ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIV INFORMATICS TECHNOLOGIES

UDC 004.312.26

Val′ O. D.[1], Zhikharevich V. V.[2], Ovchar R. I.[3], Ostapov S. E.[4]

[1]*PhD, Associate professor, Associate professor of software department, Chernivtsi Yu. Fed'kovych National University, Chernivtsi, Ukraine*

[2]*PhD, Associate professor, Associate professor of software department, Chernivtsi Yu. Fed'kovych National University, Chernivtsi, Ukraine*

[3]*Assistant professor of software department, Chernivtsi Yu. Fed'kovych National University, Chernivtsi, Ukraine*

[4]*Dr. of Science, Professor, Head of the software department, Chernivtsi Yu. Fed'kovych National University, Chernivtsi, Ukraine*

DEVELOPMENT AND INVESTIGATION OF THE KEY STREAM GENERATORS ON THE BASE OF CELLULAR AUTOMATA

This paper presents the development and investigations of the binary key stream generators statistical characteristics. Developed generators based on the elementary rules of cells interaction: simple, modified and combined classical rules. We believe that elementary rules «30», «86», «135», «149» are most promising from statistical point of view. Modifications were consist of combining of array bits before outputting and combining various elementary rules of automaton cells interaction. It was developed a new simple interaction rule, based on the logical operation XOR. The investigation of statistical properties was performed using NIST STS v1.8. All designed generators showed good statistical characteristics, which indicates their satisfactory cryptoresistance. In addition we've investigated the developed generators linear complexity using Berlekamp-Massey algorithm. Obtained results shows the high values of linear complexity (about half of the cellular automaton length), which is typical for such structures type. On the base of the developed generator with own cells interaction rule has developed a system for secure communication of audio, text and file information. The statistical investigations of encrypted file showed that it satisfies all the NIST STS requirements.

Keywords: stream cipher, binary key stream generators, cellular automaton, statistical characteristics, secure communications system.

NOMENCLATURE

$A[i]$ is a value of i-th address array elements;

a is a calculated cell address;

$B[i]$ is a buffer array elements;

$C[i]$ is a value of i-th cellular automaton cell;

CA is a cellular automaton;

$C'[i]$ is a value of i-th cellular automaton cell after the interaction act;

$C_{A[a]}$ is a value of CA cell with address $A[a]$;

$C'_{A[i]}$ is a value of CA cell with address $A[i]$ after the interaction act;

$C_R[w]$ is a value of w-th elementary cellular automaton cell;

$C_{out}[w]$ is a value of w-th resulting CA cell after rules combination;

i,k is an array index;

n is a CA length;

NIST STS is a National Institute of Standards and Technologies Statistical Suite;

PIN is a Personal Identification Number;

PLD is a Programmable Logical Devices;

R is an elementary interaction rules; R=30, 86, 135, 149;

w is a calculated cell address.

INTRODUCTION

Today most of us are living in the information society. The result of this is a large amount of information, which is transmitted by the telecommunication systems. With an open data also increase amounts of confidential information, requirements for protection of which considerably amplified. Such tendency is observed in Ukraine, especially with the introduction of the personal data protection law. If at the beginning of the computer systems development means for protection of the files, which are transmitted by the network, were used, then today on foreground is protection of information in real time.

At the same time, in Ukraine smart cards are rapidly introduced into the daily life. Now the introduction of electronic passports, medical cards, student tickets and classification books is discussed. The number of different mobile devices is rapidly increasing. Most of these gadgets have limited computing resources, but they also need to protect data transmitted open communication channels.

DOI 10.15588/1607-3274-2015-3-7

In any protection system, such as authentication, PIN-code verification and so on, generators of pseudorandom sequences are used. Limitedness of computing resources requires the development of simple generating systems, which would easily compute in parallel. Speed parameters of protection systems and their optimization for specialized real time tasks become crucial. The best for these goals cellular automaton fit.

The main purpose of this paper is the development of the binary key stream generators based on cellular automata, investigation its statistical characteristics and linear complexity.

1 PROBLEM STATEMENT

Let us call the one-dimensional cellular automaton the array $C[i]$, where i=[0, n–1], each element of which are logical zero or one. The automaton state at each time determined by the all its elements states. Automaton transition in a next state is determined by so-called transition rules, which are determined by the elements (cells) interaction with other cells that are at some distance from the selected cell. Elementary interaction rules, defined in [1], set the cell interaction with nearest neighbors.

