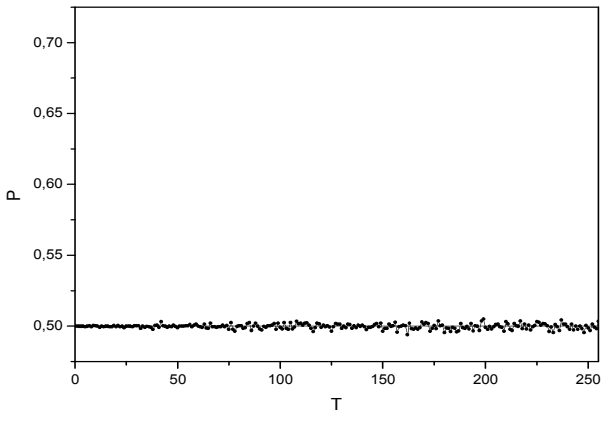

Figure 2. Results of the analysis of periodic correlations.

Simple statistical tests do not allow to judge the stability of cryptographically generated sequence. For elucidation of this question, we activated the statistical package NIST-STS, developed by the National Institute of Standards and

Technology USA [4] specifically for testing such generators. The received sequence is filed on the package entry. On output we get the results of 189 statistical tests. According to the testing method, if the probability of passing is grater than 0,9615 in the array of 10^8, the test is passed. The best generators must pass all NIST-STS tests.

In the first phase of the work with NIST-STS package, it was decided to analyze if it is possible to develop the cryptoresistant generator on the basis of cellular automata. This used the following «random-30-random» scheme: the generator start state was randomly choosen; the rule 30 of the cellular automata interaction was applied to the generated array, and a bit output to a file was selected pseudorandomly. The results (Fig. 3) allowed to conclude that the construction of such a generator is available.

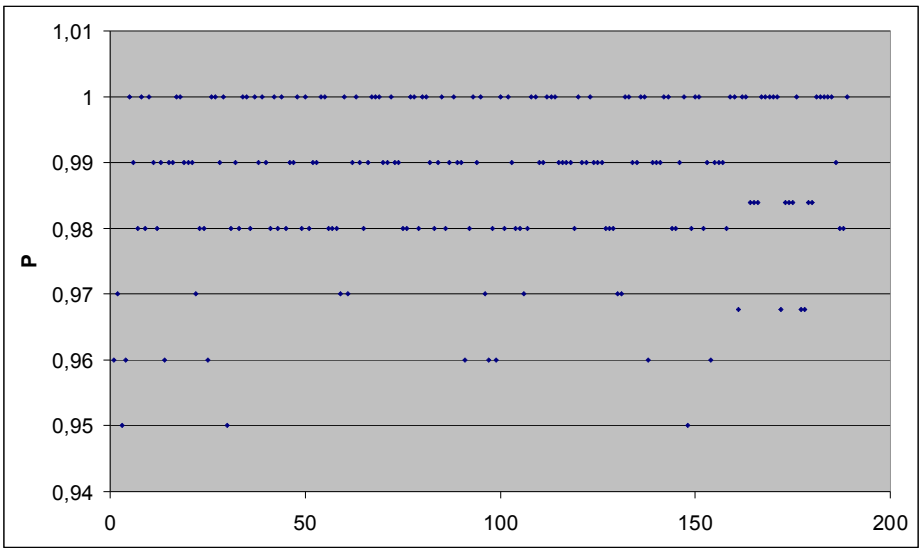

Figure 3. The testing results of the pseudorandom binary sequence statistical characteristics using the «random-30-random» scheme.

However, random nature of the initial state and outputting the resulting bits of the sequence does not allow to reproduce the state of the generator on the receiving side. Decrypting an encrypted data stream is impossible. Therefore it was decided to develop pseudorandom algorithms of the initial state formation and a key sequence the next bit outputting which can be easily reproduced on the receiving side. For this purpose a series of investigations on the sequence bits outputting mode impact was conducted.

In the first step start input of the array was carried out randomly, the rule 30 was applied to it and the entire array of 256 bits was output together. The received result is shown in Fig. 4. The figure shows that the average probability value is 0.77, which means that a significant part of tests is not passed.

