Oleg FINKO, Dmitriy SAMOYLENKO, Sergey DICHENKO, Nikolay ELISEEV

Institute of Computer Systems and Information Security of Kuban State Technological University, Krasnodar

doi:doi:10.15199/48.2015.03.06

Parallel generator of *q*-valued pseudorandom sequences based on arithmetic polynomials

Abstract. *A new method for parallel generation of q-valued pseudorandom sequence based on the presentation of systems generating logical formulae by means of arithmetic polynomials is proposed. Fragment consisting of k-elements of q-valued pseudorandom sequence may be obtained by means of single computing of a single recursion numerical formula. It is mentioned that the method of the "arithmetization" of generation may be used and further developed in order to protect the encryption gears from cryptographic onset, resulting in the initiating of mass hardware failures.*

Streszczenie. *Zaproponowano metodę równoległej generacji q-wartościowych sekwencji pseudolosowych na podstawie przedstawienia generujących układów rekurencyjnych wzorów logicznych za pomocą wielomianów liczbowych. Fragment zawierający k elementów q-wartościowych sekwencji pseudolosowej można uzyskać za pomocą jednokrotnego obliczania jednego ze wzorów numerycznych. Zwrócono uwagę na to, że proponowana metoda "arytmetyzacji" generowania takich sekwencji może w przyszłości być rozpowszechniona na przypadek zabezpieczenia urządzeń kryptograficznych przed kryptoanalitycznymi atakami, polegającymi na wywoływaniu masowych zaburzeń funkcjonowania osprzętu.* ***(Równoległy generator q-wartościowych sekwencji pseudolosowych wykorzystujący wielomiany arytmetyczne)***

Keywords: cryptographic protection of information, pseudo-random sequences, residue number system, modular arithmetic
Słowa kluczowe: kryptograficzna ochrona informacji, sekwencje pseudolosowe, system resztkowy, arytmetyka modularna

Introduction

Many specialists connect the further development of information protection facilities with the application of multiple-valued function of logical algebra (MVFLA), in particular, with the use of pseudorandom sequences (PRS) over GF(q) ($q > 2$), which possess a wider scope of unique features, if compared with binary PRS. The most effective and approved way of obtaining PRS is the use of special switching networks called linear feedback recurrent shift register (LFSR) [1–3].

General information

Construction of LFSR over GF(q) (hereinafter q-LFSR) is carried out by means of given characteristic polynomial:

$$P(z) = z^r \oplus p_{r-1}z^{r-1} \oplus p_{r-2}z^{r-2} \oplus \ldots \oplus p_0 \pmod q,$$

where $P(z) \in$ GF(q), and r is $P(z)$ polynomial order, $r \in N$, and to the constructed according to it recurrent equation:

$$s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \oplus p_0 s_n \pmod q, \tag{1}$$

$n = 0, 1, 2, \ldots$; where $p_j \in$ GF(q), $0 \le j \le r-1$; $\oplus$ – is the symbol of addition according to $\mod q$.

In general case q-LFSR consists of D_j ($j = 0, 1, \ldots, r-1$) cells and has the following initial fill: $s_0, s_1, \ldots, s_{r-1}$. Here the "cell" is the $\lceil \log_2 q \rceil$ parallel stage register ($\lceil x \rceil$ being the least integral number equal or more than x). After the first cycle q-LFSR has the following fill: $s_1, s_2, \ldots, s_r$. In general q-LFSR generates infinite q-valued PRS: $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ [2].