For example, the famous rule «30» may be written as a Boolean function:

$$C'[i] = C[i-1] \oplus (C[i+1] \vee C[i];$$

or as an arithmetic function:

$$C'[i] = (C[i–1] + C[i] + C[i+1] + C[i–1]C[i+1]) \bmod 2.$$

To avoid the first and last cell's problem automaton is «rolled» in the torus.

Another transition rules are produced similarly. We've used the «86», «135», «149» rules (see Table 1). There are 256 elementary transition rules, as it shown in [1].

Researchers can also design your own transition rules that take into account the interaction with randomly or pseudo-selected cells, or with no-neighboring cells. This makes the CA modifications and their use almost unlimited.

2 REVIEW OF THE LITERATURE

The first conclusions about the usage of CA for pseudorandom binary sequences generation in cryptographic purposes are found in the Stephen Wolfram work [1]. Soon investigations aimed at proving of the feasibility of specific applications realization appear [2–6]. In the past ten years there have been publications that describe specific generation or encryption algorithms based on the cellular automata. Among these works are articles of S. K. Rososhek et al [7] and Jegadish Kumar K. J. [8] which describes the symmetric encryption systems based on two-dimensional CA. B. M. Suhinin article [9] is about developed hardware implementation on PLD of a high-speed pseudorandom binary sequences generator on the basis of CA. Norziana Jamil article [10] is devoted to the development and researching of hash function, which uses elementary CA rules for mixing bits of a message.

However, despite of the use of the elementary rules of CA cell interactions in the cryptographic purposes, their statistical properties are insufficiently studied. For example, there is no rigorous justification for the certain rules using, the possibility of their combinations using, compatibility, linear complexity, and other characteristics that may influence on the effectiveness of one-dimensional CA application.

Elementary rules of CA interaction were identified and classified by Stephen Wolfram in [11]. Totally 256 rules of the cell interaction, divided into several classes are allocated. Each class is formed of the, so-called, statistically equivalent rules, i.e. those that can be derived from each other using simple logical change – conjunctive, reflexive and conjunctive-reflexive. Also in [1] mentions that the rule «30» by its statistical characteristics can produce qualitative generator of pseudorandom binary sequences. Therefore, for research were selected all rules belonging to one class with the rule «30» («86», «135», «149») and a few others for comparison [12].

Conducted researches prove that all rules which are in a same class with the rule «30» have such statistical properties [8], which allow use them in different modifications for developing of the cryptoresistant pseudorandom binary sequences generator. As modifications, various options of array outputting, the initial generator state effect and etc. were investigated [13].

3 MATERIALS AND METHODS

The next question that should be explained – how these characteristics can be improved by using combinations of cell interaction rules. In [14–15] it is shown that the best results show a combination of rules that belong to the same class, and combined rules must also have good statistical properties. So we have to use a combination of rules «30», «86», «135», «149».

The sequences bits were combined in the following way. We use four cellular automata that implement these intercellular rules. Each CA output bits was selected by the formula:

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

The output bits was combined each other in various ways, but the best statistical characteristics was demonstrated by generator, which sequence was formed by the rule:

$$C_{out}[w] = (C_{30}[w] \oplus C_{86}[w] \oplus 1) \oplus (C_{30}[w] \oplus \\ \oplus C_{135}[w] \oplus 1) \oplus (C_{30}[w] \oplus C_{149}[w] \oplus 1). \qquad (1)$$

Table 1 – Elementary transition rules in the cellular automata

No	Rules	Boolean form	Arithmetic form
1	«30»	$C'[i] = C[i-1] \oplus (C[i+1] \vee C[i]$	$C'[i] = (C[i–1] + C[i] + C[i+1] + C[i-1]\ C[i+1]) \bmod 2$
2	«86»	$C'[i] = C[i-1] \vee (C[i+1] \oplus C[i])$	$C'[i]=(C[i–1]+C[i]+C[i–1]C[i]+C[i+1]) \bmod 2$
3	«135»	$C'[i] = 1 \vee C[i-1] \oplus (C[i] \vee C[i+1]$	$C'[i]=(1+C[i–1]+C[i]C[i+1]) \bmod 2$
4	«149»	$C'[i] = C[i-1] \vee (C[i] \oplus C[i+1] \vee 1$	$C'[i]=(1+C[i–1]C[i]+C[i+1]) \bmod 2$

Another way to study the suitability of CA to generate high-quality pseudorandom key sequences was designing of intercellular interaction alternative rules.