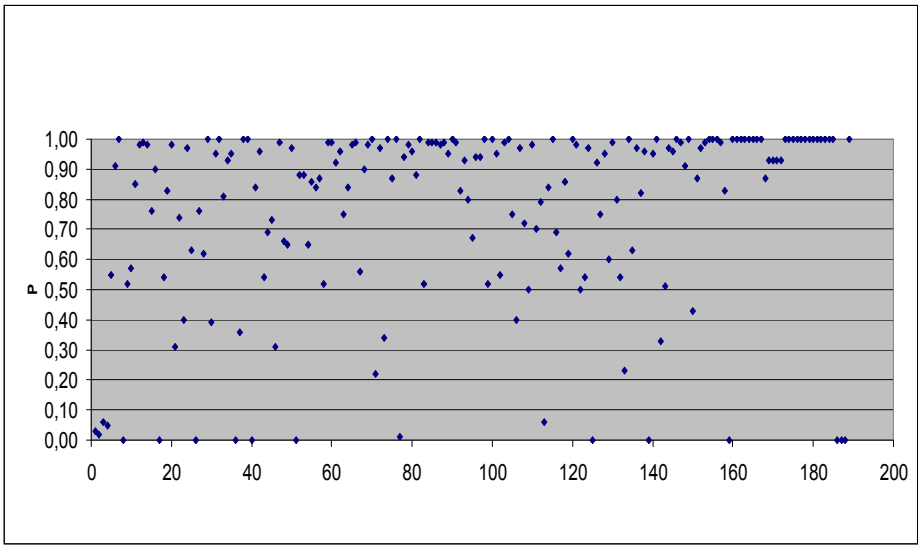

Figure 4. The result of statistical analysis of pseudorandom binary sequences, generated by the rule 30 with the continuous array output.

To improve results several bits of the array were combined using the XOR operation by the following rule

$$M[w] \cdot XOR \cdot M[v] \cdot XOR \cdot M[t], \qquad (2)$$

where w, v, t – array bit numbers.

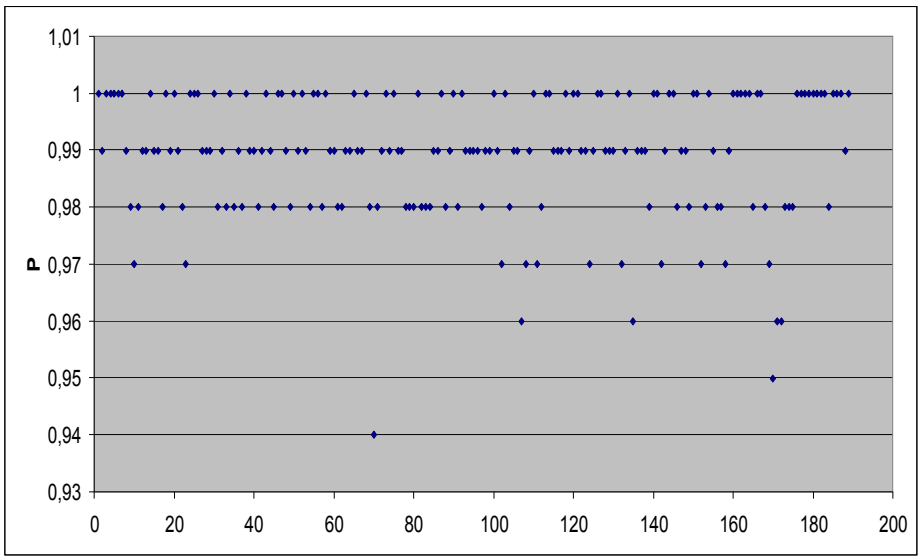

Figure 5. The result of statistical analysis of pseudorandom binary sequences with a combined array output.