In notation of linear algebra the next q-valued element of PRS s_{n+r} is represented as a product:

$$\begin{Vmatrix} s_{n+r} \\ s_{n+r-1} \\ \cdots\cdots \\ s_{n+2} \\ s_{n+1} \end{Vmatrix}^\top = \begin{Vmatrix} s_{n+r-1} \\ s_{n+r-2} \\ \cdots\cdots \\ s_{n+1} \\ s_n \end{Vmatrix}^\top \cdot \begin{Vmatrix} p_{r-1} & 1 & 0 & \ldots & 0 \\ p_{r-2} & 0 & 1 & \ldots & 0 \\ & & \cdots\cdots\cdots & & \\ p_1 & 0 & 0 & \ldots & 1 \\ p_0 & 0 & 0 & \ldots & 0 \end{Vmatrix}.$$

In the Fig. 1 Structural diagram of the sequential q-LFSR functioning is shown.

As we know, PRS over GF(q) has a range of "useful" structural properties, including [2, 3]:

- number of symbols at the period of PRS or PRS period is defined as $L = q^r - 1$;
- number of similar nonzero symbols in the PRS period is equal to q^{r-1}, and the number of zero symbols is equal to $q^{r-1} - 1$;
- addition of elements in a PRS with elements of the same PRS shifted numbering (except number equal periud repetition) gives a similar PRS shifted numbering;
- autocorrelation function of PRS is defined by means of the ratio $p(0) = 1, p(i) = -\frac{1}{q^r - 1}, 1 \le i \le q^r - 2$, etc.

Method of parallel generation of q-valued PRS

In the most of practically important cases, besides the "useful" structural quantities, every complex system should be aimed at the achievement of some limiting characteristic or some quality indicator, what can be obtained by means of the minimization of the quantity of operations, using of resources or parallelization of computational processes of the system [4]. So, the paper [5] shows the algorithm of parallelization of generation of binary PRS based on the presentation of systems generating recurrent logical formulae by means of arithmetic polynomials. At the same time the development of computing machinery and software requires the invention of the new approaches to firmware realization both of binary functions and ($q > 2$)-valued functions of logical algebra [6, 7, 8].

Let $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ – be the PRS elements, satisfying the recurrent equation (1). Because any element s_n ($n \ge r$) of the sequence $s_0, s_1, s_2, \ldots, s_{r-1}, \ldots$ are calculated recursively on the basis of known r elements, let us represent the elements of PRS section $s_{n+r}, s_{n+r+1}, \ldots, s_{n+2r-1}$ with the length r as the system of characteristic equations:

$$\begin{cases} s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ldots \\ \ldots \oplus p_0 s_n \pmod q, \\ s_{n+r+1} = p_{r-1}s_{n+r} \oplus p_{r-2}s_{n+r-1} \oplus \ldots \\ \ldots \oplus p_0 s_{n+1} \pmod q, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{n+2r-1} = p_{r-1}s_{n+2r-2} \oplus p_{r-2}s_{n+2r-3} \oplus \ldots \\ \ldots \oplus p_0 s_{n+r-1} \pmod q, \end{cases} \tag{2}$$

where $[s_{n+r}\ s_{n+r+1}\ \ldots\ s_{n+2r-1}]$ — is the vector of PRS r-condition (or inner condition of q-LFSR on the r-cycle).

By the analogy with [5], let us express the right parts of

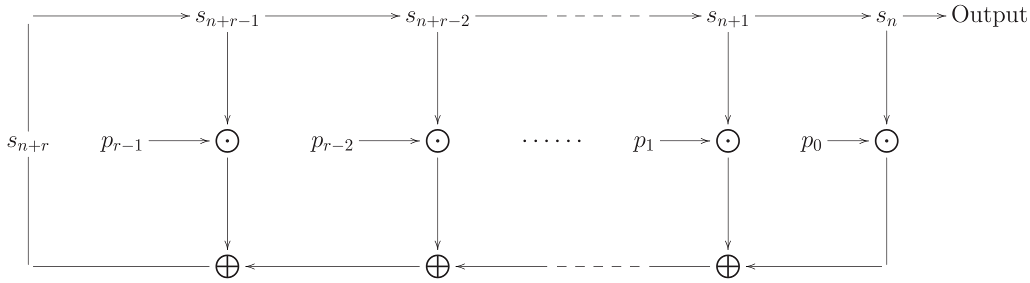

Fig. 1. Structural diagram of the operation of the sequential q-LFSR in accordance with formula (1) ($\oplus$ and $\odot$ — according to transaction of addition and multiplication of the $\mod q$)

the system (2) through the given initial condition:

