DOI 10.15276/imms.v12.no3.137
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 137-143

IMPROVEMENT OF THE PSEUDORANDOM KEY SEQUENCES GENERATION ALGORITHM BASED ON CELLULAR AUTOMATON AND MANY-VALUED LOGIC BENT-SEQUENCES

M.V.Khymenko, A.V.Sokolov

National Odesa Polytechnic University
Shevchenko Ave., 1 Odesa, 65044, Ukraine, radiosquid@gmail.com

One of the most important cryptographic structures, which is the basis of modern information protection systems, is cryptographically protected generators of pseudo-random key sequences, which are used in a wide variety of tasks, starting from the creation of initialization vectors, key information, and formation of the steganographic path, ending with their operation as the most important basic component of full-fledged stream cryptographic algorithms. Many of the available today algorithms of pseudo-random key sequences generators are characterized either by a quite complex software implementation structure or by insufficient cryptographic security, which makes urgent the task of developing effective cryptographically protected pseudo-random key sequences generators with a high level of stochastic quality. This paper proposes a scheme for an efficient pseudo-random key sequences generator based on a cellular automaton, as well as on such many-valued logic perfect algebraic constructions as IV-sets of quaternary bent-sequences with the maximum level of nonlinearity distance. The proposed generator is characterized by a significant complexity of the relationship between the output bits of the pseudo-random sequence and the elements of the short key on the basis of which they are generated, which determines the high level of its cryptographic security, while the number of protection levels of the proposed generator is easily scalable if necessary. Having only two binary linear feedback shift registers in the proposed scheme makes it adaptable to software implementation. The research performed made it possible to establish that the pseudo-random sequences generated by the proposed generator correspond to all stochastic tests from the NIST set, which makes it possible to recommend it for use in practice.

Keywords: pseudo-random key sequences generator, bent-sequence, cellular automaton.

Introduction and statement of the problem

The pseudo-random key sequences generator (PRKSG) is one of the most important cryptographic structures, which finds its numerous applications in modern information protection systems: starting from the generation of various initialization vectors, ending with full-fledged use as the main element of a stream ciphers, or in units for determining the steganographic path in steganographic algorithms. Such a considerable demand for PRKSG leads to significant attention of modern researchers to the problems of developing PRKSG, which is characterized by high cryptographic security, high stochastic quality of generated pseudo-random sequences, as well as significant performance.

Despite the fact that today there are many methods for estimating the stochastic quality of a PRKSG, the set of NIST [1] stochastic tests is generally accepted, so the compliance of PRKSG with these tests is an indicator of its high stochastic quality.

Today there are many schemes for PRKSG construction, among which a special place is occupied by PRKSG based on perfect algebraic constructions. Thus, the work [2] presents a scheme of the PRKSG based on linear feedback shift registers (LFSR) and dual pairs of bent-sequences, which is characterized by the correspondence with a set of stochastic tests [3], as well as a set of NIST stochastic tests, as it was proved in [4]. Nevertheless, despite the high cryptographic and stochastic quality of the PRKSG [3], it is not devoid of disadvantages related to the fact that the use of LFSR is not always desirable on modern devices during the software implementation of the PRKSG and may lead to a decrease in its overall performance. This circumstance led to the creation of a modification of this PRKSG [5], based on the application of cellular automaton [6], which allowed a significant increase in its performance, however, as shown in [4], it reduced the level of stochastic quality of generated pseudorandom sequences, which complicates its application in practice.

As the performed research shows, this shortcoming can be eliminated by using such many-valued logic perfect algebraic constructions as the quaternary bent-sequences, the definition of which was proposed in [7].

The *purpose* of this paper is to develop a high-speed, stochastically, and cryptographically high-quality PRKSG based on cellular automaton and IV-set of quaternary bent-sequences.

Quaternary bent-sequences

The basis for the development of the proposed modification of the generator of pseudorandom key sequences is bent-sequences of quaternary logic, which were first defined in [7], after which the research of their full class was performed in [8]. Let us introduce the basic definitions we need.

