Secure Generators of q-valued Pseudo-Random Sequences on Arithmetic Polynomials

Oleg Finko[1], Sergey Dichenko[1], and Dmitry Samoylenko[2]

[1] Institute of Computer Systems and Information Security of Kuban State
Technological University, Krasnodar, Moskovskaya St., 2, 350072, Russia
ofinko@yandex.ru
[2] Mozhaiskii Military Space Academy, St. Petersburg,
Zhdanovskaya St., 13, 197198, Russia
19sam@mail.ru

Abstract. A technique for controlling errors in the functioning of nodes for the formation of q-valued pseudo-random sequences (PRS) operating under both random errors and errors generated through intentional attack by an attacker is provided, in which systems of characteristic equations are realized by arithmetic polynomials that allow the calculation process to be parallelized and, in turn, allow the use of redundant modular codes device.

Keywords: q-valued pseudo-random sequences · Secure generators of q-valued pseudo-random sequences · Primitive polynomials · Galois fields · Linear recurrent shift registers · Modular arithmetic · Parallel logical calculations by arithmetic polynomials · Error control of operation · Redundant modular codes

1 Introduction

In the theory and practice of cryptographic information protection, one of the key tasks is the formation of PRS which width, length and characteristics meet modern requirements [1]. Many existing solutions in this area aim to obtain a binary PRS of maximum memory length with acceptable statistical characteristics [2]. However, recently it is considered that one of the further directions in the development of means of information security (MIS) is the use of multi-valued functions of the algebra of logic (MFAL), in particular, using the PRS over the Galois field GF(q) ($q > 2$), which have a wider spectrum of unique properties comparing to binary PRS [3].

The nodes of the formation of the q-valued PRS, like the others, are prone to failures and malfunction, which leads to the occurrence of errors in their functioning. In addition to random errors occurrence in the generation of PRS related to “unintentional” failures and malfunctions caused by various causes: aging of the element base, environmental influences, severe operating conditions, etc. (reasons typical for reliability theory), there are deliberate actions of an attacker aimed to create massive failures of electronic components of the formation nodes of PRS due to the hardware errors generation (one of the types of information security threats) [4].

Many methods have been developed to provide the necessary level of reliability of the digital devices functioning; the most common are backup methods and methods of noise-immune coding. However, backup methods do not provide the necessary levels of operation reliability with limitations on hardware costs, and methods of noise-immune coding are not fully adapted to the specifics of the construction and operation of MIS, in particular, generators of q-valued PRS.

The work [5] offers a solution that overcomes the complexity of using code control for the nodes of the binary PRS generation, based on the “arithmetic” of logical count and the application of the redundant modular code device, which provides the necessary level of security for their functioning. However, the solution obtained is limited to exclusive applicability in the formation of binary PRS. At the same time, work [6], is known where by means of “arithmetic” of logical count the task of parallelizing the nodes of forming of binary PRS is solved, but without monitoring their functioning. As a result, it becomes necessary to generalize the solutions obtained to ensure the security of the functioning of the nodes of q-valued PRS formation.

2 General Principles of Building Generators of *q*-valued PRS

The most common and tested methods for PRS are algorithms and devices of PRS generation — linear recurrent shift registers (q-LFSR) with feedback — based on the use of recurrent logical expressions [2].

The construction of the q-LFSR over the field GF(q) is carried out from the given generating polynomial:

$$K(x) = \sum_{i=0}^{m} k_{m-i} x^{m-i}, \tag{1}$$

where m — is the polynomial degree $K(x)$, $m \in N$; $k_i \in GF(q)$, $k_m = 1$, $k_0 \neq 0$.

Thus, the q-LFSR element is formed in accordance with the following characteristic equation [7]:

$$a_{p+m} = -k_{m-1}a_{p+m-1} - k_{m-2}a_{p+m-2} - \ldots - k_1 a_{p+1} - k_0 a_p. \tag{2}$$

The Eq. (2) is a recursion which describes an infinite q-valued PRS with period $q^m - 1$ (with nonzero initial state, as well as under condition that the polynomial (1) is primitive over the field GF(q)), each nonzero state appears once per period.

