e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 3
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 3

ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIVE INFORMATION TECHNOLOGIES

UDC 004.056, 032.817

SYNTHESIS OF CRYPTORESISTANT GENERATORS OF PSEUDORANDOM NUMBERS BASED ON GENERALIZED GALOIS AND FIBONACCI MATRIXES

Beletsky A. Ya. – Dr. Sc., Professor, Professor of the Department of Electronics, National Aviation University, Ukraine.

ABSTRACT

Context. The problem to form generalized primitive matrixes on the Galois and Fibonacci any order over the field characteristics 2 for the construction by the generators gamma functions for cryptographically stable algorithms of inline data encryption, free from the attack of Berlekamp-Messi (BM).

Objective. Development of a way to eliminate the threat an attack using the BM algorithm on LFSR-generators of pseudorandom numbers (PRN) to increase their crypto stability.

Method. Linear Feedback Shift Registers (LFSR) are themselves good pseudorandom PRN generators, but they have undesirable properties that reduce the efficiency of their use. For the registers of length shift *n* their internal state is a function of the previous output bits of the generator. Even if the feedback scheme is kept the secret, it can be determined by 2*n* output bits of the generator with the help of BM algorithm, which reduces the crypto-resistance of the generator PRN. The basis for single loop feedback circuits, which cover the classical LFSR-generators of PRN, are primitive polynomials.

There are various ways to increase the crypto-resistance of LFSR-generators. To their number concern: introduction of nonlinear transformations, use poly register generators (as, for example, in the algorithm of encryption A5) and several others. The transition from classical LFSR-generators to generators basis on the generalized matrixes of Galois and Fibonacci leads to the fact that the algorithm of BM loses the ability to determine the unattainable polynomials generating multi-circuit feedback circuits in LFSR-generators. The reason for this feature is that the series of bits generated by the generalized generator becomes dependent not only on the selected irreducible polynomial but also on the primitive element that participates in the creation of the feedback loop generator.

Results. The PRN generators developed by LFSR were used to organize bytes of streaming information encryption.

Conclusions. Statistical tests of the proposed PRN generators carried out with the help of NIST STS, and Diehard [16–18] packages have confirmed the high quality of the generated sequences. Moreover, the generators turned out to be cryptographically resistant to BM attacks. The use of these generators in the formation of long keys, necessary, for example, in RSA encryption protocols and other applications is promising. As an area of further researches, development of the generalized generators of PRN above a field of Galois of any characteristic.

KEYWORDS: irreducible polynomials, primitive matrixes, Galois fields, linear shift registers, pseudorandom number generators.

ABBREVIATIONS

BM is a Berlekamp-Messi;
CGM is a classical Galois matrix;
GGM is a generalized Galois matrix;
IP is an irreducible polynomial;
LFSR is a linear feedback shift register;
PRN is a pseudorandom number;
PrP is a primitive polynomial.

NOMENCLATURE

α_k is a polynomial coefficient;

θ is a primitive Galois field element;

ω is a forming generalized Galois element matrix;

f_n is an IP of *n*-degree;

$\boldsymbol{G}_{f,\omega}^{(n)}$ is a Galois matrix of *n*-degree, generated by an IP f_n and forming element ω;

$\boldsymbol{F}_f^{(n)}$ is a Fibonacci matrix of *n*-degree, generated by an IP f_n and forming element ω;

${}^*\boldsymbol{F}_f^{(n)}$ is a Fibonacci conjugate matrix of *n*-degree, generated by an IP f_n and forming element ω;

$\boldsymbol{E}$ is an identity matrix;

$\vec{\boldsymbol{E}}$ is a cyclic shift operator one step to the left;

$\vec{\boldsymbol{E}}$ is a cyclic shift operator one step to the right;

n is a degree of matrix or polynomial;

$\boldsymbol{P}$ is a permutation matrix;

DOI 10.15588/1607-3274-2019-3-10

$\boldsymbol{P}^{-1}$ is a permutation reverse matrix;

S is a state of generator PRN;

T is an operator of the classic (left side) transposition;

$\boldsymbol{V}$ is a $(n+1)$-bit vector;

x is a formal parameter of a polynomial;

1 is an operator of the inverse permutation matrix;

$\overleftarrow{\mathbf{1}}$ is a cyclic shift operator of the inverse permutation matrix one step to the left;

$\vec{\mathbf{1}}$ is a cyclic shift operator of the inverse permutation matrix one step to the right;

$\perp$ is a right side transposition operator.

INTRODUCTION

One of the most prime problems in the theory and practice of cryptographic information protection is the problem of constructing PRN generators of maximum length (period) with acceptable statistical properties, which are usually realized by means of linear feedback shift registers (LFSR) in the configuration (according to the scheme) of Galois or Fibonacci [1–4].

Structural schemes of classical n-bit LFSR-generators of PRN are clearly defined by n-th degree IP $f_n(x)$, using of which single-circuit feedback in shift registers is established. It is known, that for the shift register to be the maximum period register, and the corresponding feedback polynomial must be primitive. For LFSR discharges are usually used D-triggers that overwrite the input signal to the trigger output at the time of receipt of the synchroimpulse.

The main disadvantage of LFSR-generators of PRN is that the linearity of the sequence at the register output allows us to determine the feedback polynomial $f_n(x)$ by $2n$ consecutive bits using the BM algorithm [13].

The object of the study is the process of building LFSR-generators of the PRN, providing cryptographic security to attacks based on the algorithm of BM.

As a rule, the problem of providing reliable crypto-resistance of LFSR-generators is solved by introducing nonlinearity of the formed flow of PRN. However, this method of constructing generators, as a rule, is possible, if the order of the generator does not exceed 32. Therefore, the problem of synthesis of multi-digit linear generators of the PRN, providing at the same time nonlinearity of the flow of PRN.

The subject of the study is the methods of construction of LFSR-generators of PRN, covered by multi-circuit feedback circuits.

Such circuits arise as a result of the replacement of PrP on polynomials, not necessarily be primitive. However, the element θ, forming a pseudorandom sequence, must be the primitive element of the expanded field of Galois, generated by an IP, such that $\theta > 10$.

The purpose of the work is to eliminate the threat of an attack using the Berlekemp-Messi algorithm on LFSR-generators of the PRN.

1 PROBLEM STATEMENT

It is known that LFSR in itself is an excellent PRN generator, but they have undesirable properties, which reduce the efficiency of their use. For length register n, their internal state is a function of the n previous output bits of the generator. Even if the feedback scheme is kept a secret, by the output $2n$ bits of the generator, using the algorithm of BM, can determine it. The BM-attack can be eliminated by introducing the nonlinearity in the process of formation of the PRN. However, this method of attack elimination may not be acceptable, because we implement it only when the register length does not exceed, as a rule, n=32.

Proceeding from the above-stated, the main purpose of the given research is working out of a way of elimination of the threat of a BM-attack on LFSR-generators PRN of any length for an increase of their cryptographic safety.

2 REVIEW OF THE LITERATURE

Random numbers are used in many areas of research, including cryptography and information security [1, 4], computer and mathematical modeling [6, 7], sociological analysis [3], innovative work, based on the "trial and error" method and in other areas of scientific knowledge. Numerous monographs [1, 2], journal publications [5, 11], reports at scientific conferences [13, 15, 16] and Web publications [9–11, 18] are devoted to the issues of building LFSR-generators PRN.