Definition 1 [9]. A mapping $\{0,1,2,3...,q-1\}^k \to \{0,1,2,3...,q-1\}$ is called a function of a q-valued logic (hereinafter referred to as a q-function).

The most common way of defining a q-function is the truth table. In addition to the way of representation of q-functions with help of the truth tables over the alphabet $\{0,1,...,q-1\}$, exponential truth tables presented above the alphabet $z_k = e^{j\frac{2\pi}{q}k}$, $k \in \{0,1,...,q-1\}$ are also considered.

In the case of 4-functions, the alphabet of the considered vectors will consist of the following values $\{0 \quad 1 \quad 2 \quad 3\} \to \{z_0 \quad z_1 \quad z_2 \quad z_3\} \to \{e^{j\frac{2\pi}{4}\cdot 0} \quad e^{j\frac{2\pi}{4}\cdot 1} \quad e^{j\frac{2\pi}{4}\cdot 2} \quad e^{j\frac{2\pi}{4}\cdot 3}\}$.

Definition 2 [9]. The coefficients of the Vilenkin-Chrestenson transform of a function of q-valued logic is the vector obtained by multiplying its truth table of length N by a complex conjugate of the Vilenkin-Chrestenson matrix

$$\Omega_A = A \cdot \overline{V}_N, \tag{1}$$

while in the quaternary case, the Vilenkin-Chrestenson matrix is constructed in accordance with the following recurrence rule

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \end{bmatrix}, \tag{2}$$

where "+" is the addition operation, matrices V are presented in symbolic form, i.e., the summation is performed relative to indices z_i.

Definition 3 [8]. For a Vilenkin-Chrestenson matrix of order $N = q^k$, where q is a prime, a bent-sequence is a sequence $H = [h_0, h_1, \cdots, h_i, \cdots, h_{N-1}]$ over the alphabet $h_i \in \{e^{j\frac{2\pi}{q}\text{v}}\}, \text{v} = 0,1,...,q-1$ if it has a uniform absolute values of the Vilenkin-Chrestenson spectrum, which can be represented in matrix form

$$\left|\Omega_B(\omega)\right| = \left|H \cdot \overline{V}_N\right| = const, \quad \omega = \overline{0, N-1}, \tag{3}$$

where V_N is the Vilenkin-Chrestenson matrix of order N over the alphabet $h_i \in \{e^{j\frac{2\pi}{q}v}\}, q = 0,1,...,q-1$.

Since bent-sequences are unbalanced by their construction, for their practical application in cryptographic issues, the concept of a q-set of bent-sequences is most often used, the definition of which is introduced in [8].

Definition 4 [8]. A set of q q-ary bent-sequences is called a q-set if the concatenation of its truth tables is balanced, i.e., $K^0 = K^1 = ... = K^{q-1}$.

In [8], it is shown that the complete set of quaternary bent-sequences of length $N = 16$ and cardinality $J = 200704$ can be classified into 4428 different IV-sets.

He proposed PRKSG scheme

In the proposed PRKSG scheme, two LFSR are used to form the initial state of the cellular automaton with the number of states of each cell $q = 4$. The size of the used cellular automaton is $n = 16$, while the radius of the neighborhood is chosen as equal to $r = 2$. The IV-set of quaternary bent-sequences is used as the evolution rule. After a given number of steps of evolution $t = 7$ is performed, the data in the register of the cellular automaton enters the pseudo-random bit generation block, which decides the value of the output pseudo-random bit. The scheme of operation of the proposed PRKSG is presented in Fig. 1.