(3)
$$\begin{cases} s_{n+r} = p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ \dots \\ \dots \oplus p_0 s_n \quad (\mathrm{mod}\ q), \\ s_{n+r+1} = p_{r-1}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ \dots \\ \dots \oplus p_0 s_n) \oplus p_{r-2}s_{n+r-1} \oplus \ \dots \oplus p_0 s_{n+1} \quad (\mathrm{mod}\ q), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ s_{n+2r-1} = p_{r-1}(p_{r-1}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ \dots \\ \dots \oplus p_0 s_n) \oplus p_{r-2}s_{n+r-1} \oplus \ \dots \ \oplus p_0 s_{n+1}) \oplus \\ \oplus p_{r-2}(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ \dots \oplus p_0 s_n) \oplus \ \dots \\ \dots \oplus p_0(p_{r-1}s_{n+r-1} \oplus p_{r-2}s_{n+r-2} \oplus \ \dots \\ \dots \ \oplus p_0 s_n) \quad (\mathrm{mod}\ q). \end{cases}$$

Let represent the system (3) as the system r MVFLA or of r-variables:

(4)
$$\begin{cases} f_1(s_{n+r-1}, \dots, s_n) = \\ p^{(0)}_{r-1}s_{n+r-1} \oplus p^{(0)}_{r-2}s_{n+r-2} \oplus \dots \oplus p^{(0)}_0 s_n \quad (\mathrm{mod}\ q), \\ f_2(s_{n+r-1}, \dots, s_n) = \\ p^{(1)}_{r-1}s_{n+r-1} \oplus p^{(1)}_{r-2}s_{n+r-2} \oplus \dots \oplus p^{(1)}_0 s_n \quad (\mathrm{mod}\ q), \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f_r(s_{n+r-1}, \dots, s_n) = \\ p^{(r-1)}_{r-1}s_{n+r-1} \oplus p^{(r-1)}_{r-2}s_{n+r-2} \oplus \dots \\ \dots \oplus p^{(r-1)}_0 s_n \quad (\mathrm{mod}\ q). \end{cases}$$

Coefficients $p^{(j)}_i \in \{0, 1, \dots, q-1\}$ are formed after reduction formulas (3). Structural diagram of the parallel operation of the generator in accordance with formula (4) has the form (see Fig. 2).

We know that the arbitrary MVFLA may be represented as arithmetical polynomial defines as [7, 8, 9]:

(5)
$$A(S) = \sum_{i=0}^{q^{r-1}-1} a_i \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}},$$

where a_i is the i-ratio of arithmetical polynomial; $S = s_n, s_{n+1}, \dots, s_{n+r-1}$ are the arguments of MVFLA $s_u \in 0, 1, \dots, q-1$ $(u = 0, 1, \dots, r-1)$; $(i_0\ i_1\ \dots\ i_{r-1})_q$ is the representation of the i parameter in the q-ary notation system:

$$(i_0\ i_1\ \dots\ i_{r-1})_q = \sum_{u=0}^{r-1} i_u q^{r-u-1} \quad (i_u \in 0, 1, \dots, q-1);$$

$$s_u^{i_u} = \begin{cases} 1, & i_u = 0, \\ s_u, & i_u \neq 0. \end{cases}$$

By analogy with [8] we may realize the MVFLA system (4) by calculation of some arithmetical polynomial.