Let us note the fundamental differences both in the presentation of the problem of synthesis of LFSR-generators and the methods of their implementation, adopted in this paper in comparison with the cited sources. First, note that the numbering of register digits and shift of the generator contents in Galois configurations is performed from right to left. The chosen order of numerical of cells the register and the direction of their contents displacement are not only natural (as, for example, in decimal numbering), but also lead to more transparent algorithms of generalized Galois matrices construction. And, secondly, if in classical (named by us single-circuit) LFSR-generators feedback in registers is created by PrP, and the matrixes of Galois are generated by the primitive forming element, polynomials, using which feedback in the generalized (multi-circuit) LFSR-generators of PRN, should not be primitive at all. Regardless of whether primitive or non-primitive is polynomic of feedback, the primitive constituent element the GGM must exceed 10. It is under such conditions that the increase in the crypto-resistance of the proposed variants of LFSR-generators of PRN in comparison with the crypto-resistance of classical generators is provided. The reason for such phenomenon consists that the generalized LFSR-generators appear protected from the attack of BM [14].

3 MATERIALS AND METHODS

Each LFSR-generator of PRN according to the scheme of Galois or Fibonacci is answered by unequivocally connected matrixes which we will name as well as corresponding generators, and to designate symbols $\boldsymbol{G}$

DOI 10.15588/1607-3274-2019-3-10

and $\boldsymbol{F}$. A distinctive feature of matrixes of Galois and Fibonacci consists that on their basis it is possible to create the binary *m*- sequence similar to the numbers formed by classical LFSR-generator of PRN.

Let's the $S(k)$ -state of the n -bit generator in the configuration of Galois after the k -th synchroimpulse, the calculation scheme of which is represented by the matrix expression,

$$S(k+1) = S(k) \cdot \boldsymbol{G}_f^{(n)}, \quad k = 0, 1, \ldots, \quad S(0) = \underbrace{00\ldots1}_{n \text{ bit}} \qquad (1)$$

Our task is to make sure that the given PrP $f = 1\alpha_{n-1}\alpha_{n-1}\ldots\alpha_1 1, \quad \alpha_k \in GF(2) = \{1, 2\}$, to calculate matrixes of Galois the $n-$degree, using which the ratio (1) forms the same number of PRN as the generator of PRN built based the LFSR, covered by the feedback chain caused by PrP f .

Let us try to deal with this problem for small orders of matrixes first. Let us turn to the scheme of the PRN generator, reduced to Fig. 1.

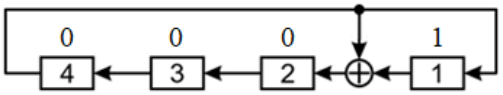

Figure 1 – Illustration of the initial state of the Galois PRN generator

The numeric above of the generator discharge characterize the logical signal level at the output of the corresponding register cell (trigger). As synchronous sends are received, a unit from the lower (right) digit of the generator moves to its higher digits, as it is shown in Fig. 2.

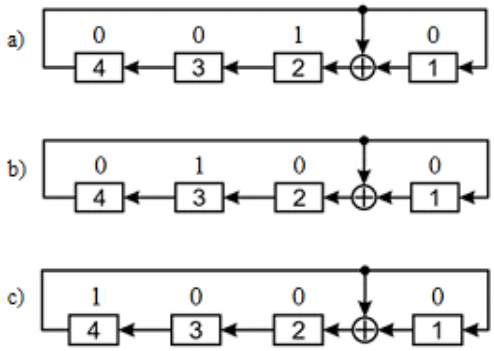

Figure 2 – The PRN generator states after:
a) – First, b) – Second, c) – Third synchrotact

From Fig. 2 follows that the third synchrotacte the logical units arrive at the inputs of both the first and the second trigger and, consequently, at the fourth step of PRN generation (Fig. 3) appear at the outputs of these triggers.

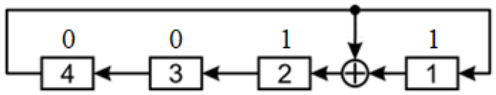

Figure 3– The PRN generator status after the fourth synchrotact

Let us make a matrix $\boldsymbol{G}_{13}^{(4)}$ of the totality of state vectors into which the Galois generator passes after the first four synchrotacte, having vectors in the matrix starting from its lower line.

$$\boldsymbol{G}_{13}^{(4)} = \begin{array}{c} \uparrow k \\ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ \leftarrow t \quad 4 \quad 3 \quad 2 \quad 1 \end{array} \begin{array}{c} \\ 4 \\ 3 \\ 2 \\ 1 \end{array} \qquad (2)$$

Note that the lower index 13 in the matrix designation $\boldsymbol{G}_f^{(n)}$ in (2) is nothing, but a 16-number system a record of PrP f=1'0011. We will use the same form of representation of numerical values of polynomials f in the future. Besides, we will take into account that the numbering of rows of Galois matrix is carried out from bottom to top and the columns - from right to left, different from the generally accepted ones. The chosen way of the numbering of matrix rows and columns $\boldsymbol{G}_f^{(n)}$ simplifies, as we will see later, the separate tasks of building a structural scheme of PRN LFSR-generators.

The sequence of PRN, formed by the LFSR-generator of Galois (Fig. 1), coincides with the sequence, calculated by the formula (1) for the matrix (2), and is summarized in Table 1.

Table 1 – The multiplicative group formed by the PRN generator (Fig. 1 or matrix (2))

Degree (or step)	Deduction ranks			
k	4	3	2	1
0	0	0	0	1
1	0	0	1	0
2	0	1	0	0
3	1	0	0	0
4	0	0	1	1
5	0	1	1	0
6	1	1	0	0
7	1	0	1	1
8	0	1	0	1
9	1	0	1	0
10	0	1	1	1
11	1	1	1	0
12	1	1	1	1
13	1	1	0	1
14	1	0	0	1
15	0	0	0	1

DOI 10.15588/1607-3274-2019-3-10

It is easy to see that, firstly, the matrix rows (2) make up a set of linearly independent vectors, which makes $\boldsymbol{G}_{13}^{(4)}$ is a nonsingular matrix. Secondly, the matrix $\boldsymbol{G}_{13}^{(4)}$, being substituted in equation (1), forms several four-digit codes, summarized in Table 1. In addition, thirdly, the top line of the matrix (2) is nothing but the PrP of the fourth-degree $f = 1'0011$, in which the older unit is removed.

Based on the analysis of the matrix $\boldsymbol{G}_{13}^{(4)}$, written out by the ratio (2), we come to the following rule of construction of CGM $\boldsymbol{G}_f^{(n)}$ of the order n generated by PrP degree n. Let us call it the Rule of GGM [(1)]. In item 4 the Rule of GGM will be introduced.

Rule of GGM [(1)]: The basis of the matrix $\boldsymbol{G}_f^{(n)}$ is a single matrix $\boldsymbol{E}$ of the order $(n-1)$, framed by a zero column on the right and a PrP f with a thrown out the senior (left) unit.

The general form of GGM $\boldsymbol{G}_f^{(n)}$, in which bold font for clarity are selected fringing elements (right – zero column and the top – the line, which is shortened by one digit on the left PrP, generating GGM $\boldsymbol{G}_f^{(n)}$), looks like:

$$\boldsymbol{G}_f^{(n)} = \begin{pmatrix} \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_2 & \alpha_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & & 1 & 0 \end{pmatrix} \begin{matrix} n \\ n-1 \\ n-2 \\ \cdots \\ 2 \\ 1 \end{matrix} \\ \begin{matrix} n & n-1 & \cdots & 3 & 2 & 1 \end{matrix} . \quad (3)$$

By the general form (3) we will make, for example, the matrix of the eighth-order $\boldsymbol{G}_f^{(8)}$ with the PrP in a feedback circuit $f_8 = 101100101$

$$\boldsymbol{G}_{165}^{(8)} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix} \\ \begin{matrix} 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{matrix} . \quad (4)$$

The scheme of LFSR-generator PRN in Galois configuration, corresponding to the matrix (4), is presented in Fig. 4 a.