We can propose the following rule. CA contains cells with logical «1» and «0». We use the address array $A[i]$ to select the interacting cells. This array contains decimal numbers (cell's addresses) from 1 to n, pseudo-random filled and duplicated in the buffer array $B[i]$. Cells interact by the simple rule on the base of XOR. Interacted cells are selected as follows:

$$C'_{A[i]} = C_{A[a]} \oplus C_{A[i+1]} \oplus C_{A[i]}; \qquad (2)$$

$$a = (i + 1 + \sum_{k=0}^{(\log_2 n)-1} C_{i+1+k} 2^{(\log_2 n)-1-k}) \bmod n. \qquad (3)$$

First of all, it's necessary to select the target cell address. This cell will contain the interaction result. Its address is determined by the address array $A[i]$. Then we may determine the address of first interaction cell $A[i+1]$. The address of a second interacting cell $A[a]$ is calculated by (3). Here we use the CA cells. The interaction result is recorded to the CA cell and outputted as a next key bit. After the interaction act the i-th and a-th elements of the buffer array are swapped: $B[i] \Leftrightarrow B[a]$. If the array index i is reached its end, the address array $A[i]$ is swapped with the buffer array $B[i]$:

$$\sum_{i=1}^{n} A[i] \Leftrightarrow \sum_{i=1}^{n} B[i].$$

These steps continue as long as necessary for encryption or investigation of the statistical and other generator's characteristics. We have investigated the statistical characteristics and the linear complexity of the obtained key sequences. In the last case we've used the Berlekamp-Massey algorithm [16].

In all cases we have a binary stream, which have been used as key stream in G. Vernam cipher (one-time pad).

4 EXPERIMENTS

Computer programs that implement the proposed generators and encryption systems have been developed. In all cases, we've used cellular automata length of 256 bits.

Statistical investigations of the obtained sequences were performed by the NIST STS technique, which is usual for pseudorandom generators testing [17].

According to this technique it was generated the binary sequences with the length of 10^8 bits each. The sequences were fed to the input of NIST STS v.1.8 as a text file. Statistical suite divided these sequences at the 100 equal parts of 10^6 bits each, making it possible to explore the 100 sequences.

These sequences have been tested by 16-th different groups of tests: frequency and block-frequency tests; cumulative-sums test; runs and longest-run tests; binary matrix rank test; digital Fourier transform; nonperiodic- and overlapping-templates tests; universal test; random-excursions tests; serial test; Lempel-Ziv test; linear-complexity test.

Because of these tests are running with different parameters, we've obtained the vector with 189 values. Details of the method are described in [11], but we can assume that the whole key sequence have passed the statistical test only if at least 96 of the 100 investigated parts have passed the test.

NIST STS returns the sequence statistical portrait in the text file «FinalAnalysisReport», and than we have built the resulting histograms are shown below.

Additionally we performed linear-complexity tests by the Berlekamp-Massey algorithm for the 256-, 2560- and 25600-bits key sequences. In all cases, we have generated 10 sequences and calculated linear complexity for each of them.

5 RESULTS

Statistical testing results are shown in the fig. 1–2.

The results of linear-complexity investigations are shown in fig. 3. We've studied the various elementary rules for cellular automaton length of 256 bits.

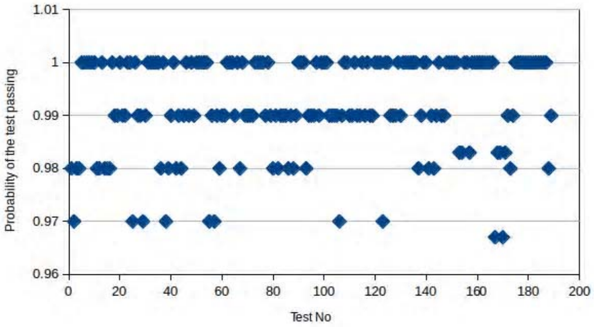

Figure 1 – Statistical portrait of the generator on the base of rule (1)

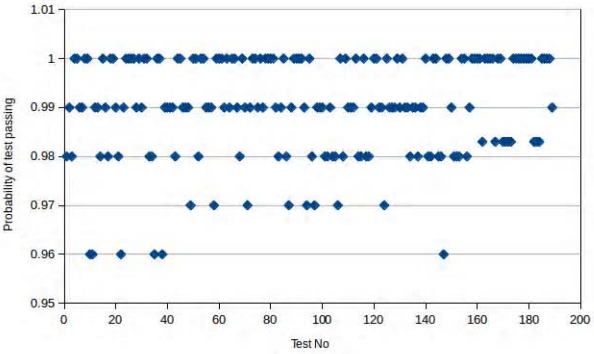

Figure 2 – Statistical portrait of the generator on the base of rule (2)