To do that, let us coordinate MVFLA (4) system with the system of arithmetical polynomials (5). Then we get:

(6)
$$\begin{cases} A_1(S) = \sum_{i=0}^{q^{r-1}-1} a_{1,i} \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}}, \\ A_2(S) = \sum_{i=0}^{q^{r-1}-1} a_{2,i} \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ A_r(S) = \sum_{i=0}^{q^{r-1}-1} a_{r,i} \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}}. \end{cases}$$

Let multiple the polynomials of the system (6) by weights q^{l-1} $(l = 1, 2, \dots, r)$:

$$\begin{cases} A_1^*(S) = q^0 P_1(S) = \sum_{i=0}^{q^{r-1}-1} a^*_{1,i} \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}}, \\ A_2^*(S) = q^1 P_2(S) = \sum_{i=0}^{q^{r-1}-1} a^*_{2,i} \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ A_r^*(S) = q^{r-1} P_r(S) \sum_{i=0}^{q^{r-1}-1} a^*_{r,i} \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}}, \end{cases}$$

where $a^*_{l,\,i} = q^{l-1} a_{l,\,i}$ $(l = 1, 2, \dots, r; i = 0, 1, \dots, q^r - 1)$.

Then we get:

$$D(S) = \sum_{i=0}^{q^{r-1}-1} \sum_{l=1}^{d} a^*_{l,i} \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}}.$$

According to paper [8] the modular form of an arithmetical polynomials can be received:

(7)
$$\boxed{M(S) = \bigoplus_{i=0}^{q^{r-1}-1} c_i \, s_n^{i_0} s_{n+1}^{i_1} \ \dots \ s_{n+r-1}^{i_{r-1}} \quad (\mathrm{mod}\ q^r),}$$

where

$$c_i = \bigoplus_{l=1}^{r} a^*_{l,\,i} \ \ (i = 0, 1, \dots, q^{r-1} - 1).$$

Let computing the values of the required MVFLA. To do that, we should represent the result of calculation of MVFLA in q-valued notation system and apply the masking operator $\Xi^t\{M(S)\}$ [9]:

$$\Xi^t\{M(S)\} = \left\lfloor \frac{M(S)}{q^t} \right\rfloor \quad (\mathrm{mod}\ q),$$

where t is the required q-stage of the representation $M(S)$. Structural diagram of the parallel operation of the generator in accordance with formula (7) has the form (see Fig. 3).

Numerical example

Let examine the construction $q = 3$ LFSR, generating 3-digit PRS given by characteristic equation: $s_{k+3} = 2s_{k+2} \oplus s_k \ (\mathrm{mod}\ 3)$ and initial fill: $s_0 = 0,\ s_1 = 1,\ s_2 = 2.$