Galois $\boldsymbol{G}_f^{(n)}$ and Fibonacci's $\boldsymbol{F}_f^{(n)}$ matrixes are linked by a right-sided transposition operator $\perp$, i.e. transposition relative to an auxiliary diagonal,

$$\boldsymbol{G}_f^{(n)} \underset{\perp}{\overset{\perp}{\rightleftharpoons}} \boldsymbol{F}_f^{(n)} . \quad (5)$$

The transformation (5) of the Galois matrix (4) leads to the Fibonacci's matrix,

$$\boldsymbol{F}_{165}^{(8)} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix} \\ \begin{matrix} 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{matrix} . \quad (6)$$

The scheme of LFSR-generator PRN in Fibonacci configuration, corresponding to the matrix (4), is presented in Fig. 4 b.

Let us denote through ${}^*\boldsymbol{G}_f$ (${}^*\boldsymbol{F}_f$) – matrixes formed by classical (left-hand) transposition of Galois (Fibonacci) matrixes and call them conjugated to matrixes $\boldsymbol{G}_f$ and $\boldsymbol{F}_f$, accordingly. We have

$$\boldsymbol{G}_f^{(n)}\left(\boldsymbol{F}_f^{(n)}\right) \underset{T}{\overset{T}{\rightleftharpoons}} {}^*\boldsymbol{G}_f^{(n)}\left({}^*\boldsymbol{F}_f^{(n)}\right) . \quad (7)$$

The conjugate matrixes of Galois and Fibonacci of the eighth order, generated by matrixes (4) and (6) and transformations (5), look like:

$${}^*\boldsymbol{G}_{165}^{(8)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix} \\ \begin{matrix} 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{matrix} ; \quad (8)$$

A structural scheme of conjugate LFSR-generators of PRN, corresponding to matrixes of Galois ${}^*\boldsymbol{G}_{165}^{(8)}$ from (8) and Fibonacci ${}^*\boldsymbol{F}_{165}^{(8)}$ – (9), are presented on Fig. 5 a, b.

DOI 10.15588/1607-3274-2019-3-10

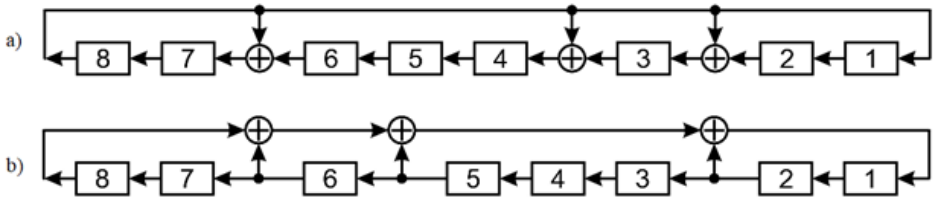

Figure 4 – The scheme of LFSR-generators of PRN in the configuration of Galois (a) and Fibonacci (b)

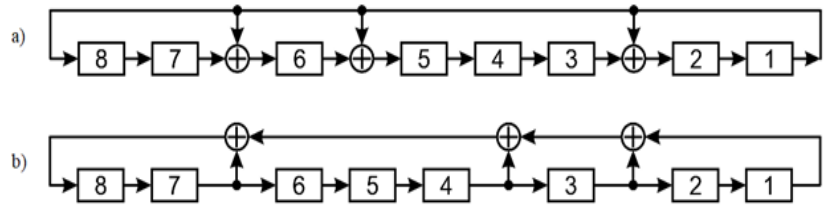

Figure 5 – The scheme of conjugate LFSR-generators of PRN in the configuration of Galois (a) and Fibonacci (b)

$$ {}^{*}\boldsymbol{F}_{165}^{(8)} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{matrix} 8 \\ 7 \\ 6 \\ 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{matrix} \\ 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1 \qquad (9) $$

The set of $\boldsymbol{G}_f^{(n)}$, $\boldsymbol{F}_f^{(n)}$ and conjugate matrixes ${}^{*}\boldsymbol{G}_f^{(n)}$, ${}^{*}\boldsymbol{F}_f^{(n)}$ can be displayed, as shown in Fig. 6. Arrows in Fig. 3 denote directions in rows or columns of matrixes, in which the coefficients α_k, $k=\overline{0,n}$, of PrP f_n are arranged, starting with the lowest coefficient α_0 up to the road of the higher coefficient.

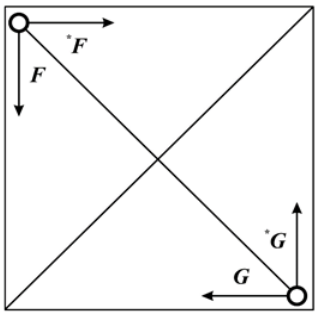

Figure 6 – Conditional graphics display Galois and Fibonacci matrixes

The rule for constructing CGM can be rephrased by calling it the updated version of the Construction Rules option:

Rule of GGM [(2)]: In the right corner of the bottom line of the synthesized GGM of order *n*, the element $\theta_{\min}=10$, forming it is written, which is the minimal primitive element of the field generated $GF(2^n)$ by a PrP f_n of degree *n*. The digits of the line to the left of the are $\theta_{\min}$ filled with zeros. Subsequent rows of the matrix $\boldsymbol{G}_f^{(n)}$ (bottom-up) are obtained by shifting the previous row one digit to the left, and zeros are entered into the released right digits. If, when a row is shifted, its most significant unit goes beyond the matrix $\boldsymbol{G}_f^{(n)}$, then the $(n+1)-$ bit vector $\boldsymbol{V}=1\underbrace{00\ldots0}_{n\ \text{bit}}$ corresponding to this row is reduced to the remainder modulo PrP f_n and, thus, the row becomes a $n-$ bit because the vector deduction $\boldsymbol{V}$ is equal to the polynomial f_n, which ejected the older unit.

Synthesized by Rule [(2)] (as well as by Rule [(1)]) the Galois matrixes $\boldsymbol{G}_f^{(n)}$ refer to the set of primitive matrixes in the sense that several powers of such matrixes, starting with a zero for which $(\boldsymbol{G}_f^{(n)})^0$ it is equal to the identity matrix, forms several maximum lengths. In this case, algebraic transformations are performed over the field Galois $GF(2)$; that is, all elements of the matrixes obtained in the course of matrix calculations are reduced to the remainder modulo 2.

Primitive matrixes $\boldsymbol{G}_f^{(n)}$ can be constructed not only based on the PrP, but also of any IP (IP), which are not necessarily primitive, provided that the element ω forming $\boldsymbol{G}_f^{(n)}$ is a primitive element of the field $GF(2^n)$ over the IP f_n.

We call the Galois matrixes generated by not necessarily the PrP f_n, which forms an element ω such that, $\omega \geq \theta_{\min}=10$, GGM and introduce the notation for them $\boldsymbol{G}_{f,\omega}^{(n)}$ [12]. Synthesis of GGM $\boldsymbol{G}_{f,\omega}^{(n)}$ is carried out according to the rule called the GGM rule, similar to the above-formulated GGM Rules.

DOI 10.15588/1607-3274-2019-3-10

Rule of GGM. The bottom line of the synthesized GGM $\boldsymbol{G}_{f,\omega}^{(n)}$ is recorded forming its element $\omega \geq 10$, which is an element of the field $GF(2^n)$, generated by an IP f_n. If at shift the non-zero bit of a line goes beyond the left border of a matrix, the vectors, answering to such lines, are led to the rest on the module f_n and, by this way, the line becomes $n-$ bit again.