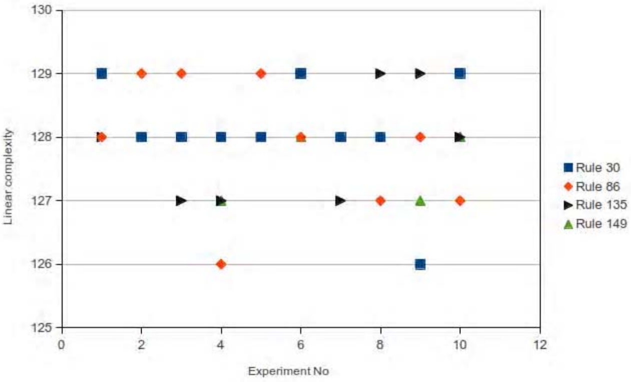

Figure 3 – The results of linear-complexity investigations for the generators on the base of different elementary rules (automaton length – 256 bits)

As a final result of our research, we have developed software for secure data exchange. The software allows you to share encrypted audio information in real time and provides secure text messages (chat) and file exchange. We have used the G. Vernam cipher on the base of developed key sequence generators.

The results of the statistical tests of the input text and encrypted file are shown in fig. 4–5.

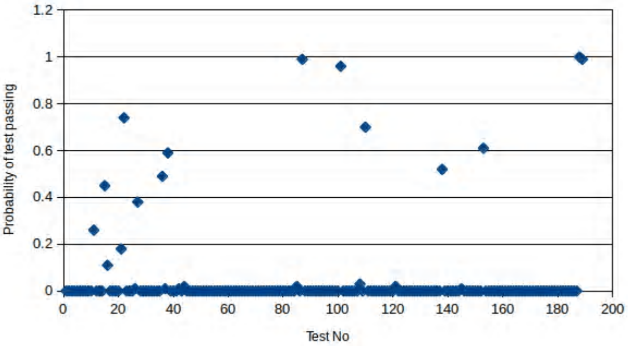

Figure 4 – Statistical portrait of the input text file

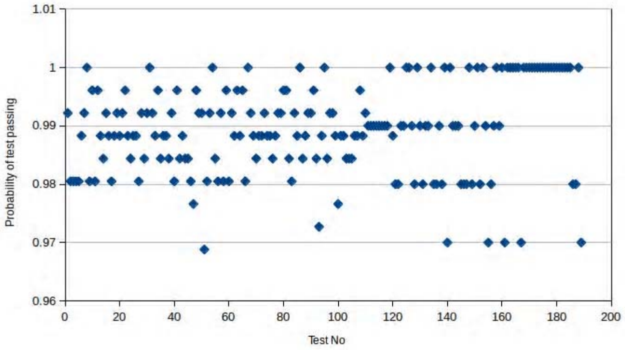

Figure 5 – Statistical portrait of the text file encrypted by stream cipher

6 DISCUSSION

One can see from fig. 1–2, the developed generators have successfully passed all of the statistical NIST tests. In the first case, almost all tests passed with the value >0.97 and only two of them are below this mark.

In the second case (see fig. 2) only five tests are passed with the value 0.96 and rest of them – with the value 0.97 or higher.

These results indicate the high statistical characteristics of the developed generators.

The high statistical characteristics are confirmed by large values of linear complexity. As one can see from fig. 3, the linear complexity values are located near the half of CA length: ~128 for 256-bit CA; ~ 1280 and 12800 – for 2560 – and 25600-bit CA respectively. It is known (see [18]) that the high linear complexity values are traditional for binary pseudorandom generators, which was demonstrated in our paper. Moreover, the NIST STS also has a linear-complexity test, and all our generators have passed it with the value not less than 0.98. High linear complexity values was shown by those generators, which not demonstrated the satisfactory statistical characteristics, such as rules «22», «54», «73», «150», «158». Perhaps in the future one can use these rules in the hash function or block ciphers construction as an additional diffusion or confusion element.

The statistical portraits of the input text and encrypted by stream cipher file are shown in fig. 4–5. It was necessary to perform such investigations in order to assess the quality of encryption subsystem in the actual operating conditions. Fig. 4 shows that the input file (Microsoft Word document) passed only three from 189 NIST STS tests. The encrypted file passed all 189 tests (see fig. 5). This fact confirms the results of statistical investigation of the generator on the base of (2), which was used in this software.

The aim of this development was to show the potential of the developed generator applying in the stream data exchange systems. This software gives an opportunity of the real time data exchanging for the network users. It can provide secure voice communication or protected text messages transmission (chat) or other files exchange. The software architecture is client-server and can be used in peer-to-peer networks [19].