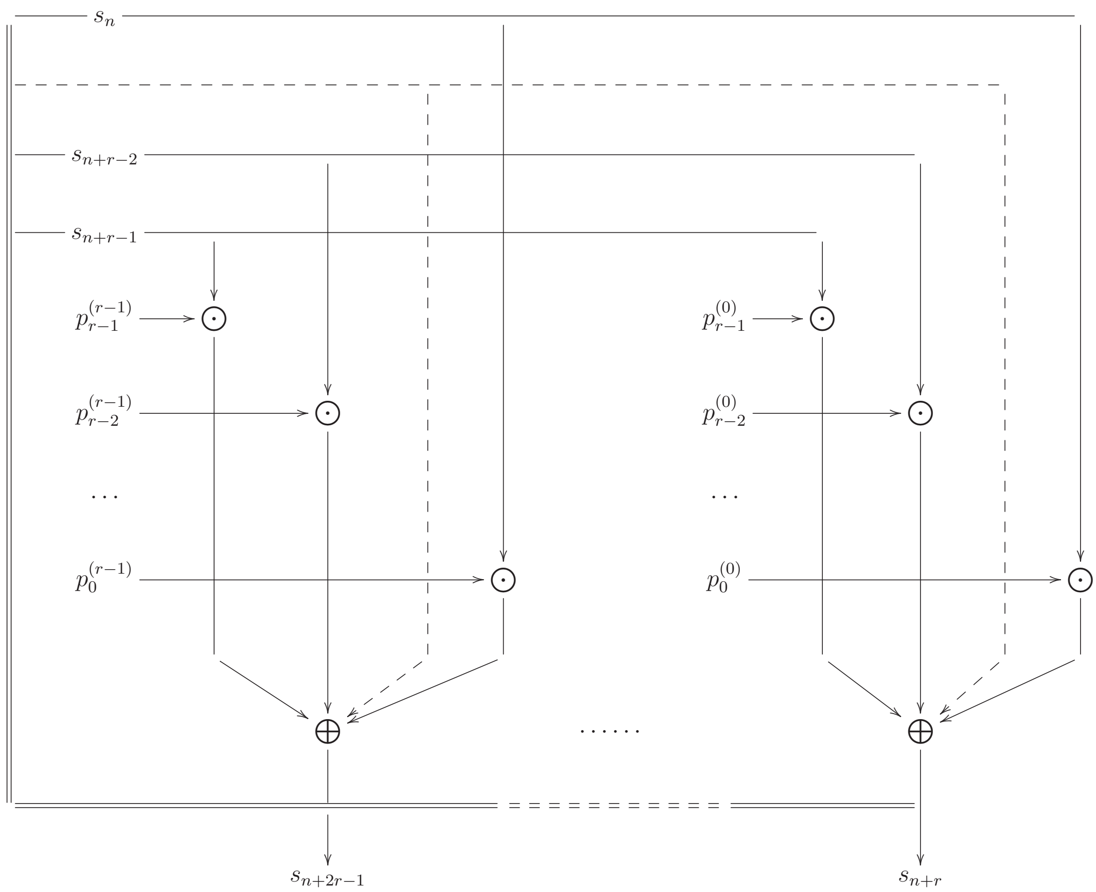

Fig. 2. Structural diagram of the operation of the parallel q-LFSR in accordance with the formula (4)

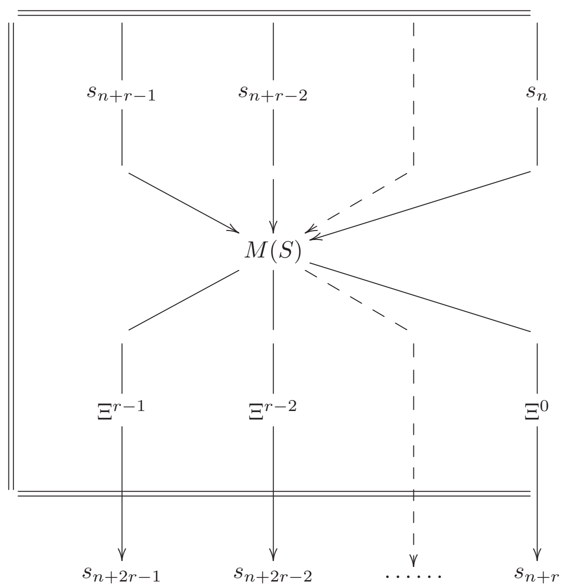

Fig. 3. Structural diagram of the operation of the parallel q-LFSR in accordance with the arithmetic polynomials (7)

The corresponding characteristic polynomial is represented as: $P(z) = z^3 + 2z^2 + 1$.

In this case the system of characteristic equations for the PRS section of three elements will be represented as follows:

$$\begin{cases} s_3 = 2s_2 \oplus s_0 \pmod 3, \\ s_4 = 2s_3 \oplus s_1 \pmod 3, \\ s_5 = 2s_4 \oplus s_2 \pmod 3. \end{cases}$$

Then let us represent the system of characteristic equations as the MVFLA system with right part of equalities, expressed by means of initial given conditions:

$$\begin{cases} f_3(s_2, s_1, s_0) = 2s_2 \oplus s_0 \pmod 3, \\ f_4(s_2, s_1, s_0) = s_2 \oplus s_1 \oplus 2s_0 \pmod 3, \\ f_5(s_2, s_1, s_0) = s_0 \oplus 2s_1 \pmod 3. \end{cases}$$