A homogeneous recurrent Eq. (2) can be presented in the following form:

$$a_{p+m} = k_{m-1}a_{p+m-1} \oplus k_{m-2}a_{p+m-2} \oplus \ldots \oplus k_1 a_{p+1} \oplus k_0 a_p$$

or

$$a_{p+m} = \bigoplus_{i=1}^{m} k_{i-1} a_{p+i-1}, \tag{3}$$

where $\oplus$ — is the symbol of addition on module q.

The q-LFSR corresponding to the polynomial (3) is shown in Fig. 1, whose cells contain field GF(q) elements: a_p, …, a_{p+m-1}.

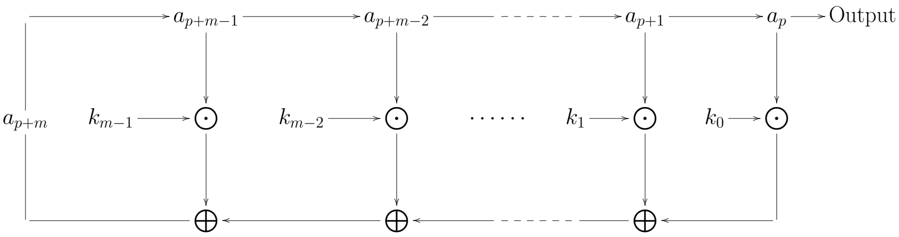

Fig. 1. Structural diagram of the operation of the sequential q-LFSR in accordance with formula (3) ($\oplus$ and $\odot$ — according to transaction of addition and multiplication of the $\mod q$)

3 Analysis of Possible Modifications q-valued PRS Caused by the Error Occurred

It is known that the consequences of accidental errors that occur during the PRS generation associated with "unintentional" failures, as well as the consequences of intentional actions by an attacker based on the use of thermal, high-frequency, ionizing or other external influences in order to obtain mass malfunctions of the equipment by initiation of calculation errors, lead to similar types of PRS modification.

Fig. 2 shows main types of modification of PRS over the GF(q) field. The attacker's actions based on error generation are highly effective for most of the known and currently used algorithms for generating q-valued PRS [8–10]. It is known [11] that the probability of error generation is proportional to the irradiation time of the respective registers in a favorable state for the error occurrence and to the number of bits within which an error is expected. This type of impact has not been sufficiently studied and therefore represents a threat to the information security of modern and promising MIS functioning.

One of the ways to solve this problem is to develop a technique for improving the safety of the operation of the MIS nodes most susceptible to these effects, in particular, the nodes of q-valued PRS formation.