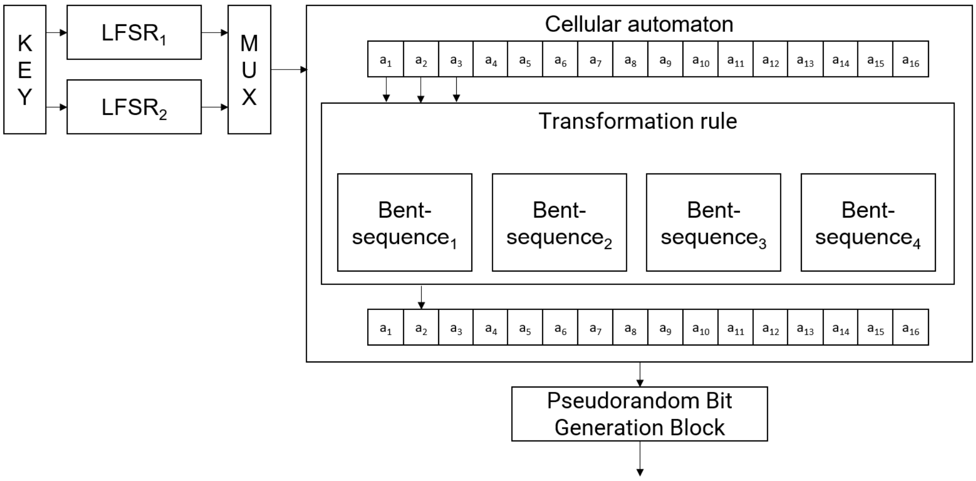
K
E
Y
LFSR$_1$
LFSR$_2$
M
U
X
Cellular automaton
a$_1$ a$_2$ a$_3$ a$_4$ a$_5$ a$_6$ a$_7$ a$_8$ a$_9$ a$_{10}$ a$_{11}$ a$_{12}$ a$_{13}$ a$_{14}$ a$_{15}$ a$_{16}$
Transformation rule
Bent-sequence$_1$
Bent-sequence$_2$
Bent-sequence$_3$
Bent-sequence$_4$
a$_1$ a$_2$ a$_3$ a$_4$ a$_5$ a$_6$ a$_7$ a$_8$ a$_9$ a$_{10}$ a$_{11}$ a$_{12}$ a$_{13}$ a$_{14}$ a$_{15}$ a$_{16}$
Pseudorandom Bit Generation Block

Fig. 1. Scheme of the proposed PRKSG

Let us explain in specific steps the algorithms of the proposed PRKSG, the scheme of which is shown in Fig. 1.

Initialization algorithm of the PRKSG

Step 1. Select 2 primitive irreducible polynomials $f_1(x)$ and $f_2(x)$, and to ensure the best stochastic and cryptographic properties of the PRKSG, the degrees of the selected polynomials must be mutually prime $\mathrm{GCD}(\deg\{f_1(x)\}, \deg\{f_2(x)\}) = 1$.

Step 2. Construct on the basis of selected primitive irreducible polynomials LFSR$_1$ and LFSR$_2$, the initial states of which are considered as the cryptographic key of the generator.

Step 3. In accordance with **Definition 4**, select the IV-set of quaternary bent-sequences, which are a nonlinear element of the generator.

Algorithm for generating a bit of a pseudo-random sequence

Step 1. Using LFSR1 and LFSR2, generate the next 16 bits of two pseudo-random sequences, which must then be multiplexed into 16 elements of the quaternary sequence $\left[a_1\; a_2\; a_3\; a_4\; a_5\; a_6\; a_7\; a_8\; a_9\; a_{10}\; a_{11}\; a_{12}\; a_{13}\; a_{14}\; a_{15}\; a_{15}\right]$ — the initial state of the cellular automaton.

Step 2. The evolution rule is applied $t = 7$ times to each element of the cellular automaton sequence. For each element of the sequence $a_i, i = 1,2,...,16$, a triplet of elements $\{a_{(i-1)\bmod 16}, a_i, a_{(i+1)\bmod 16}\}$ is considered, where the element $a_{(i+1)\bmod 16}$ determines the index of the quaternary bent-sequence in the IV-set, while the elements $a_{(i-1)\bmod 16}, a_i$ determine the index of the element of the selected quaternary bent-sequence, the value of which will be used in the next step of evolution.