According to (6) we shall get the system of arithmetical polynomials as follows:

$$\begin{cases} A_3(S) = \frac{1}{4}(14s_2 - 6s_2^2 + 4s_0 - 39s_2s_0 + 21s_0s_2^2 + \\ +15s_0^2s_2 - 9s_0^2s_2^2), \\ A_4(S) = \frac{1}{8}(8s_2 + 8s_1 + 42s_1s_2 - 30s_1s_2^2 - 30s_2s_1^2 + \\ +18s_1^2s_2^2 + 28s_0 - 78s_0s_2 + 30s_0s_2^2 - 78s_0s_1 + \\ +78s_0s_1s_2 + 30s_0s_1^2 - 18s_0s_1^2s_2^2 - 12s_0^2 + \\ +42s_0^2s_2 - 18s_0^2s_2^2 + 42s_0^2s_1 - 72s_0^2s_1s_2 + \\ +18s_0^2s_1s_2^2 - 18s_0^2s_1^2 + 18s_0^2s_2s_1^2), \\ A_5(S) = \frac{1}{4}(14s_1 - 6s_1^2 + 4s_0 - 39s_1s_0 + 21s_0s_1^2 + \\ +15s_0^2s_1 - 9s_0^2s_1^2). \end{cases}$$

Let realize the system of arithmetical expressions as arithmetical polynomial:

$$\begin{cases} D(S) = \\ \frac{1}{4}\left(14s_2 - 6s_2^2 + 4s_0 - 39s_2s_0 + 21s_0s_2^2 + 15s_0^2s_2 - \right. \\ \left. -9s_0^2s_2^2\right) + 3^1\left(\frac{1}{8}(8s_2 + 8s_1 + 42s_1s_2 - 30s_1s_2^2 - \right. \\ -30s_2s_1^2 + 18s_1^2s_2^2 + 28s_0 - 78s_0s_2 + 30s_0s_2^2 - \\ -78s_0s_1 + 78s_0s_1s_2 + 30s_0s_1^2 - 18s_0s_1^2s_2^2 - \\ -12s_0^2 + 42s_0^2s_2 - 18s_0^2s_2^2 + 42s_0^2s_1 - 72s_0^2s_1s_2 + \\ \left. +18s_0^2s_1s_2^2 - 18s_0^2s_1^2 + 18s_0^2s_2s_1^2)\right) + 3^2\left(\frac{1}{4}(14s_1 - \right. \\ \left. -6s_1^2 + 4s_0 - 39s_1s_0 + 21s_0s_1^2 + 15s_0^2s_1 - 9s_0^2s_1^2)\right). \end{cases}$$

Modular polynomial form will be expressed as:

$$M(S) = $$
$$7s_0 \oplus 9s_0^2 \oplus 21s_1 \oplus 18s_0s_1 \oplus 9s_0^2s_1 \oplus 18s_0s_1^2 \oplus$$
$$\oplus 20s_2 \oplus 15s_0s_2 \oplus 6s_0^2s_2 \oplus 9s_1s_2 \oplus 9s_0s_1s_2 \oplus$$
$$\oplus 9s_1^2s_2 \oplus 12s_2^2 \oplus 3s_0s_2^2 \oplus 18s_0^2s_2^2 \oplus 9s_1s_2^2 \pmod{27}.$$