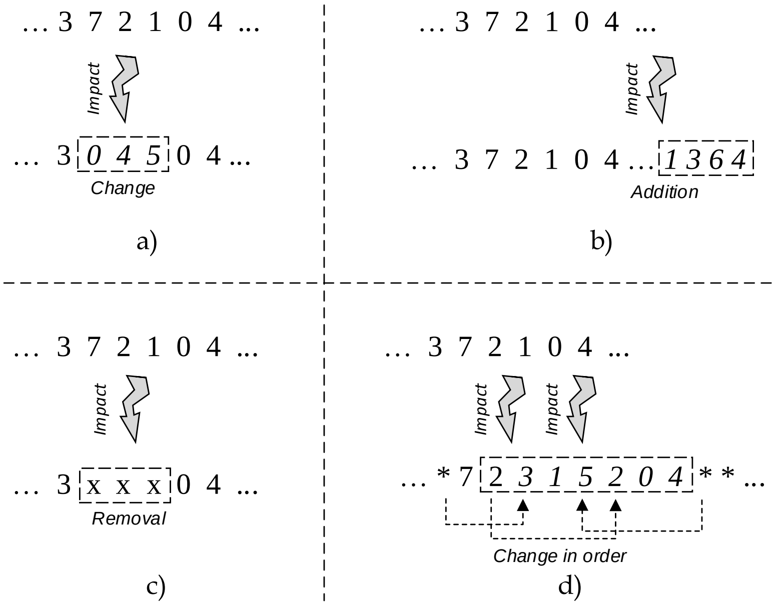

Fig. 2. The main types of PRS modification: a) change in the elements of the PRS, b) addition of new PRS elements, c) removal of the CAP elements, d) change in the order of the PRS elements

4 Analysis of Ways to Control the Generation of *q*-valued PRS

Currently, the necessary level of security for the functioning of the nodes for the q-valued PRS formation is achieved both through the use of redundant equipment (structural backup) and temporary redundancy due to various calculations repetition.

In the field of digital circuit design solutions based on the use of block redundant coding methods are known. To apply these methods to q-valued PRS generators it is necessary to solve the problem of parallelizing the calculation process of the q-valued PRS.

The solution of the problem is based on the use of classical parallel recursion calculation algorithms [12], for which the characteristic Eq. (3) corresponding to the generating polynomial (2) can be represented as a system of characteristic equations:

$$\begin{cases} a_{t,\,m-1} = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(m-1)} a_{t-1,\,p+i-1}, \\ a_{t,\,m-2} = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(m-2)} a_{t-1,\,p+i-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{t,\,1} = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(1)} a_{t-1,\,p+i-1}, \\ a_{t,\,0} = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(0)} a_{t-1,\,p+i-1}, \end{cases} \tag{4}$$

where $k_{i-1}^{(j)} \in \mathrm{GF}(q)$; $j = 0,\, 1,\, \dots,\, m-2,\, m-1$.

The system (4) forms an information matrix:

$$\mathbf{G_{Inf}} = \begin{Vmatrix} k_0^{(m-1)} & k_1^{(m-1)} & \dots & k_{m-2}^{(m-1)} & k_{m-1}^{(m-1)} \\ k_0^{(m-2)} & k_1^{(m-2)} & \dots & k_{m-2}^{(m-2)} & k_{m-1}^{(m-2)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k_0^{(1)} & k_1^{(1)} & \dots & k_{m-2}^{(1)} & k_{m-1}^{(1)} \\ k_0^{(0)} & k_1^{(0)} & \dots & k_{m-2}^{(0)} & k_{m-1}^{(0)} \end{Vmatrix}.$$

Similar result can be obtained in another convenient way [1]:

$$\mathbf{G_{Inf}} = \begin{Vmatrix} k_{m-1} & k_{m-2} & \dots & k_1 & k_0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{Vmatrix}^{m},$$

where the elements raised to the power m are of a matrix which is created according to the known rules of linear algebra for the calculation of the next q-valued element of the PRS a_{p+m}:

$$\begin{Vmatrix} a_{p+m} \\ a_{p+m-1} \\ \vdots \\ a_{p+2} \\ a_{p+1} \end{Vmatrix} = \left\| \begin{Vmatrix} a_{p+m-1} \\ a_{p+m-2} \\ \vdots \\ a_{p+1} \\ a_p \end{Vmatrix} \cdot \begin{Vmatrix} k_{m-1} & \dots & k_0 \\ 1 & \dots & 0 \\ 0 & \dots & 0 \\ 0 & \dots & 0 \\ 0 & \dots & 0 \end{Vmatrix} \right\|_q,$$

where $|\cdot|_q$ — is the smallest nonnegative deduction of the number “$\cdot$” on module q.