From the theory of polynomials of one variable x it is known, that multiplication of an arbitrary degree k polynomial $\omega_k(x)$ by the x equivalent of its shift by one digit to the left. Or, in other words,

$$x \cdot \omega_k(x) \rightarrow \omega_{k+1}(x). \qquad (10)$$

Using ratio (10) and taking into account how GGM is formed, record the transformation chain

$$\boldsymbol{G}_{f,\omega}^{(n)} \Rightarrow \begin{bmatrix} x^{n-1} \cdot \omega \\ x^{n-2} \cdot \omega \\ \cdots \\ x \cdot \omega \\ x \end{bmatrix} \bmod f_n = \omega \cdot \begin{bmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{bmatrix} \bmod f_n. \qquad (11)$$

Elements of the right vector-column inequality (11) are monomers, which, being represented in binary form, convert this vector-column into a single matrix, i.e.

$$\begin{bmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} = \boldsymbol{E}, \qquad (12)$$

which makes it possible to formulate the following statement.

Affirmation. The GGM $\boldsymbol{G}_{f,\omega}^{(n)}$ of the order n above IP f_n isomorphous to its constitutive element, which is a field $GF(2^n)$ element

$$\boldsymbol{G}_{f,\omega}^{(n)} \leftrightarrow \omega. \qquad (13)$$

Therefore, according to the expressions (12) and (13), there is a mutually unambiguous correspondence (isomorphism) between GGM $\boldsymbol{G}_{f,\omega}^{(n)}$ and its forming element ω, which is reflected by the ratio (10) and leads to such consequences:

Consequence 1. The generalized matrixes of Galois $\boldsymbol{G}_{f,\omega}^{(n)}$ are non-singular at any parameters f_n and ω, as are formed linearly independent lines.

Consequence 2. To elevate the matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ for the degree k, it is enough to calculate IE $\omega_k = \omega^k \pmod{f_k}$ and make a matrix $\boldsymbol{G}_{f,\omega_k}^{(n)}$ using the diagonal filling method.

Consequence 3. The minimum non-zero value of degree *e* providing equality $\left(\boldsymbol{G}_{f,\omega}^{(n)}\right)^e = \boldsymbol{E}$ coincides with the order of the element ω, which forms the matrix $\boldsymbol{G}_{f,\omega}^{(n)}$.

Consequence 4. The generalized matrix of Galois $\boldsymbol{G}_{f,\omega}^{(n)}$ is primitive, if the element forming ω it is primitive, i.e. if $\omega = \theta$, there is θ a primitive element of the field $GF(2^n)$.

Consequence 5. The operation of multiplication of Galois $\boldsymbol{G}_{f,\omega_1}^{(n)}$ and $\boldsymbol{G}_{f,\omega_2}^{(n)}$, $\omega_1 \neq \omega_2$, is a commutative operation, because according to the ratio (10) of the product in the left and right parts of the equality $\boldsymbol{G}_{f,\omega_1}^{(n)} \cdot \boldsymbol{G}_{f,\omega_2}^{(n)} = \boldsymbol{G}_{f,\omega_2}^{(n)} \cdot \boldsymbol{G}_{f,\omega_1}^{(n)}$, which must satisfy the commutative product, are equivalent to the products of elements $(\omega_1 \cdot \omega_2)$ and $(\omega_2 \cdot \omega_1)$, calculated on the module of the IP f_n, and their equality is quite obvious.

Consequence 6. Arbitrary modular algebraic transformations (summation, subtraction, multiplication, and division) over Galois matrixes are isomorphic to the same transformations over the constitutive elements of these matrixes.

Consequence 7. Set GGMs can be expanded by introducing similar Galois matrixes ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$ or Fibonacci ${}^*\boldsymbol{F}_{f,\omega}^{(n)}$ defined by

$${}^*\boldsymbol{G}_{f,\omega}^{(n)}({}^*\boldsymbol{F}_{f,\omega}^{(n)}) = \boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega}^{(n)}(\boldsymbol{F}_{f,\omega}^{(n)}) \cdot \boldsymbol{P}, \qquad (14)$$

It is most convenient to choose the permutation matrixes $\boldsymbol{P}$ of the order *n* as matrixes for transformation (14) because reverse matrixes are just calculated for them $\boldsymbol{P}^{-1} = \boldsymbol{P}^T$. In contrast to GGM $\boldsymbol{G}_{f,\omega}^{(n)}$, such matrixes ${}^*\boldsymbol{G}_{f,\omega}^{(n)}$ remain commutative and lose their isomorphism properties.

The most important feature of the generalized of Galois matrixes is that the PRN generators based on linear shift registers with feedback formed by GGM are cryptoresistant about to the BM attack, which is explained in more detail in the next chapter.

Definition. Linear PRN generators will be called generalized if the feedback in the linear shift registers that make up the basis of the generators are formed by generalized matrixes of Galois or Fibonacci.

DOI 10.15588/1607-3274-2019-3-10

The relationships (5) and (7) enable the following representation of the relationship between the generalized Galois and Fibonacci matrixes, including their associated variants (Fig. 7)

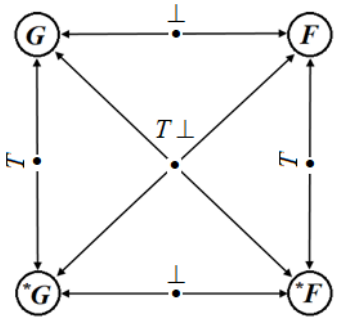

Figure 7 – Transpose operators in multiple Galois and Fibonacci matrixes

All GGMs (as well as KGMs), which will include not only the Galois matrix $\boldsymbol{G}$ itself, but also those formed from $\boldsymbol{G}$ the right-hand transposition of the Fibonacci matrix $\boldsymbol{F}$, as well as the corresponding conjugate matrixes ${}^{*}\boldsymbol{G}$ and ${}^{*}\boldsymbol{F}$, are mutually unambiguously connected by the transformation of similarity (11), as shown in Fig. 8.

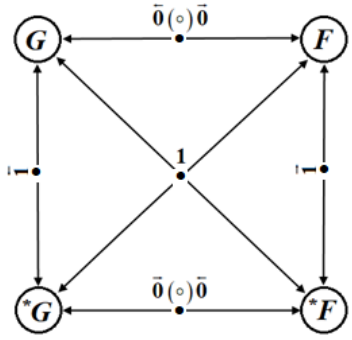

Figure 8 – Stylized display of transformations of the Galois and Fibonacci family of matrixes

Let us consider an example of the synthesis of generalized primitive matrixes and generators of Galois, choosing as an irreducible binary polynomial of the fourth-degree $f_4 = 11111$, which is not primitive, and primitive forming element equal to 111.

The components of similarity transformations include involutive matrixes, i.e. matrixes inverse to themselves, designated by the operator $\mathbf{1}$, as well as matrixes formed by a cyclic shift by a single digit of involutive matrixes rows to the left (matrix $\overleftarrow{\mathbf{1}}$), or the right (matrix $\overrightarrow{\mathbf{1}}$).