According to the given initial conditions we may obtain the following three-digit fragment of PRS:

$$\text{step } 1 \begin{cases} s_3 = \Xi^0\{19\} = 1, \\ s_4 = \Xi^1\{19\} = 0, \\ s_5 = \Xi^2\{19\} = 2; \end{cases} \quad \text{step } 5 \begin{cases} s_{15} = \Xi^0\{5\} = 2, \\ s_{16} = \Xi^1\{5\} = 1, \\ s_{17} = \Xi^2\{5\} = 0; \end{cases}$$

$$\text{step } 2 \begin{cases} s_3 = \Xi^0\{14\} = 2, \\ s_4 = \Xi^1\{14\} = 1, \\ s_5 = \Xi^2\{14\} = 1; \end{cases} \quad \text{step } 6 \begin{cases} s_3 = \Xi^0\{17\} = 2, \\ s_4 = \Xi^1\{17\} = 2, \\ s_5 = \Xi^2\{17\} = 1; \end{cases}$$

$$\text{step } 3 \begin{cases} s_3 = \Xi^0\{10\} = 1, \\ s_4 = \Xi^1\{10\} = 0, \\ s_5 = \Xi^2\{10\} = 1; \end{cases} \quad \text{step } 7 \begin{cases} s_3 = \Xi^0\{4\} = 1, \\ s_4 = \Xi^1\{4\} = 1, \\ s_5 = \Xi^2\{4\} = 0; \end{cases}$$

$$\text{step } 4 \begin{cases} s_3 = \Xi^0\{9\} = 0, \\ s_4 = \Xi^1\{9\} = 0, \\ s_5 = \Xi^2\{9\} = 1; \end{cases} \quad \text{step } 8 \begin{cases} s_3 = \Xi^0\{19\} = 1, \\ s_4 = \Xi^1\{19\} = 0, \\ s_5 = \Xi^2\{19\} = 0; \end{cases}$$

. . . .

Conclusion

Here is the representation of one of the possible non-standard methods of realization of parallel algorithm of generation of q-valued PRS, based on the arithmetical representation of MVFLA. The developed algorithm may be used for the realization of perspective high-performance cryptographic facilities for information protection.

The further direction of the research is the realization of the developed algorithm of generation of q-valued PRS using the redundant code redundant number system, which provide control over the errors while computing the PRS elements.

REFERENCES

[1] Ferguson N., Schneier B. Practical cryptography, *John Wiley* & Sons, 2003.

[2] Lidl R., Niederreiter H. Introduction to finite fields and their applications, *Cambridge: Cambridge Univ. Press*, 1987.

[3] MacWilliams F., Sloane N. Pseudo-random sequences and arrays, *Proc. IEEE*, 64, pp. 1715–1729, 1976.

[4] Malyugin V. D. Representation of boolean functions as arithmetic polynomials, *Automation and Remote Control*, 43(4), pp. 496–504, 1982.

[5] Dichenko S. A., Eliseev N. I., Finko O. A. Control over the functional errors of generators of binary PRS, realized on arithmetical polynomials, *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunication and Control Systems*, 176(4), pp. 142–149, 2013.

[6] Faradzhev R. G. Linear sequential machines, *Moscow: Soviet radio*, 1975.

[7] Strazdins I. J., The Polynomial Algebra of Multivalued Logic, *Algebra, Combinatorics and Logic in Computer Science.* 42. pp. 777-785. 1986.

[8] Aslanova N. H., Faradzhev R. G. Arithmetic representation of functions of many-valued logic and parallel algorithm for finding such a representation, *Automation and Remote Control*, 53(2), pp. 251–261, 1992.

[9] Finko O. A. Modular forms of system of k-valued functions of the algebra of logic, *Automation and Remote Control*, 66(7), pp. 1081–1100, 2005.

Authors: *prof. PhD, D.Sc. Oleg Finko; Ph.D. Dmitriy Samoylenko; PhD. Sergey Dichenko; PhD. Nikolay Eliseev, Institute of Computer Systems and Information Security of Kuban State Technological University, 350072, Krasnodar, Moskovskaya St., 2, Russia, email: ofinko@yandex.ru; ofinko@member.ams.org; Personal page: http://www.mathnet.ru/eng/person/40004*