The Fig. 5 shows that the results we've received are rather better than previous ones: only two values are below 0.96, so the way of bits sequence output greatly influences a generator cryptoresistance. It's further confirmed in the next step – the next *w* bit choice of (2) is set by the formula:

$$w = (i + 3 + \sum_{k=0}^{(\log_2 n)-1} C_{i+3+k} \cdot 2^k) \bmod n, \quad (3)$$

where C – value of the $i+3+k$ cell, n – general amount of cells.

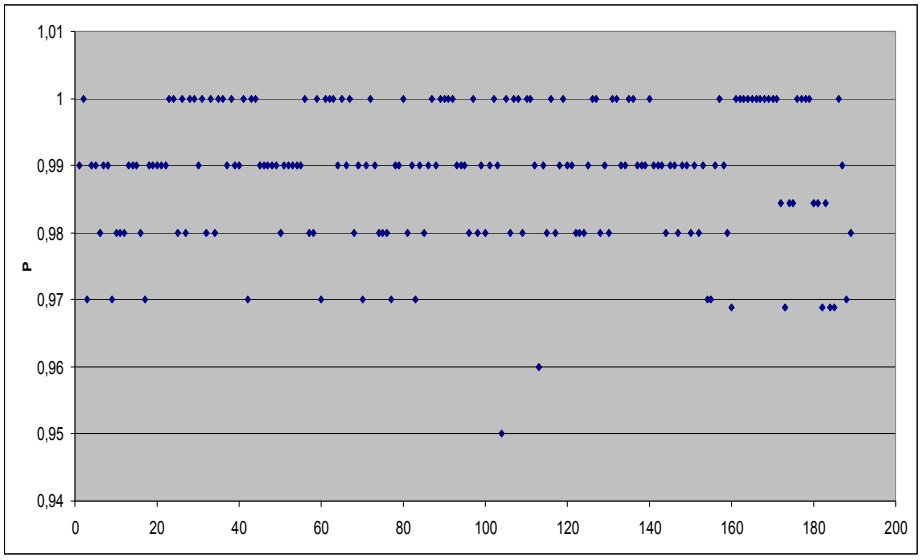

Figure 6. The result of statistical analysis of pseudorandom binary sequences with a combined array output the (3).

The Fig.6. shows even better results then those shown in fig.5, only one value is below 0,96.

On the basis of the investigations carried out we can make the following conclusions: statistical properties of the binary stream generator strongly depends on the output of the next beat sequence; generated sequence passes NIST-STS tests in the case of the combined bits output and does not pass it in the case of their consecutive output.

The next step was changing the initial state of the generator. The zero elements array in which only the 128 element was equal 1, was initialized.

In order to detect an optimal initial state idle cycles of cell interaction ranging from 150 to 550 without output were performed. The obtained results (Fig. 7) not point out any dear dependence of the average values of the NIST-STS tests on the number of idle cycles. All the values are concentrated around 0,98 and it is evident that the maximum value is observed at 250 cycles. So in this case the generator statistical portrait weakly depends on its initial state.

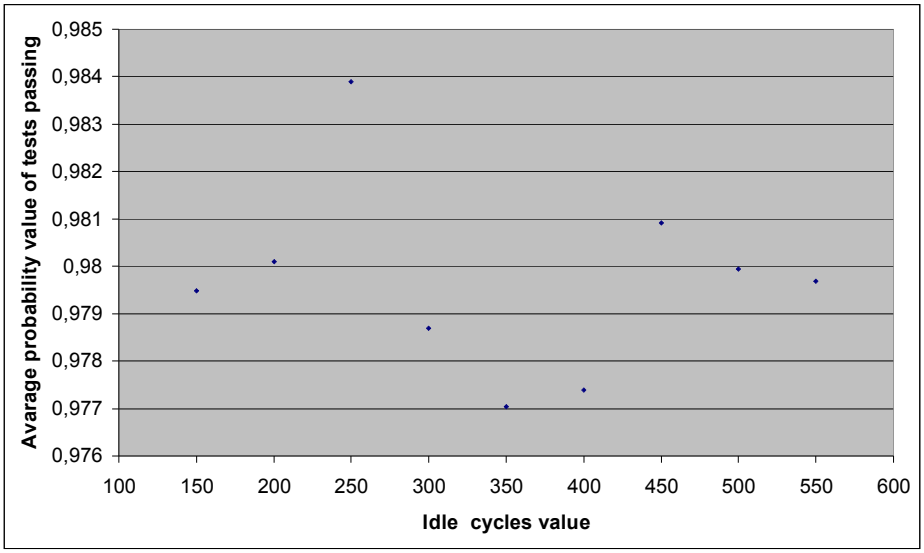

Figure 7. The idle cycles quantity of the NIST-STS tests average value dependence.