When two subscribers open the connection generation and synchronization of encryption key using Diffie-Hellman-Merkle algorithm is implemented. The received general key is used for stream encryption based on cellular automata system initialization, or for symmetric cryptosystem based on Blowfish encryption algorithm session key creation.

CONCLUSION

Summarizing the conducted researches, we can make the following conclusions.

1. For the first time the systematic researches of the statistical characteristics of the pseudorandom binary sequences generators on the basis of elementary CA were conducted. The possibility of modified cell interaction rules application for pseudorandom sequences generating is shown.

2. It was shown that one of the effective ways to increase such generators cryptoresistance is a combination of different cell interaction rules.

3. For the first time the simple interaction rule on the base of XOR was proposed. This rule allows generating binary sequences with good statistical characteristics.

4. Secure voice, text and file exchanging software based on the developed generator was created. This software allows perform protection of audio stream in real time, which indicates on their high speed characteristics.

ACKNOWLEDGEMENTS

This investigation is supported by the department research project of Chernivtsi Yury Fed’kovych National University «Dynamic systems: modeling and software development» (state registration number 0110U005858).

REFERENCES

1. Wolfram S. Random sequence generation by cellular automata / S. Wolfram // Advances in Applied Mathematics. – 1986. – Vol. 7. – P. 123–164. DOI: http://dx.doi.org/10.1016/0196-8858(86)90028-X
2. Kar B. K. Theory and applications of cellular automata in cryptography / B. K. Kar, S. Nandi, P. P. Chaundhuri // IEEE Transactions on Computers. – 1994. – Vol. 43(12). – P. 1346–1357. DOI: http://dx.doi.org/10.1109/12.338094
3. Mazoyer J. Signals in one-dimensional cellular automata / J. Mazoyer, V. Terrier // Theoretical Computer Science. – 1999. – Vol. 217(1). – P. 53–80. DOI: http://dx.doi.org/10.1016/S0304-3975(98)00150-9

4. Mihaljevic M. A cellular automaton based fast one-way hash function suitable for hardware implementation / M. Mihaljevic, Y. Zheng, H. Imai // Public Key Cryptography : Lecture Notes in Computer Science. – Springer Verlag. – 1988. – P. 217–234. DOI: http://dx.doi.org/10.1007/BFb0054027
5. Porter R. B. Evolving FPGA based cellular automata / R. B. Porter, N. W. Bergmann // In: B. McKay, X. Yao, C. S. Newton, J-H. Kim, and T. Furuhashi (eds.). – SEAL : Lecture Notes in Computer Science. – 1998, Vol. 1585. – P. 114–121. DOI: http://dx.doi.org/10.1007/3-540-48873-1_16
6. Seredynski F. Cellular automata computations and secret key cryptography / F. Seredynski, P. Bouvry, A. V. Zomaya // Parallel Computing. – 2003. – Vol. 30. – P. 753–766. DOI: http://dx.doi.org/10.1016/j.parco.2003.12.014
7. Росошек С. К. Криптосистемы клеточных автоматов / С. К. Росошек, С. И. Боровков, О. О. Евсютин // Прикладная дискретная математика. – 2008. – Т. 1 (1). – С. 43–49. – [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/kriptosistemy-kletochnyh-avtomatov
8. Jegadish Kumar K. J. Novel and Efficient Cellular Automata Based Symmetric Key Encryption Algorithm for Wireless Sensor Networks / K. J. Jegadish Kumar, K. Chenna Kesava Reddy, S. Salivahanan // International Journal of Computer Applications. – 2011. – Vol. 13(4). – P. 30–37. DOI: http://dx.doi.org/10.5120/1767-2424
9. Сухинин Б. М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов / Б. М. Сухинин // Прикладная дискретная математика. – 2010. – Т. 2 (8). – С. 34–41. – [Электронный ресурс]. – Режим доступа: http://cyberleninka.ru/article/n/vysokoskorostnye-generatory-psevdosluchaynyh-posledovatelnostey-na-osnove-kletochnyh-avtomatov
10. Norziana J. A New Cryptographic Hash Function Based on Cellular Automata Rules 30, 134 and Omega-Flip Network / J. Norziana, M. Ramlan, Muhammad Reza Z'aba // 2012 International Conference on Information and Computer networks (ICICN-2012). – IACSIT Press, Singapore. – 2012. – V. 27. – P. 163–169. – [Electronic resource]. – Access mode: http://www.ipcsit.com/vol27/32-ICICN2012-N10006.pdf
11. Wolfram S. A New Kind of Science / S. Wolfram // Wolfram Media, Inc. – 2002. – 1197 p. – [Electronic resource]. – Access mode: http://www.wolframscience.com/nksonline/toc.html
12. Валь Л. О. Розробка та дослідження криптостійкого генератора двійкових послідовностей на основі клітинних автоматів / Л. О. Валь, В. В. Жихаревич, С. Е. Остапов // Науковий вісник Чернівецького університету. Комп'ютерні системи і компоненти. – 2009. – № 479. – С. 147–150.
13. Валь Л. О. Використання клітинних автоматів для генерування псевдовипадкових двійкових послідовностей / Л. О. Валь, В. В. Жихаревич, С. Е. Остапов // Науковий вісник Чернівецького університету. Комп'ютерні системи і компоненти. – 2010. – Т. 1 (1). – С. 67–72.
14. Чайка Л. О. Криптостійкий генератор псевдовипадкових послідовностей на основі клітинних автоматів / Л. О. Чайка, В. В. Жихаревич, С. Е. Остапов // Вісник Національного університету імені Тараса Шевченко. Серія фізико-математичних наук. – 2011. – № 1. – С. 215–219.
15. Валь О. Д. Розробка та дослідження генераторів ключового потоку на основі комбінації клітинних автоматів / О. Д. Валь, Л. О. Чайка, С. Е. Остапов // Науковий вісник Чернівецького університету. Комп'ютерні системи і компоненти. – 2012. – Т. 3 (2). – С. 6–11.
16. Остапов С. Э. Генераторы псевдослучайных последовательностей на основе клеточных автоматов / С. Э. Остапов, Л. А. Чайка // Информационные технологи и системы в менеджменте, образовании, науке ; под. общей ред. В. С. Пономаренко. – Харьков : Цифрова друкарня. – 2013. –№ 1. – С. 178–190.
17. Потій О. В. Метод статистичного тестування NIST STS та математичне обґрунтування тестів / О. В. Потій, А. В. Лєншин, Ю. А. Ізбенко // Технічний звіт ІІТ-001-2004. – Інститут інформаційних технологій. – 2004. – 62 с.
18. Кренгель Е. И. Исследование и разработка новых классов псевдослучайных последовательностей и устройств их генерирования для систем кодовым разделением каналов / Е. И. Кренгель // [Электронный ресурс]. – Режим доступа: http://1-ebook.com/asu-peredacha-dannih/lineynaya-slojnost.html.
19. Система захищеного обміну даними на основі клітинних автоматів / [Л. О. Чайка, В. В. Жихаревич, Р. І. Овчар, С. Е. Остапов] // Науковий вісник Чернівецького університету. Комп'ютерні системи і компоненти. – 2011. – Т. 2 (1). – С. 15–20.