The technique for raising a matrix to the power can be performed with help of symbolic calculations in any computer algebra system with the subsequent simplification (in accordance with the axioms of the algebra and logic) of the elements of the resulting matrix of the form $Yk_j^b = k_j$ according to the rules:

1) $k_j^b = k_j$; 2) $Y = 0$, for even Y and $Y = 1$, for odd Y. Thus, we obtain the t-block of PRS:

$$\mathbf{A}_t = \left|\mathbf{G_{Inf}} \cdot \mathbf{A}_{t-1}\right|_q ,$$

where

$$\mathbf{A}_t = \left[a_{t,\,p+m-1}\; a_{t,\,p+m-2}\; \dots\; a_{t,\,1}\; a_{t,\,0}\right]^\top ,$$
$$\mathbf{A}_{t-1} = \left[a_{t-1,\,p+m-1}\; a_{t-1,\,p+m-2}\; \dots\; a_{t-1,\,1}\; a_{t-1,\,0}\right]^\top .$$

To create conditions for the use of a separable linear redundant code, we obtain a generating matrix $\mathbf{G_{Gen}}$, consisting of the information and verification matrixes by adding in the (4) test expressions:

$$\begin{cases} a_{t,\,p+m-1} = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(m-1)} a_{t-1,\,p+i-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{t,\,0} = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(0)} a_{t-1,\,p+i-1}, \\ a^*_{t,\,p+r-1} = \bigoplus\limits_{i=1}^{r} c_{i-1}^{(r-1)} a_{t-1,\,p+i-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a^*_{t,\,0} = \bigoplus\limits_{i=1}^{r} c_{i-1}^{(0)} a_{t-1,\,p+i-1}, \end{cases}$$

where $k_{i-1}^{(j)}$, $c_{i-1}^{(z)} \in \mathrm{GF}(q)$; $z = 0, \dots, r-1$; r — is the number of redundant symbols of the applied linear code; $j = 0, \dots, m-1$.

The forming matrix takes the form:

$$\mathbf{G_{Gen}} = \begin{Vmatrix} k_0^{(m-1)} & k_1^{(m-1)} & \dots & k_{m-2}^{(m-1)} & k_{m-1}^{(m-1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ k_0^{(0)} & k_1^{(0)} & \dots & k_{m-2}^{(0)} & k_{m-1}^{(0)} \\ c_0^{(r-1)} & c_1^{(r-1)} & \dots & c_{r-2}^{(r-1)} & c_{r-1}^{(r-1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_0^{(0)} & c_1^{(0)} & \dots & c_{r-2}^{(0)} & c_{r-1}^{(0)} \end{Vmatrix} .$$

Then the t-block of the q-valued PRS with test digits (linear code block)

$$\mathbf{A}^*_t = \left[a_{t,\,p+m-1}\; \dots\; a_{t,\,0}\; a^*_{t,\,p+r-1}\; \dots\; a^*_{t,\,0}\right]^\top$$

is calculated as:

$$\mathbf{A}^*_t = \left|\mathbf{G_{Gen}} \cdot \mathbf{A}_{t-1}\right|_q .$$

The anti-jamming decoding procedure is performed using known rules [13].

The use of linear redundant codes and “hot” backup methods is not the only option for realizing functional diagnostics and increasing the fault tolerance of digital devices. Important advantages for these purposes are found in arithmetic redundant codes, in particular, the so-called AN-codes and codes of modular arithmetic (MA). However, arithmetic redundant codes are not applicable to logical data types. In logical calculations, their structure collapses, which leads to the impossibility of monitoring errors in logical calculations.

The use of arithmetic redundant codes to control logical data types must be ensured by the introduction of additional procedures related to the “arithmetic” of the logical count.

5 The Procedure for Parallelizing the Generation of q-valued PRS by Means of Arithmetic Polynomials

Parallelizing the “calculation” processes of complex systems or minimizing the number of operations involving the use of all resources makes it possible to achieve any utmost characteristic or quality index, which in turn is necessary in most practically important cases. In turn, the new direction formed at the end of the last century – parallel-logical calculations through arithmetic (numerical) polynomials [14], also allowed to provide “useful” structural properties. It became possible to use arithmetic redundant codes to control logical data types and increase the fault tolerance of implementing devices by representing arithmetic expressions [14] as logical operations, in particular, by linear numerical polynomials (LNP) and their modular forms [15].