Step 3. After $t = 7$ steps of the evolution iterations of the cellular automaton, the j-th bit of the pseudorandom sequence is calculated as

$$g_j = \left(\sum_{h=1}^{16} a_h\right) \bmod 2. \tag{4}$$

The results of testing

The results of testing of the proposed PRKSG are given for the following initial data. The following primitive irreducible polynomials are used to construct LFSR1 and LFSR2

$$\left[\begin{array}{l} f_1(x) = x^{83} + x^{46} + x^{45} + x + 1; \\ f_2(x) = x^{31} + x^{21} + x^{12} + x^3 + x^2 + x + 1, \end{array}\right. \tag{5}$$

while the following initial states are selected

$$\left[\begin{array}{l} \alpha_1 = \{11111111111101011111110111111111111111111111 \\ \qquad\qquad\qquad 111111111110011111010110111010010110100\}; \\ \alpha_2 = \{1001101011111001001110001011000\}. \end{array}\right. \tag{6}$$

Thus, with other non-secret parameters, the value of protection levels number of the PRKSG will be equal to $\Psi = 2^{83}2^{31} = 2^{114}$, which is considered as sufficient. It is obvious that the value of protection levels number can be easily scaled, if necessary, by choosing primitive irreducible polynomials for LFSR1 and LFSR2 of the necessary degree.

The following set is selected as the IV-set of quaternary bent-sequences

$$\begin{array}{ll} H_1 = \{0331132333230113\}; & H_3 = \{3220301121111013\}; \\ H_2 = \{3222302222103101\}; & H_4 = \{3221020030012000\}. \end{array} \tag{7}$$

For the purposes of experimental research of the stochastic properties of the proposed PRKSG, the 5 000 000 bits of pseudorandom sequence were generated based on the initial data (5), (6), and (7), which were presented in the form of an image shown in Fig. 2.

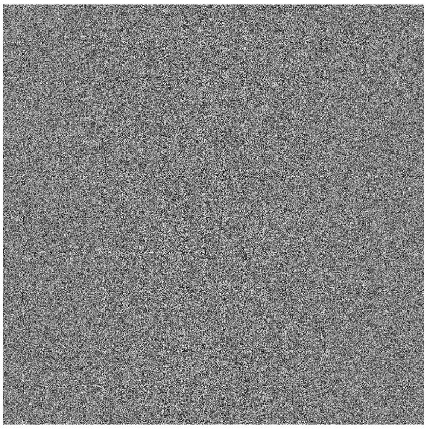

Fig. 2. Graphical representation of a pseudo-random sequence generated by the developed PRKSG

In the Table 1, we present the results of the research of compliance of the developed PRKSG with NIST test set [1].

Table 1

The results of testing the developed PRKSG by the set of NIST tests set

No.	Test	P-value	Pass rate
1	Monobit test	0.8279	✓
2	Frequency within block test	0.9050	✓
3	Runs test	0.6788	✓
4	Longest run ones in a block test	0.3916	✓
5	Binary matrix rank test	0.9980	✓
6	DFT test	0.4676	✓
7	Non overlapping template matching test	1	✓
8	Overlapping template matching test	0.2565	✓
9	Maurers universal test	0.1880	✓
10	Linear complexity test	0.3440	✓
11	Serial test	0.0490	✓
12	Approximate entropy test	0.1002	✓
13	Cumulative sums test	0.4000	✓
14	Random excursion test	0.3192	✓
15	Random excursion variant test	0.2170	✓

Analysis of the data presented in Table 1 allows us to draw a conclusion about the full compliance of the sequences generated by the developed PRKSG with the set of NIST tests, which confirms its high effectiveness. We also note that the high degree of complexity of the relationship between key elements and the generated gamma allows us to draw a conclusion about the high level of cryptographic strength of the developed generator. Thus, the developed generator can be recommended for use in practical applications.

Conclusions

Let us note the main results of the performed research:

1. The scheme of an effective PRKSG based on a cellular automaton and IV-set of quaternary bent-sequences, including two LFSR, is proposed. The proposed scheme is characterized by the simplicity of software implementation, as well as a high level of cryptographic strength in terms of the complexity of the relationship between the elements of the short key and the generated bits of the output sequence. The value of protection levels number of the developed generator is easily scalable and in the considered example is equal to $\Psi = 2^{114}$, which is sufficient.

2. Performed research of the proposed PRKSG showed its full compliance with all stochastic quality tests of the NIST set, which is a confirmation of the high effectiveness of the developed generator and allows us to recommend its use in practical applications.