Article was submitted 13.01.2015.
After revision 03.02.2015.

Валь А. Д.[1], Жихаревич В. В.[2], Овчар Р. И.[3], Остапов С. Э.[4]

[1]Канд. физ.-мат. наук, доцент, доцент кафедры программного обеспечения компьютерных систем Черновицкого Национального университета имени Юрия Федьковича, Черновцы, Украина

[2]Канд. физ.-мат. наук, доцент, доцент кафедры программного обеспечения компьютерных систем Черновицкого Национального университета имени Юрия Федьковича, Черновцы, Украина

[3]Ассистент кафедры программного обеспечения компьютерных систем Черновицкого Национального университета имени Юрия Федьковича, Черновцы, Украина

[4]Д-р. физ.-мат. наук, профессор, заведующий кафедрой программного обеспечения компьютерных систем Черновицкого Национального университета имени Юрия Федьковича, Черновцы, Украина

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ГЕНЕРАТОРОВ КЛЮЧЕВОГО ПОТОКА НА ОСНОВЕ КЛЕТОЧНЫХ АВТОМАТОВ

В работе представлены результаты разработки и исследования статистических характеристик генераторов бинарного ключевого потока на основе клеточных автоматов. Разработанные генераторы используют элементарные правила межклеточного взаимодействия, «30», «86», «135» и «149», как наиболее обещающие со статистической точки зрения. Модификации правил заключались как в комбинировании самих правил взаимодействия, так и битов массивов перед выводом очередного бита. Разработано собственное правило межклеточного взаимодействия на основе сложения по модулю два. Исследования статистических характеристик выполнялись с помощью пакета NIST STS v1.8. Все разработанные генераторы продемонстрировали хорошие статистические свойства, которые подтверждают их удовлетворительную криптостойкость. Исследована также линейная сложность разработанных генераторов с использованием алгоритма Берлекемпа-Месси. Получены высокие значения линейной сложности (около половины длины клеточного автомата), что считается традиционным для такого рода систем. На основе исследованных генераторов разработана система защищенного обмена аудио-, текстовой и файловой информацией в реальном времени, что свидетельствует о высоком быстродействии системы защиты. Статистические тесты показывают, что система удовлетворяет всем требованиям NIST STS.