In [5] an algorithm for parallelizing the generation of binary PRS is presented based on the representation of systems of generating recurring logical formulas by means of LNP offered by V. D. Malyugin, which allowed using the redundant modular code device to control the errors of the functioning of the PRS generation nodes and, ensure the required safety of their functioning in the MIS.

To ensure the possibility of applying code control methods to generators of q-valued PRS, it is necessary to solve the problem of parallelizing the process of calculating them, while in [6] in general terms, approach for the synthesis of parallel generators of q-valued PRS on arithmetic polynomials is presented, the essence of which is the following.

Let a_0, a_1, a_2, $\ldots$, $a_{m-1}, \ldots$ — be the elements of the q-valued PRS satisfying the recurrence Eq. (3). Knowing that random element a_p $(p \geq m)$ of the sequence a_0, a_1, a_2, $\ldots$, a_{m-1}, $\ldots$ is determined by the preceding m elements, let us present the elements a_{p+m}, a_{p+m+1}, $\ldots$, a_{p+2m-1} of the section of the q-

valued PRS by the length m in the form of a system of characteristic equations:

$$\begin{cases} a_{p+m} = \bigoplus\limits_{i=1}^{m} k_{i-1} a_{p+i-1}, \\ a_{p+m+1} = \bigoplus\limits_{i=1}^{m} k_{i-1} a_{p+i}, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{p+2m-1} = \bigoplus\limits_{i=1}^{m} k_{i-1} a_{p+i+m-2}, \end{cases} \tag{5}$$

where $[a_{p+m}\ a_{p+m+1}\ \dots\ a_{p+2m-1}]$ — is the vector of the m-state of the q-valued PRS (or the internal state of the q-LFSR on m-cycle of work).

By analogy with [5] let us express the right-hand sides of the system (5) through the given initial conditions and let us write it as the m MFAL system of m variables:

$$\begin{cases} f_1\left(a_p,\, a_{p+1},\, \dots,\, a_{p+m-1}\right) = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(0)} a_{p+i-1}, \\ f_2\left(a_p,\, a_{p+1},\, \dots,\, a_{p+m-1}\right) = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(1)} a_{p+i-1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f_m\left(a_p,\, a_{p+1},\, \dots,\, a_{p+m-1}\right) = \bigoplus\limits_{i=1}^{m} k_{i-1}^{(m-1)} a_{p+i-1}, \end{cases} \tag{6}$$

where the coefficients $k_{i-1}^{(j)} \in \{0,\, 1,\, \dots,\, q-1\}$ $(i = 1,\, \dots,\, m;\ j = 0,\, \dots,\, m-1)$ are formed after expressing the right-hand parts of the system (5) through given initial conditions.

It is known that random MFAL can be represented in the form of an arithmetic polynomial in simple way [16, 17]:

$$L\left(a_p,\, a_{p+1},\, \dots,\, a_{p+m-1}\right) = \sum_{i=0}^{q^{m-1}-1} l_i\ a_p^{i_0} a_{p+1}^{i_1}\ \dots\ a_{p+m-1}^{i_{m-1}}, \tag{7}$$

where $a_u \in \{0,\, 1,\, \dots,\, q-1\}$; $u = 0,\, \dots,\, m-1$; l_i — i-coefficient of an arithmetic polynomial; $\left(i_0\ i_1\ \dots\ i_{m-1}\right)_q$ — representation of the parameter i in the q-scale of notation:

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

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

Similar to [16,17] let us implement the MFAL system (6) by computing some arithmetic polynomial. In order to do this, we associate the MFAL system (6) with a system of arithmetic polynomials of the form (7), we obtain:

$$\begin{cases} L_1\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = \sum\limits_{i=0}^{q^{m-1}-1} l_{1,\,i}\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}}, \\ L_2\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = \sum\limits_{i=0}^{q^{m-1}-1} l_{2,\,i}\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ L_m\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = \sum\limits_{i=0}^{q^{m-1}-1} l_{m,\,i}\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}}. \end{cases} \tag{8}$$

Let us multiply the polynomials of the system (8) by weights q^{e-1} ($e = 1,\, 2,\, \ldots,\, m$):

$$\begin{cases} L_1^*\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = q^0 L_1\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) \\ = \sum\limits_{i=0}^{q^{m-1}-1} l_{1,i}^*\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}}, \\ L_2^*\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = q^1 L_2\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) \\ = \sum\limits_{i=0}^{q^{m-1}-1} l_{2,i}^*\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ L_m^*\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = q^{m-1} L_m\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) \\ = \sum\limits_{i=0}^{q^{m-1}-1} l_{m,i}^*\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}}, \end{cases}$$

where $l_{e,\,i}^* = q^{e-1} l_{e,\,i}$ $(e = 1, 2, \ldots, m; \quad i = 0, \ldots, q^m - 1)$.

Then we get:

$$L\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = \sum_{i=0}^{q^{m-1}-1} \sum_{e=1}^{d} l_{e,\,i}^*\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}} \tag{9}$$

or using the provisions of [18]:

$$D\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right) = \left| \bigoplus_{i=0}^{q^{m-1}-1} v_i\; a_p^{i_0} a_{p+1}^{i_1}\; \ldots\; a_{p+m-1}^{i_{m-1}} \right|_{q^m}, \tag{10}$$

where

$$v_i = \bigoplus_{e=1}^{m} l_{e,\,i}^* \; (i = 0,\, 1,\, \ldots,\, q^{m-1} - 1).$$

Let us calculate the values of the desired MFAL. For this, the result of the calculation (10) is presented in the q-scale of notation and we apply the camouflage operator $\varXi^w\{D\left(a_p,\, a_{p+1},\, \ldots,\, a_{p+m-1}\right)\}$:

$$\Xi^{w}\{D\,(a_p,\,a_{p+1},\,\ldots,\,a_{p+m-1})\} = \left|\left\lfloor \frac{D\,(a_p,\,a_{p+1},\,\ldots,\,a_{p+m-1})}{q^{w}} \right\rfloor\right|_{q}$$

, where w — is the desired q-digit of the representation $D\,(a_p,\,a_{p+1},\,\ldots,\,a_{p+m-1})$.

The presented method, based on the MFAL arithmetic representation, makes it possible to control the q-valued PRS generation errors by means of arithmetic redundant codes.

6 Control of Errors in the Operation of Generators of q-valued PRS by Redundant MA Codes

In MA, the integral nonnegative coefficient $l^{*}_{e,\,i}$ of an arithmetic polynomial (9) is uniquely presented by a set of balances on the base of MA ($s_1,\,s_2,\,\ldots,\,s_\eta <$ $< s_{\eta+1} < \ldots < s_\psi$ — simple pairwise):

$$l^{*}_{e,\,i} = (\alpha_1,\,\alpha_2,\,\ldots,\,\alpha_\eta,\,\alpha_{\eta+1},\,\ldots,\,\alpha_\psi)_{\mathrm{MA}}, \tag{11}$$

where $\alpha_\tau = \left|l^{*}_{e,\,i}\right|_{s_\tau}$; $\tau = 1,\,2,\,\ldots,\,\eta,\,\ldots,\,\psi$. The working range $S_\eta = s_1 s_2 \ldots s_\eta$ must satisfy $S_\eta > 2^{g}$, where $g = \sum\limits_{1\le\varepsilon\le\sigma} \theta_\varepsilon$ — is the number of bits required to represent the result of the calculation (9).