The group of involutive matrixes (for example, the fourth-order matrixes were chosen) is represented by the following relations:

$$\mathbf{1} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

$$\overleftarrow{\mathbf{1}} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}; \quad \overrightarrow{\mathbf{1}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \qquad (15)$$

The second group of operators consists of matrixes formed by the cyclic shift of lines of a unit matrix at shift by one digit to the left $\overleftarrow{\boldsymbol{E}}$ and right $\overrightarrow{\boldsymbol{E}}$, represented by the system of operators:

$$\overleftarrow{\boldsymbol{E}} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}; \quad \overrightarrow{\boldsymbol{E}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}. \qquad (16)$$

Let us briefly explain the technology of using operators (15) and (16) in the column of similarity transformations. With the help of involutive operators (15), generated by inverse permutation matrixes, transformations are realized:

$$\begin{matrix} \boldsymbol{G} \\ \boldsymbol{F} \end{matrix} \xleftrightarrow{\mathbf{1}(\circ)\mathbf{1}} \begin{matrix} {}^{*}\boldsymbol{F} \\ {}^{*}\boldsymbol{G} \end{matrix}; \quad \begin{matrix} \boldsymbol{G} \\ \boldsymbol{F} \end{matrix} \xleftrightarrow[\overrightarrow{\mathbf{1}}(\circ)\overrightarrow{\mathbf{1}}]{\overleftarrow{\mathbf{1}}(\circ)\overleftarrow{\mathbf{1}}} \begin{matrix} {}^{*}\boldsymbol{G}; \\ {}^{*}\boldsymbol{F}, \end{matrix}$$

whereas the operators (16) carry out transformations of this type:

$$\begin{matrix} \boldsymbol{G} \\ {}^{*}\boldsymbol{G} \end{matrix} \xleftrightarrow[\overrightarrow{\boldsymbol{E}}(\circ)\overrightarrow{\boldsymbol{E}}]{\overleftarrow{\boldsymbol{E}}(\circ)\overleftarrow{\boldsymbol{E}}} \begin{matrix} \boldsymbol{F} \\ {}^{*}\boldsymbol{F} \end{matrix}.$$

Let us consider an example of the synthesis of generalized primitive matrixes and generators of Galois, choosing as an irreducible binary polynomial of the fourth degree, which is not primitive and primitive SE, equal to 111. The matrices corresponding to the selected parameters are represented by the system (17).

The structural scheme of the generalized basic four-digit of Galois generator, corresponding to GGM $\boldsymbol{G}^{(4)}_{f,7}$, is presented in Fig. 9.

$$\boldsymbol{G}^{(4)}_{f,7} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}; \quad \boldsymbol{F}^{(4)}_{f,7} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix};$$

$$(17)$$

$${}^{*}\boldsymbol{G}^{(4)}_{f,7} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}; \quad {}^{*}\boldsymbol{F}^{(4)}_{f,7} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

Replacing in Fig. 9 the contents of cells of vertical registers of feedback by matrix elements $\boldsymbol{F}^{(4)}_{f,7}$ from the

DOI 10.15588/1607-3274-2019-3-10

system (17), we get the scheme of PRN generator in the configuration of Fibonacci.

Structural scheme of the PRN generator, the conjugate scheme of the considered Galois generator, is presented in Fig. 10. If in the scheme in Fig. 10 to carry out the replacement of contents of cells of feedback registers by matrix elements ${}^{*}\boldsymbol{F}_{f,7}^{(4)}$ from the system (17) we come to the conjugate generator of PRN in a configuration of Fibonacci.

Vertically arranged registers of generators, marked with a symbol at the top, implement the operation of bit multiplication and registers marked with a symbol $\oplus$ – the operation of adding the contents of the register on module 2.

Note that if the generators of PRN, which are shown in Fig. 9, the feedback circuits are "twisted" in a clockwise direction, and in the conjugate generators (Figures 10) – in a counter-clockwise direction. The binary sequences, formed by these generators, are given in Tables 3 and 4.

The general rules of conversion of linear operating systems of a known generator to feedback circuits of any of the remaining generators are shown in Table 2.

Table 2 – Conversion operators of feedback in LFSR-generators of PRN

	$\boldsymbol{G}$	$\boldsymbol{F}$	$^{\bullet}\boldsymbol{G}$	$^{\bullet}\boldsymbol{F}$
$\boldsymbol{G}$	–	$1 \circ 1$	$\circ 1$	$1 \circ$
$\boldsymbol{F}$	$1 \circ 1$	–	$1 \circ$	$\circ 1$
$^{\bullet}\boldsymbol{G}$	$\circ 1$	$1 \circ$	–	$1 \circ 1$
$^{\bullet}\boldsymbol{F}$	$1 \circ$	$\circ 1$	$1 \circ 1$	–

Table 3 – The multiplicative group formed by the PRN generator (Fig. 9 or matrix $\boldsymbol{G}_{f,7}^{(4)}$ from (17))

Degree (or step) k	Deduction ranks			
	4	3	2	1
0	0	0	0	1
1	0	1	1	1
2	1	0	1	0
3	1	0	0	0
4	0	1	1	0
5	1	1	0	1
6	0	0	1	0
7	1	1	1	0
8	1	0	1	1
9	1	1	1	1
10	1	1	0	0
11	0	1	0	1
12	0	1	0	0
13	0	0	1	1
14	1	0	0	1
15	0	0	0	1

Table 4 – The multiplicative group formed by the PRN generator (Fig. 10 or matrix ${}^{*}\boldsymbol{F}_{f,7}^{(4)}$ from (17))

Degree (or step) k	Deduction ranks			
	4	3	2	1
0	0	0	0	1
1	0	1	0	1
2	1	1	1	0
3	0	1	1	0
4	0	1	0	0
5	1	0	1	1
6	1	0	0	0
7	0	0	1	0
8	1	1	1	1
9	0	0	1	1
10	1	0	1	0
11	1	1	0	1
12	1	1	0	0
13	1	0	0	1
14	0	1	1	1
15	0	0	0	1

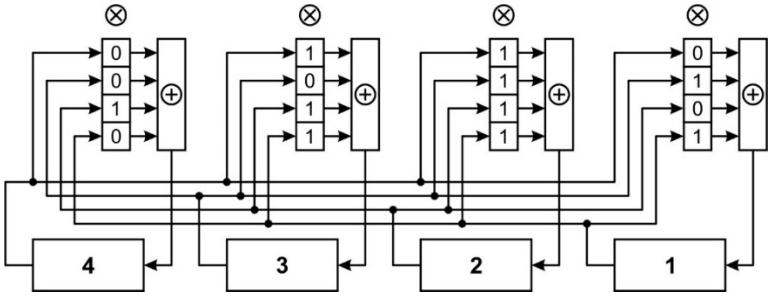

Figure 9 – The structural scheme of the Galois generalized generator $\boldsymbol{G}_{f,7}^{(4)}$ of PRN

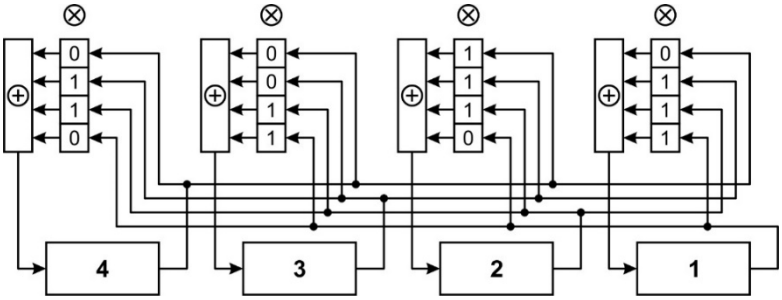

Figure 10 – The structural scheme of the Fibonacci generalized conjugate generator of PRN

DOI 10.15588/1607-3274-2019-3-10

From the comparison of this Tables 1, 3 and 4 we can easily see that the binary sequences formed in the different bits of generators differ only in the order of the cyclic shift and satisfy all the postulates of Golomb [20], as it should be.

The meaning of the term "feedback schemes" of PRN LFSR-generators (by the example of generators, the structural schemes of which are presented in Fig. 4, 5) can be explained by referring to their stylized representation shown in Fig. 11.

Let's pay attention to such peculiarities of the links presented in Fig. 11. Feedback in the registers of basic generators $\boldsymbol{G}$ and $\boldsymbol{F}$ is done in a clockwise direction, while in the registers of conjugate generators ${}^{*}\boldsymbol{G}$ and ${}^{*}\boldsymbol{F}$ – counterclockwise.