Ключевые слова: потоковый шифр, генератор бинарного ключевого потока, клеточный автомат, статистические характеристики, система защищенного обмена данными.

Валь О. Д.[1], Жихаревич В. В.[2], Овчар Р. І.[3], Остапов С. Е.[4]

[1]Канд. фіз.-мат. наук, доцент, доцент кафедри програмного забезпечення комп'ютерних систем Чернівецького Національного університету імені Юрія Федьковича, Чернівці, Україна

[2]Канд. фіз.-мат. наук, доцент, доцент кафедри програмного забезпечення комп'ютерних систем Чернівецького Національного університету імені Юрія Федьковича, Чернівці, Україна

[3]Асистент кафедри програмного забезпечення комп'ютерних систем Чернівецького Національного університету імені Юрія Федьковича, Чернівці, Україна

[4]Д-р фіз.-мат. наук, професор, завідувач кафедри програмного забезпечення комп'ютерних систем Чернівецького Національного університету імені Юрія Федьковича, Чернівці, Україна

РОЗРОБКА ТА ДОСЛІДЖЕННЯ ГЕНЕРАТОРІВ БІНАРНОГО КЛЮЧОВОГО ПОТОКУ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ

В роботі подано результати розробки та дослідження статистичних характеристик генераторів бінарного ключового потоку на основі клітинних автоматів. Розроблені генератори використовують елементарні правила міжклітинної взаємодії, «30», «86», «135» и «149», як найбільш перспективні зі статистичної точки зору. Модифікації правил зводилися як до комбінування власне правил взаємодії, так і бітів масиву перед виводом чергового біта. Розроблено власне правило міжклітинної взаємодії на основі додавання за модулем два. Дослідження статистичних характеристик виконувалося за допомогою пакета NIST STS v1.8. Усі розроблені генератори продемонстрували хороші статистичні властивості, що підтверджує їх задовільну криптостійкість. Досліджено також лінійну складність з використанням алгоритму Берлекемпа-Мессі та отримано високі її значення (приблизно половину довжини клітинного автомата), що вважається традиційним для такого роду систем. На базі досліджених генераторів розроблено систему захищеного обміну аудіо-, текстовою та файловою інформацією в реальному часі, що свідчить про високу швидкодію системи захисту. Результати статистичних тестів демонструють, що система задовольняє усі вимоги NIST STS.

Ключові слова: потоковий шифр, генератор бінарного ключового потоку, клітинний автомат, статистичні характеристики, система захищеного обміну даними.