Balances $\alpha_1,\,\alpha_2,\,\ldots,\,\alpha_\eta$ are informational, and $\alpha_{\eta+1},\,\ldots,\,\alpha_\psi$ — are control. In this case, MA is called extended and covers the complete set of states presented by all the ψ balances. This area is the full MA range $[0,\,S_\psi)$, where $S_\psi = s_1 s_2 \ldots s_\eta s_{\eta+1} \ldots s_\psi$, and consists of the operating range $[0,\,S_\eta)$, defined by the information bases of the MA, and the range defined by the redundant bases $[S_\eta,\,S_\psi)$, representing an invalid area for the results of the calculations. This means that operations on numbers $l^{*}_{e,\,i}$ are performed in the range $[0,\,S_\psi)$. Therefore, if the result of the MA operation goes beyond the limits S_η, then the conclusion about the calculation error follows.

Let us study the MA given by the $s_1,\,s_2,\,\ldots,\,s_\eta,\,\ldots,\,s_\psi$ bases. Each coefficient $l^{*}_{e,\,i}$ of a polynomial (9) is presented in the form (11) and we obtain an MA redundant code, represented by a system of polynomials:

$$\begin{cases} U^{(1)} = L^{(1)}\,(a_p,\,a_{p+1},\,\ldots,\,a_{p+m-1}) = \sum\limits_{i=0}^{q^{m-1}-1} \sum_{e=1}^{d} l^{*(1)}_{e,\,i}\; a_p^{i_0} a_{p+1}^{i_1} \ldots a_{p+m-1}^{i_{m-1}}, \\ U^{(2)} = L^{(2)}\,(a_p,\,a_{p+1},\,\ldots,\,a_{p+m-1}) = \sum\limits_{i=0}^{q^{m-1}-1} \sum_{e=1}^{d} l^{*(2)}_{e,\,i}\; a_p^{i_0} a_{p+1}^{i_1} \ldots a_{p+m-1}^{i_{m-1}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ U^{(\eta)} = L^{(\eta)}\,(a_p,\,a_{p+1},\,\ldots,\,a_{p+m-1}) = \sum\limits_{i=0}^{q^{m-1}-1} \sum_{e=1}^{d} l^{*(\eta)}_{e,\,i}\; a_p^{i_0} a_{p+1}^{i_1} \ldots a_{p+m-1}^{i_{m-1}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ U^{(\psi)} = L^{(\psi)}\,(a_p,\,a_{p+1},\,\ldots,\,a_{p+m-1}) = \sum\limits_{i=0}^{q^{m-1}-1} \sum_{e=1}^{d} l^{*(\psi)}_{e,\,i}\; a_p^{i_0} a_{p+1}^{i_1} \ldots a_{p+m-1}^{i_{m-1}}. \end{cases} \tag{12}$$

Substituting in (12) the values of the MA balances for the corresponding bases for each coefficient (9) and the values of the variables a_p, a_{p+1}, …, a_{p+m-1}, we obtain the values of the polynomials of the system (12), where $U^{(1)}$, $U^{(2)}$, …, $U^{(\eta)}$, …, $U^{(\psi)}$ — are nonnegative integrals. In accordance with the Chinese balances theorem, we solve the system of equations:

$$\begin{cases} U^* = \left|U^{(1)}\right|_{s_1}, \\ U^* = \left|U^{(2)}\right|_{s_2}, \\ \dots\dots\dots\dots \\ U^* = \left|U^{(\eta)}\right|_{s_\eta}, \\ \dots\dots\dots\dots \\ U^* = \left|U^{(\psi)}\right|_{s_\psi}. \end{cases} \tag{13}$$

Since s_1, s_2, …, s_η, …, s_ψ are simple pairwise, the only solution (13) gives the expression:

$$U^* = \left|\sum_{d=1}^{\psi} S_{d,\,\psi}\mu_{d,\,\psi}U^{(d)}\right|_{S_\psi}, \tag{14}$$

where $S_{d,\,\psi} = \dfrac{S_\psi}{s_d}$, $\mu_{d,\,\psi} = \left|S_{d,\,\psi}^{-1}\right|_{s_d}$, $S_\psi = \prod\limits_{d=1}^{\psi} s_d$.