Let's clarify the physical meaning of transformation operators in Table 1. The operator $\circ 1$ means that the feedback scheme indicated by the symbol undergoes rotation on 180° relatively vertical axis. The operation $\circ 1$ is similar to the operation of inverse permutation of matrix columns $\boldsymbol{M}$, which is realized by multiplying it by the inverse permutation matrix $\mathbf{1}$ on the right. In turn, the operator $1\circ$ rotates the feedback scheme relative to the horizontal axis. This operation is similar to the operation of inverse permutation of matrix lines $\boldsymbol{M}$, if you multiply it by the inverse permutation matrix $\mathbf{1}$ on the left. The specified transformations of feedback take place in pairs of generators $(\boldsymbol{G}, {}^{*}\boldsymbol{F})$ or $(\boldsymbol{F}, {}^{*}\boldsymbol{G})$. Finally, the operator $1\circ 1$ means that the feedback scheme is rotated on 180° both vertical and horizontal axes. Such transformations of feedback circuits are performed in pairs of generators $(\boldsymbol{G}, \boldsymbol{F})$ or $({}^{*}\boldsymbol{G}, {}^{*}\boldsymbol{F})$.

4 EXPERIMENTS

The attempt to increase the crypto-resistance of LSFR-generators by increasing the order of registers and, accordingly, the degree of PrP used in the feedback circuits, comes up against a known problem [13]. The essence of it consists is as follows. In the open literary sources are given, as a rule, strongly rarefied IP of high orders. The use of such polynomials reduces the cryptographic strength of PRN generators. Besides, classic LFSR-generators are subject to BM attacks, which narrows the scope of their applications.

The cryptographic strength of PRN LFSR generators is the ability of generators to withstand attacks, which allow us to calculate the minimum IP used in the feedback circuit of the shift registers. There are various ways to increase the cryptographic security of PRN generators. To their number concern: an introduction of nonlinear transformations, use of multi-register generators and several others.

Below it will be shown, that the transition from classical LFSR-generators of PRN to generators based on gene-realized matrixes of Galois and Fibonacci leads to the fact, that the algorithm of BM loses the ability to determine the IP is generating the generator of PRN. The reason for the noted feature of such generators is that the series of bits formed by them depends not only on the chosen IP, but also on the primitive constituent element involved in the formation of the feedback chain of the generator.

For experimental confirmation of the stated statement, and the basic theoretical positions concerning properties of matrixes of a feedback, we shall address to results of computer modelling (reduced in Table 5) of the generalized eight-digit Galois generator of PRN. The PrP $f = 100011101$ was chosen as the polynomial forming the feedback loop of the generator.

According to Table 5, the eight forming elements located in the top row of the table is such that each of them leads to the correct solution produced by the BM tester. We will call such forming elements "weak keys" of the flow code, the encrypting gamma of which is formed by the analyzed PRN generator. It is quite easy to eliminate weak keys. For this purpose, it is enough to choose a polynomial that is not primitive.

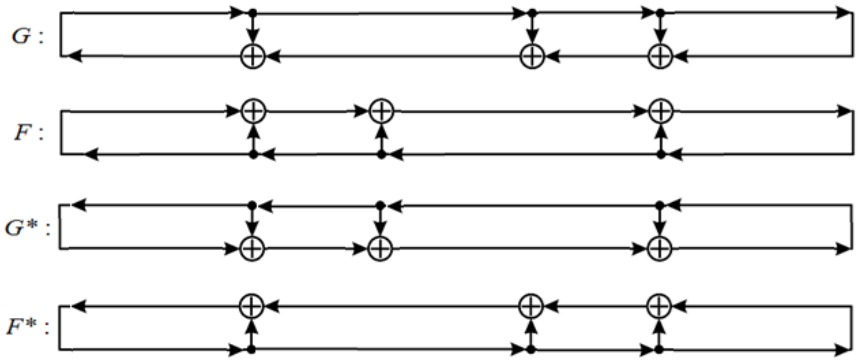

Figure 11 – A stylized representation of feedback in PRN LFSR-generators

DOI 10.15588/1607-3274-2019-3-10

Table 5 – BM tester solutions on many primitive elements of the field generated by the PrP $f = 100011101$

№	**IP: 100011101**	Forming element							
	PrP	1	2	3	4	5	6	7	8
1	100011101	002	004	020	035	114	137	205	235
2	100101011	006	015	024	121	207	302	321	332
3	100101101	113	033	210	130	220	227	300	336
4	101001101	112	123	211	233	307	313	322	325
5	101011111	037	122	110	232	306	312	323	324
6	101100011	036	102	111	133	215	225	237	311
7	101100101	022	103	030	132	214	224	236	310
8	101101001	022	023	030	031	134	135	200	201
9	101110001	011	036	101	107	203	216	314	330
10	110000111	050	064	071	074	077	171	273	345
11	110001101	052	060	143	151	242	274	367	370
12	110101001	043	161	166	172	245	252	260	340
13	111000011	042	160	167	173	244	253	261	341
14	111001111	157	176	262	267	354	360	363	372
15	111100111	062	155	257	343	350	352	356	376
16	111110101	053	061	142	150	243	275	366	371

5 RESULTS

The main research results achieved in this work are as follows. Firstly, the so-called generalized matrixes of Galois and Fibonacci are offered, which essentially expand the set of classical matrixes, involved in the construction of PRN generators in the corresponding configurations. Expansion of a set of matrixes is reached in two ways. In the first of them, the synthesis of matrixes is carried out using not reducible polynomials at all primitive. In classical PRN LSFR generators, only PrP can be used as generators. The second way of construction of matrixes it is supposed that as a forming element of matrixes any element (different from value 10), is a primitive element of the expanded field of Galois generated by the chosen IP can be accepted.

Another one significant scientific result can be formulated as follows. Unlike classical LSFR of PRN generalized generators are not subject to hacking according to BM algorithm. The reason for this property is that an attack on generalized generators can only be successful if, in addition to calculating the generating polynomial, the forming element of the generalized matrix is also determined. This pair of parameters together determine the structure of the feedback chain in the generator.

However, the BM algorithm is not designed to calculate both of these characteristics. This precisely explains the fact that the generalized PRN generators are not subject to BM-attacks and, thus, have a crypto-resistance that exceeds the crypto-resistance of classic PRN generators.

6 DISCUSSION

Visual perception of vectors adjoining the main diagonal of the square in Fig. 6, may give rise to an erroneous assumption. Indeed, the hypothesis that these vectors can be positioned relative to the auxiliary diagonal of the square (as shown, for example, in Fig. 12) may seem consistent.

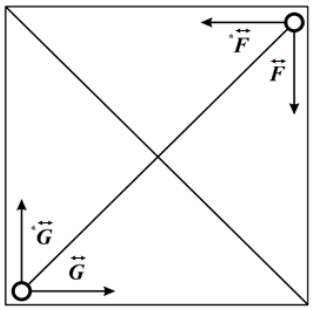

Figure 12 – Alternative arrangement of vectors of forming elements

None of the variants of vectors placement on the auxiliary diagonal of the square can be considered as an alternative to their placement on the main diagonal. The reason for this conclusion is as follows. Let us consider, for example, the classical of Galois matrix represented by expression (2). Having unfolded this matrix relative to the vertical axis, we obtain

$$\vec{G}_{13}^{(4)} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \qquad (18)$$

The PRN sequence, generated by the matrix (18) and ratio (1), is presented in Table 6.