REFERENCES

1. Wolfram S. Random sequence generation by cellular automata, *Advances in Applied Mathematics*, 1986, Vol. 7, pp. 123–164. DOI: http://dx.doi.org/10.1016/0196-8858(86)90028-X
2. Kar B. K., Nandi S., Chaundhuri P. P. Theory and applications of cellular automata in cryptography, *IEEE Transactions on Computers*, 1994, Vol. 43 (12), pp. 1346–1357. DOI: http://dx.doi.org/10.1109/12.338094
3. Mazoyer J., Terrier V. Signals in one-dimensional cellular automata, *Theoretical Computer Science,* 1999, Vol. 217 (1), pp. 53–80. DOI: http://dx.doi.org/10.1016/S0304-3975(98)00150-9
4. Mihaljevic M., Zheng Y., Imai H. A cellular automaton based fast one-way hash function suitable for hardware implementation, *Public Key Cryptography: Lecture Notes in Computer Science*. Springer Verlag, 1988, pp. 217–234. DOI: http://dx.doi.org/10.1007/BFb0054027
5. Porter R. B., Bergmann N. W. Evolving FPGA based cellular automata, In: B. McKay, X. Yao, C. S. Newton, J-H. Kim, and T. Furuhashi (eds.), *SEAL : Lecture Notes in Computer Science*, 1998, Vol. 1585, pp. 114–121. DOI: http://dx.doi.org/10.1007/3-540-48873-1_16
6. Seredynski F., Bouvry P., Zomaya A. V. Cellular automata computations and secret key cryptography, *Parallel Computing*, 2003, Vol. 30, P. 753–766. DOI: http://dx.doi.org/10.1016/j.parco.2003.12.014
7. Rososhek S. K., Borovkov S. I., Evsjutin O. O. Kriptosistemy kletochnyh avtomatov, *Prikladnaja diskretnaja matematika*, 2008, Vol. 1 (1), pp. 43–49. – [Electronic resource]. – Access mode: http://cyberleninka.ru/article/n/kriptosistemy-kletochnyh-avtomatov
8. Jegadish Kumar K. J., Chenna Kesava Reddy K., Salivahanan S. Novel and Efficient Cellular Automata Based Symmetric Key Encryption Algorithm for Wireless Sensor Networks, *International Journal of Computer Applications*, 2011, Vol. 13(4), pp. 30–37. DOI: http://dx.doi.org/10.5120/1767-2424
9. Suhinin B. M. Vysokoskorostnye generatory psevdosluchajnyh posledovatel'nostej na osnove kletochnyh avtomatov, *Prikladnaja diskretnaja matematika*, 2010, Vol. 2(8), pp. 34–41. [Electronic resource]. Access mode: http://cyberleninka.ru/article/n/vysokoskorostnye-generatory-psevdosluchaynyh-posledovatelnostey-na-osnove-kletochnyh-avtomatov
10. Norziana J., Ramlan M., Muhammad Reza Z'aba A New Cryptographic Hash Function Based on Cellular Automata Rules 30, 134 and Omega-Flip Network /J. Norziana, M. Ramlan, Muhammad Reza Z'aba, *2012 International Conference on Information and Computer networks (ICICN-2012)*, IACSIT Press, Singapore, 2012, Vol. 27, pp. 163–169. [Electronic resource]. Access mode: http://www.ipcsit.com/vol27/32-ICICN2012-N10006.pdf
11. Wolfram S. A New Kind of Science, *Wolfram Media, Inc.*, 2002, 1197 p. [Electronic resource]. Access mode: http://www.wolframscience.com/nksonline/toc.html
12. Val' L. O., Zhyharevych V. V., Ostapov S. E. Rozrobka ta doslidzhennja kryptostijkogo generatora dvijkovyh poslidovnostej na osnovi klitynnyh avtomativ, *Naukovyj visnyk Chernivec'kogo universytetu. Komp'juterni systemy i komponenty*, 2009, No. 479, pp. 147–150.
13. Val' L. O., Zhyharevych V. V., Ostapov S. E. Vykorystannja klitynnyh avtomativ dlja generuvannja psevdovypadkovyh dvijkovyh poslidovnostej, *Naukovyj visnyk Chernivec'kogo universytetu. Komp'juterni systemy i komponenty*, 2010, Vol. 1 (1), pp. 67–72.
14. Chaika L. O., Zhyharevych V. V., Ostapov S. E. Kryptostijkyj generator psevdovypadkovyh poslidovnostej na osnovi klitynnyh avtomativ, *Visnyk Nacional'nogo universytetu imeni Tarasa Shevchenko. Serija fizyko-matematychnyh nauk,* 2011, No. 1, pp. 215–219.
15. Val' O. D., Chaika L. O., Ostapov S. E. Rozrobka ta doslidzhennja generatoriv kljuchovogo potoku na osnovi kombinacii' klitynnyh avtomativ, *Naukovyj visnyk Chernivec'kogo universytetu. Komp'juterni systemy i komponenty*, 2012, Vol. 3(2), pp. 6–11.
16. Ostapov S. E., Chaika L. A. Generatory psevdosluchajnyh posledovatel'nostej na osnove kletochnyh avtomatov, *In: Informacionnye tehnologii i sistemy v menedzhmente, obrazovanii, nauke: V. S. Ponomarenko (eds).* Harkiv, Cyfrova drukarnja No. 1, 2013, pp. 178–190.
17. Potij O. V., Lenshyn A. V., Izbenko Yu. A. Metod statystychnogo testuvannja NIST STS ta matematychne obg'runtuvannja testiv, *Tehnichnyi zvit IIT-001-2004. Instytut informatsiynyh tehnologiy*, 2004, 62 p.
18. Krengel E. I. Issledovanie i razrabotka novyh klassov psevdosluchajnyh posledovatel'nostej i ustrojstv ih generirovanija dlja sistem kodovym razdeleniem kanalov. [Electronic resource]. Access mode: http://1-ebook.com/asu-peredacha-dannih/lineynaya-slojnost.html.
19. Chaika L. O., Zhikharevich V. V., Ovchar R. I., Ostapov S. E. Systema zahyshhenogo obminu danymy na osnovi klitynnyh avtomativ, *Naukovyj visnyk Chernivets'kogo universytetu. Kompyuterni systemy i komponenty*, 2011, Vol. 2(1), pp. 15–20.