References

1. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg, MD : U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2000. 153 p.
2. Mazurkov M. I., Sokolov A. V., Barabanov N.A. The key sequences generator based on bent functions dual couples. *Proceedings of Odesa Polytechnic University*. 2013. No. 3. P. 150-156.
3. Ivanov M. A., Chugunkov I. V. Theory, application and evaluation of the quality of generators of pseudo-random sequences. Moscow: KUDITS-OBRAZ, 2003. 240 p.
4. Sokolov A.V., Khimenko M.V. Testing key sequence generators based on perfect algebraic constructions. *Science and social life of Ukraine in the era of global challenges for humanity in the digital era. International scientific-practical conference on the occasion of the 30th anniversary of the declaration of independence of Ukraine and the 25th anniversary of the adoption of the Constitution of Ukraine.* Odesa: Helvetyka Publishing House, 2021. Vol. 1, P. 610-613.
5. Sokolov A.V. The cellular automata key sequences generator. *Proceedings of the ONPU*, 2014. No. 1(43). P. 180-186.
6. Szaban M., Seredynski F. Cryptographically Strong S-Boxes Based on Cellular Automata. *Lecture Notes in Computer Science*. 2008. Vol. 5191. P. 478-485.
7. Schmidt K. Quaternary Constant-Amplitude Codes for Multicode CDMA. *IEEE International Symposium on Information Theory*. Nice. 2007. P. 2781-2785.
8. Sokolov A.V. Properties of the full class of quaternary bent-functions of two variables. *Journal of Discrete Mathematical Sciences and Cryptography*. 2022. Vol. 25, No. 8. P. 2569-2582.
9. Sokolov A.V., Zhdanov O.N. Cryptographic constructions based on many-valued logic functions. Monograph. Scientific thought, 2020. 192 p.

УДОСКОНАЛЕННЯ АЛГОРИТМУ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ КЛЮЧОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ КЛІТИННОГО АВТОМАТУ І БЕНТ-ПОСЛІДОВНОСТЕЙ БАГАТОЗНАЧНОЇ ЛОГІКИ

М.В. Хименко, А.В. Соколов

Національний університет «Одеська політехніка»
Україна, Одеса, 65044, пр-т Шевченка, 1, radiosquid@gmail.com

Одним із найважливіших криптографічних конструктів, що лежить в основі сучасних систем захисту інформації, є криптографічно захищені генератори псевдовипадкових ключових послідовностей, які застосовуються у найрізноманітніших задачах, починаючи від створення векторів ініціалізації, ключової інформації та формування стеганошляху, закінчуючи їх роботою у складі повноцінних потокових криптографічних алгоритмів, для яких вони складають найважливіший компонент. Наявні на сьогоднішній день генератори псевдовипадкових ключових послідовностей характеризуються або досить складною для програмної реалізації структурою, або недостатньою криптографічною захищеністю, що робить актуальною задачу розробки ефективних криптографічно захищених генераторів псевдовипадкових ключових послідовностей, що володіють високим рівнем стохастичної якості. У даній статті запропоновано схему ефективного генератора псевдовипадкових ключових послідовностей на основі клітинного автомату, а також таких досконалих алгебраїчних конструкцій багатозначної логіки, як IV-набори четвіркових бент-послідовностей, що володіють максимальним рівнем дистанційної нелінійності. Запропонований генератор характеризується значною складністю взаємозв'язку вихідних бітів псевдовипадкової послідовності та елементів короткого ключа, на основі якого вони генеруються, що обумовлює високий рівень його криптографічної стійкості, при цьому число рівнів захисту запропонованого генератора є легко масштабованим в разі необхідності. Наявність у запропонованій схемі лише двох двійкових регістрів зсуву з лінійним зворотним зв'язком робить її адаптованою до програмної реалізації. Проведені дослідження дозволили встановити, що генеровані запропонованим генератором псевдовипадкові послідовності відповідають всім стохастичним тестам з набору NIST, що дозволяє рекомендувати його для використання на практиці.

Ключові слова: генератор псевдовипадкових ключових послідовностей, бент-послідовність, клітинний автомат.