Table 6 – The sequence of generator states (18)

Step	Deduction ranks			
k	4	3	2	1
0	0	0	0	1
1	0	1	0	0
2	0	0	0	1

As it follows from Table 6, the sequence of PRN formed by the generator (18) does not produce a multiplicative group. In addition, the sequence length equal to two is not a divider of the maximum order, which is 15 for the

DOI 10.15588/1607-3274-2019-3-10

considered four-digit generator. Therefore, the variant of arrangement of vectors of forming elements in the vicinity of the auxiliary diagonal (as shown in Fig. 12) is unacceptable for the construction of generating matrices.

CONCLUSIONS

The main problem with the stream ciphers, whose gamma function is generated by LFSR-generators (such as A5 ciphers used for encoding in GSM standard), is the following. The cryptanalyst with the help of the BM algorithm has an opportunity to reconstruct the PrP, using which a one-loop feedback circuit is formed in the LFSR-generator under test. This attack on the LFSR-stream ciphers is easily eliminated. For this purpose, it is enough to refuse from the use of classical registers with single-loop feedback circuits, having replaced them with generalized LFSR with multiline feedback circuits. Such multiline circuits can easily be constructed using generalized Galois, Fibonacci matrices or their associated variants.

The scientific novelty of obtained results is that the unlike classical LFSR-generators of PRN, the scheme of single-circuit feedback in which is defined by a PrP, in the developed generalized LFSR-generators of PRN multi-circuit feedback in registers of the shift are formed not necessarily PrP. Feedback polynomial can be an ordinary IP. However, the element participating together with the IP in the formation of generalized matrixes of Galois and Fibonacci, using which the multi-circuit feedback circuits are created, should be a primitive element of the expanded field of Galois, generated by IR. The main advantage of the proposed PRN generators is that they are free from BM attack.

The practical significance of the obtained results is that the development of purely software algorithms for generating PRN basis on generalized Galois and Fibonacci matrices or their associated variants. Such way of construction, the generators PRN, unlike hardware LFSR-systems, provides the possibility of more flexible control the parameters of the generator, such as not reducible polynomials and primitive forming elements, which gives the basis to recommend the offered algorithms for use in practice.

Prospects for further research are too focused on the generalization of BM algorithm in such a way that to provide the possibility of calculation not only IP of feedback but also the forming element of the generalized matrix of Galois or Fibonacci.

ACKNOWLEDGEMENTS

A group of students from the Electronics Department of the National Aviation University provided a great deal of assistance in this research area. Among them Dmitry Poltoratsky, Konstantin Novikov, Arsen Kovalchuk and others. They have developed numerous programs that have provided the opportunity to conduct various computer experiments to assess the effectiveness of generalized PRN generators under development. The author expresses deep gratitude to all his selfless assistants.

REFERENCES

1. Schneier B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C. New York, John Wiley & Sons, 1996, 758 p. ISBN-13: 978-0471117094
2. Lidl R., Niederreiter H. Finite Fields. Cambridge, University Press, 1996, 407 p. ISBN 0-521-30706-6
3. Knuth D. E. The Art of Computer Programming: Fundamental Algorithms. Massachusetts, England, 1997, 762 p. ISBN 0-201-89683-4
4. Knuth D. E. The Art of Computer Programming: Seminumerical Algorithms. Massachusetts, England, 1997, 832 p. ISBN 0-201-89684-2
5. Peterson W. W., Weldon E. J. Error Correcting Codes MIT Press, Cambridge, 1972, 560 p. ISBN: 9780262160063
6. Chen L., Gong G. Pseudorandom Sequence (Number) Generators, *Communication Systems Security, Appendix A,* 2008, P. 750. ISBN 9781439840368
7. Ivanov M. A., Chugunkov I. V. Theory, application and evaluation of the quality of the pseudorandom generators. Moscow, KUDITZ-OBRAZ, 2003, 240 p. ISBN 5-93378-056-1
8. Fomichev V. M. Discrete mathematics and cryptology. Moscow, Dialogue-MIFI, 2013, 397 p. ISBN 978-5-86404-185-7
9. Shear register with linear feedback [Electronic resource] – Access mode: https://ru.wikipedia.org/wiki/Registr_ shift_with_linear_feedback
10. Linear Feedback Shift Registers [Electronic resource] – Access mode: http://homepage.mac.com/afj/lfsr.html.
11. Random number generation [Electronic resource] – Access mode: http://en.wikipedia.org/wiki/Random_wikin umber_ generation.
12. Beletsky A. Ya., Beletsky E. A. Generators of pseudorandom sequences of Galois, *Electronics and Control Systems*, 2014, No. 4(42), pp. 116–127.
13. Beletsky A. Ya. Synthesis, analysis and cryptographic applications of generalized Galois matrixes – Group monograph, Information technology. Kharkov, 2016, pp. 167–189.
14. Berlekamp E. R. Math. Comp., 1970. V. 24, pp. 713–735.
15. Hardware generator of random numbers GSCH-6. [Electronic resource]. Access mode: http://tegir.ru/ml/k66.html.
16. Anderson R. J. On Fibonacci Keystream Generators [Electronic source]. Access mode: http://www. iacr.org/cryptodb/data/paper.php?pubkey=2963.
17. NIST Statistical Test Suite. [Electronic resource]. Access mode: http://csrc.nist.gov/groups/ST/toolkit/rng/ documentation_software.html.
18. Marsaglia G. DIEHARD Statistical Tests. [Electronic resource]. Access mode: http://stat.fsu.edu/~geo/diehard.html.
19. Rukhin A., Soto J. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Electronic resource]. Access mode: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf.
20. Golomb S. W. Shift register sequences. San Francisco, Holden Day, 1967, 247 p.

Received 23.03.2019.
Accepted 27.06.2019.

DOI 10.15588/1607-3274-2019-3-10

УДК 004.056, 032.817

СИНТЕЗ КРИПТОГРАФИЧЕСКИ СТІЙКИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ УЗАГАЛЬНЕНИХ МАТРИЦЬ ГАЛУА І ФІБОНАЧЧІ

Білецький А. Я. – д-р техн. наук, проф., професор кафедри електроніки Національного авіаційного університету, Україна.

АНОТАЦІЯ

Актуальність. Розглянуто задачу формування узагальнених примітивних матриць Галуа і Фібоначчі будь-якого порядку над полем характеристики 2 для побудови генераторів гамма-функцій криптографически стійких алгоритмів потокового шифрування даних, вільних від атаки Берлекемпа-Мессі.

Метод. Лінійні регістри зсуву з лінійними зворотними зв'язками (РСЛЗЗ) самі по собі є хорошими генераторами псевдовипадкових чисел (ПВЧ), але вони мають небажані властивості, що знижують ефективність їх використання. Для регістрів зсуву довжини n їх внутрішній стан є функцією попередніх вихідних бітів генератора. Навіть якщо схема зворотного зв'язку тримається в секреті, її можна визначити по $2n$ вихідних бітах генератора за допомогою алгоритму Берлекемпа-Мессі, що зменшує криптостійкість генератора псевдовипадкових чисел. Основу одноконтурних ланцюгів зворотного зв'язку, якими охоплені класичні РСЛЗЗ-генератори ПВЧ, складають примітивні поліноми.

Існують різні способи підвищення криптостійкості РСЛЗЗ-генераторів ПВЧ. До їх числа відносяться: введення нелінійних перетворень, використання полірегістрових генераторів (як, наприклад, в алгоритмі поточного шифрування А5) і ряд інших. Перехід від класичних РСЛЗЗ-генераторів до генераторів на основі узагальнених матриць Галуа і Фібоначчі призводить до того, що алгоритм Берлекемпа-Мессі втрачає здатність визначати незвідні поліноми, що породжують багатоконтурні ланцюги зворотного зв'язку в РСЛЗЗ-генераторах ПВЧ. Причина зазначеної особливості полягає в тому, що серія бітів, що породжується узагальненим генератором, стає залежною не лише від обраного незвідного поліному, а й від примітивного елемента, який бере участь у створенні ланцюга зворотного зв'язку генератора.