The occurrence of the calculation result (14) in the range (test expression)

$$0 \leq U^* < S_\eta,$$

means no detectable calculation errors.

Otherwise, the procedure for restoring the reliable functioning of the q-valued PRS generator can be implemented according to known rules [19].

7 Conclusion

A secure parallel generator of q-valued PRS on arithmetic polynomials is presented. The implementation of generators of q-valued PRS using arithmetic polynomials and redundant MA codes makes it possible to obtain a new class of solutions aimed to safely implement logical cryptographic functions. At the same time, both functional monitoring of equipment (in real time, which is essential for MIS) and its fault tolerance is ensured due to the possible reconfiguration of the calculator structure in the process of its degradation. The classical q-LFSR, studied in this work, forms the basis of more complex q-valued PRS generators.

References

1. Klein, A.: Stream Ciphers. Springer, http://www.springer.com. (2013)

2. Schneier, B.: Applied Cryptography. Wiley, New York (1996)
3. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge: Cambridge Univ. Press. (1987)
4. Yang, B., Wu, K., Karri, R.: Scan based side channel attack on data encryption standard. Report **2004**(324), 114–116 (2004)
5. Finko, O.A., Dichenko, S.A.: Secure Pseudo-Random Linear Binary Sequences Generators Based on Arithmetic Polynoms. Advances in Intelligent Systems and Computing, Soft Computing in Computer and Information Science, **342**, Springer, Cham, pp. 279–290 (2015)
6. Finko, O.A., Samoylenko, D.V., Dichenko, S.A., Eliseev, N.I.: Parallel generator of q-valued pseudorandom sequences based on arithmetic polynomials. Przeglad Elektrotechniczny, **3**, pp. 24–27 (2015)
7. MacWilliams, F., Sloane, N.: Pseudo-random sequences and arrays, Proc. IEEE, **64**, pp. 1715–1729 (1976)
8. Canovas, C., Clediere, J.: What do DES S-boxes say in differential side channel attacks? Report **2005**(311), 191–200 (2005)
9. Carlier, V., Chabanne, H., Dottax, E.: Electromagnetic side channels of an FPGA implementation of AES. Report **2004**(145), 111–124 (2004)
10. Page, D.: Partitioned cache architecture as a side-channel defence mechanism. Report **2005**(280), 213–225 (2005)
11. Gutmann, P.: Software generation of random numbers for cryptographic purposes. Usenic security symp., usenix assoc., berkeley, pp. 243–257, Calif (1998)
12. Ortega, J.M.: Introduction to Parallel & Vector Solution of Linear Systems. Plenum Press, New York (1988)
13. Hamming, R.: Coding and Information Theory. Prentice-Hall (1980)
14. Malyugin, V.D.: Representation of boolean functions as arithmetic polynomials. Autom. Remote. Control. **43**(4), 496–504 (1982)
15. Finko, O.A.: Large systems of boolean functions: realization by modular arithmetic methods. Autom. Remote. Control. **65**(6), 871–892 (2004). June
16. Finko, O.A.: Modular forms of systems of k-valued functions of the algebra of logic. Autom. Remote. Control. **66**(7), 1081–1100 (2005)
17. Kukharev, G.A., Shmerko, V.P., Zaitseva, E.N.: Algorithms and systolic processors of multivalued data. Minsk: Science and Technology (1990) (in Russian)
18. Aslanova, N.H., Faradzhev, R.G.: Arithmetic representation of functions of many-valued logic and parallel algorithm for finding such a representation. Autom. Remote. Control. **53**(2), 251–261 (1992)
19. Omondi, A., Premkumar, B.: Residue Number System: Theory and Implementation. Imperial Collegt Press, London (2007)