The last step was to investigate another mechanism of cells interaction, which considers the so-called «far interaction», that is an interaction with non-direct neighbors. As similarly to the previous step, a 256 bits array was filled with zeros and only the 128 bit equaled 1. 250 idle cycles of interaction without outputting were carried out, then initial array was processed by the 30 rule with «far interaction». Bits sequences output was done by (2), that is the array several bits combination.

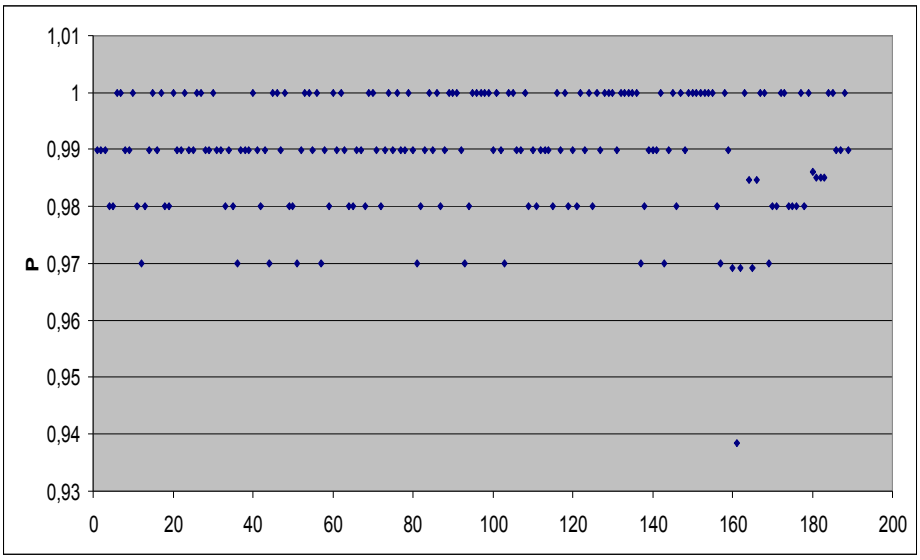

Figure 8. The result of statistical analysis of pseudorandom binary sequences with a «far interaction».

Results shown in Fig. 8. are the best of obtained ones – only one point is below 0.96.

III. CONCLUSION

Summarizing the conducted researches, we can made the following conclusions: a software key pseudorandom binary sequences generator both simple, and with «far interaction»on the basis of cellular automata (rule 30) was developed and implemented; investigations of generator statistical portrait using the NIST-STS package were carried out; strong dependence of a key sequence quality on the way of its bits output was found out; the dependence of a sequence quality on the initial generator state wasn't observeded.

The giving findings point out rather high quality of the developed generator, which can be used in the streaming encryption systems.

REFERENCES

[1] S. Wolfram. "Random sequence generation by cellular automata" // Advances in Applied Mathematics. – 1986. – v.7. – P. 123-164.

[2] W. Meier and O. Staffelbach. "Analysis of pseudo random sequence generated by cellular automata" // Advances in Cryptology EUROCRYPT '91 Proceedings, Springer-Verlag. – 1991. – P. 186-199.

[3] Sergey Ostapov, Vladimir Zhikharevich, Lidiya Val'. "Investigation of Properties of Pseudorandom Binary Sequences Generator on the Basis of Cellular Automata." // Prooceeding of the 9-th International Conference on DAS. – May 2008. –P. 115-117.

[4] Andrew Rukhin, Juan Soto, James Nechvatal, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications". NIST Special Publication 800-22; U.S.Government printing office Washington: 2000.