Результати. Розроблені узагальнені РСЛОС-генератори псевдовипадкових чисел можуть знайти широке застосування в системах шифрування потокової інформації.

Висновки. Статистичні тестування розроблених узагальнених РЗЛЗЗ-генераторів псевдовипадкових чисел, виконані за допомогою пакетів НІСТ СТС та Діхард, підтвердили високу якість генеруються послідовностей. Більш того, генератори виявилися криптографически стійкими до атак Берлекемпа-Мессі. Перспективним є використання цих генераторів для цілей формування ключів великої розмірності, необхідних, наприклад, в протоколах шифрування RSA і в інших додатках. Як напрямки подальших досліджень передбачається розробка узагальнених РЗЛЗЗ-генераторів псевдовипадкових чисел над полем Галуа довільній характеристики.

КЛЮЧОВІ СЛОВА: незвідні поліноми, примітивні матриці, поля Галуа, регістри лінійних зсувів, генератори псевдовипадкових чисел.

УДК 004.056, 032.817

СИНТЕЗ КРИПТОГРАФИЧЕСКИ СТОЙКИХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ОБОБЩЕННЫХ МАТРИЦ ГАЛУА И ФИБОНАЧЧИ

Белецкий А. Я. – д-р техн. наук, проф., профессор кафедры электроники Национального авиационного университета, Украина.

АННОТАЦИЯ

Актуальность. Рассмотрена задача формирования обобщенных примитивных матриц Галуа и Фибоначчи произвольного порядка над полем характеристики 2 для построения генераторов гамма-функций криптографически стойких алгоритмов поточного шифрования данных, свободных от атаки Берлекэмпа-Месси.

Метод. Линейные регистры сдвига с линейными обратными связями (РСЛОС) сами по себе являются хорошими генераторами псевдослучайные чисел (ПСЧ), но они обладают нежелательными свойствами, которые снижают эффективность их использования. Для регистров сдвига длины n их внутреннее состояние является функцией предыдущих выходных битов генератора. Даже если схема обратной связи держится в секрете, ее можно определить по $2n$ выходным битам генератора с помощью алгоритма Берлекэмпа-Месси, что уменьшает криптостойкость генератора псевдослучайных чисел. Основу одноконтурных цепей обратной связи, которыми охвачены классические РСЛОС-генераторы ПСЧ, составляют примитивные полиномы.

Существуют различные способы повышения криптостойкости РСЛОС-генераторов ПСЧ. К их числу относятся: введение нелинейных преобразований, использование полирегистровых генераторов (как, например, в алгоритме поточного шифрования А5) и ряд других. Переход от классических РСЛОС-генераторов к генераторам на основе обобщенных матриц Галуа и Фибоначчи приводит к тому, что алгоритм Берлекэмпа-Месси теряет способность определять неприводимые полиномы, порождающие многоконтурные цепи обратной связи в РСЛОС-генераторах ПСЧ. Причина указанной особенности заключается в том, что серия битов, порождаемая обобщенным генератором, становится зависимой не только от выбранного неприводимого полинома, но и от примитивного элемента, который участвует в создании цепи обратной связи генератора.

Результаты. Разработанные обобщенные РСЛОС-генераторы псевдослучайных чисел могут найти широкое применение в системах поточного шифрования информации.

Выводы. Статистические тестирования разработанных обобщенных РСЛОС-генераторов псевдослучайных чисел, выполненные с помощью пакетов НИСТ СТС и Дихард, подтвердили высокое качество генерируемых последовательностей. Более того, генераторы оказались криптографически стойкими к атакам Берлекэмпа-Месси. Перспективным является использование этих генераторов для целей формирования ключей большой размерности, необходимых, например, в протоколах шифрования RSA и в других приложениях. В качестве направления дальнейших исследований предполагается разработка обобщенных РСЛОС-генераторов псевдослучайных чисел над полем Галуа произвольной характеристики.

DOI 10.15588/1607-3274-2019-3-10

КЛЮЧЕВЫЕ СЛОВА: неприводимые полиномы, примитивные матрицы, поля Галуа, регистры линейных сдвигов, генераторы псевдослучайных чисел.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Schneier B. Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C / B. Schneier. – New York : John Wiley & Sons, 1996. – 758 p. ISBN-13: 978-0471117094
2. Lidl R. Finite Fields / R. Lidl, H. Niederreiter. – Cambridge: University Press, 1996. – 407 p. ISBN 0-521-30706-6
3. Knuth D. E. The Art of Computer Programming: Fundamental Algorithms / D. E. Knuth. – Massachusetts, England, 1997. – 762 p. ISBN 0-201-89683-4
4. Knuth D. E. The Art of Computer Programming: Seminumerical Algorithms. / D. E. Knuth. – Massachusetts, England, 1997. – 832 p. ISBN 0-201-89684-2
5. Peterson W. W. Error Correcting Codes / W. W. Peterson, E. J. Weldon. – MIT Press, Cambridge, 1972. – 560 p. ISBN: 9780262160063
6. Chen L. Pseudorandom Sequence (Number) Generators / L. Chen, G. Gong // Communication Systems Security, Appendix A, 2008. – P. 750. ISBN 9781439840368
7. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательеьностей / М. А. Иванов, И. В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с. ISBN 5-93378-056-1
8. Фомичев В. М. Дискретная математика и криптография / В. М. Фомичев. – М. : Диалог-МИФИ, 2013. – 397 с. ISBN 978-5-86404-185-7
9. Shear register with linear feedback [Electronic resource] – Access mode: https://ru.wikipedia.org/wiki/Registr_ shift_with_linear_feedback
10. Linear Feedback Shift Registers [Electronic resource] – Access mode: http://homepage.mac.com/afj/lfsr.html.
11. Random number generation [Electronic resource] – Access mode: http://en.wikipedia.org/wiki/Random_wikin umber_ generation.
12. Beletsky A. Ya. Generators of pseudorandom sequences of Galois / A. Ya. Beletsky, E. A. Beletsky // Electronics and Control Systems. – 2014. – № 4(42). – P. 116–127.
13. Белецкий А. Я. Синтез, анализ и криптографические применения обобщенных матриц Галуа / А. Я. Белецкий. – Коллективная монография : Информационные технологии. – Харьков, 2016. – С. 167–189.
14. Berlekamp E. R. Math. Comp. / E. R. Berlekamp. – 1970. – V. 24. – P. 713–735.
15. Hardware generator of random numbers GSCH-6. [Electronic resource] – Access mode: http://tegir.ru/ml/k66.html.
16. Anderson R. J. On Fibonacci Keystream Generators [Electronic source]. – Access mode: http://www. iacr.org/cryptodb/data/paper.php?pubkey=2963.
17. NIST Statistical Test Suite. [Electronic resource] – Access mode: http://csrc.nist.gov/groups/ST/toolkit/rng/ documentation_software.html.
18. George Marsaglia, DIEHARD Statistical Tests. [Electronic resource]. – Access mode: http://stat.fsu.edu/~geo/diehard.html.
19. Rukhin A. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / A. Rukhin, J. Soto. [Electronic resource] – Access mode: http://csrc.nist.gov/publications/nistpubs/800–22– rev1a/SP800-22rev1a.pdf.
20. Golomb S. W. Shift register sequences / S. W. Golomb. – San Francisco : Holden Day, 1967. – 247 p.

DOI 10.15588/1607-3274-2019-3-10