Generalized Pseudorandom Generators of the Galois and Fibonacci Sequences

Anatoly Beletsky [0000-0002-3798-8150]

National Aviation University, Kyiv, Ukraine
abelnau@nau.edu.ua

Abstract. The article deals with the formation of generalized primitive matrices of Galois $\boldsymbol{G}$ and Fibonacci $\boldsymbol{F}$ of any order above the field $GF(2)$. The terms "Galois and Fibonacci matrices" are borrowed from the theory of cryptography, in which pseudorandom sequence generators (PRS) on Galois and Fibonacci schemes are widely used. Matrixes $\boldsymbol{G}$ and $\boldsymbol{F}$ software are used to generate the same PRS as the corresponding generators. The generalized matrices include the Galois matrices (as well as the transposition related to them relative to the auxiliary diagonal of the Fibonacci matrix), formed by primitive elements $\theta > 10$ of the field $GF(2)$ over the irreducible polynomials (IP) f_n, which are not necessarily primitive. In the classical Galois and Fibonacci matrices, the constitutive element is $\theta = 10$. Synthesis of matrices $\boldsymbol{G}$ and $\boldsymbol{F}$ is based on the use of IP degree and primitive field elements, generated by polynomials f_n. The statement, according to which the generalized matrix of Galois is isomorphic to their forming elements of the field $GF(2)$. The ways of construction of conjugate ($\boldsymbol{G}^*, \boldsymbol{F}^*$) and inverse ($\bar{\boldsymbol{G}}, \bar{\boldsymbol{F}}$) Galois and Fibonacci matrices are considered. A new effective algorithm for calculating the inverse elements of Galois's extended fields is proposed. The interrelation of the found variety of Galois and Fibonacci matrices is established. The ways of using such matrices in cryptographic applications to solve the problem of building generalized linear PRS generators of the maximum period are discussed.

Keywords: pseudorandom binary sequences, linear feedback shift registers, irreducible polynomials, primitive matrices.

1 Introduction

1.1 Terminological definitions

One of the key problems in the theory and practice of cryptographic protection of information is the problem of formation (generation) of binary pseudorandom sequences (PRS) of maximum length with acceptable statistical characteristics. As a rule, PRS generators are implemented using a linear feedback shift register (LFSR) [1]. Only LFSR with specially selected feedback functions can pass through all non-zero internal states - these are the so-called *maximum period registers*. For LFSR to be the maximum period register, the corresponding feedback polynomial must be a primitive [2].

Each PRS generator can be assigned uniquely to the associated Galois (or Fibonacci) matrices, which calculate the same sequences as those generated by the LFSR

 CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

generators. The terms "Galois and Fibonacci Matrix" are borrowed from the theory of cryptography and coding [3], in which binary PRS generators based on Galois and Fibonacci schemes are used mainly.

The main task of this article is to develop algorithms for constructing PRS generators based on the so-called generalized LFSR and *primitive matrices* (PrM) *of Galois and Fibonacci* $n-$order over the field $GF(2)$. The matrices being synthesized unambiguously determine both the structure of the corresponding generalized $n-$bit LFSR of the maximum period and the PRS of the maximum length ($m-$sequences) formed by them.

1.2 Classic Galois and Fibonacci PRS generators

The classical generator (register) Galois, which example is shown in Fig. 1, compares to each non-zero element of the field $GF(2^n)$ some degree $\theta = 10$ of a minimum primitive element of the field on module PrP f_n.

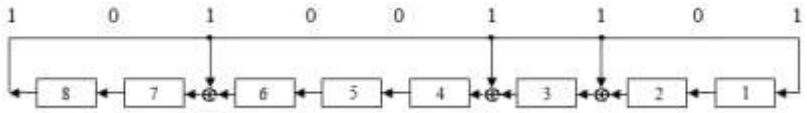

Fig. 1. Structural diagram of the typical Galois generator over the PrP $f_8 = 101001101$

Feedbacks in the classic Galois generators are unambiguously determined by the selected primitive polynom (PrP) f_n and are formed as follows: the responses of each digit of the register arrive at the inputs of the next digits, being for them the excitation functions. Also, the response of the register's highest digit is provided (according to the XOR scheme) to input inputs of those and only those register digits, the numbers of which coincide with the non-zero numbers of PrP monomials. The simplicity of the algorithm of construction (synthesis) of Galois generators, easily traceable in Fig. 1, is a consequence of the accepted variant of LFSR discharge numbers ranking (from right to left), whereas usually the numbering of shift register discharges is performed from left to right [4].

Let's $S(t)-$ the state of Galois register at a discrete point in time t. Denote $\boldsymbol{G}_f^{(n)}-$ the Galois matrix, corresponding to the selected Galois generator. With the help of this matrix forms the same binary sequence as the corresponding PRS. The order n of the matrix $\boldsymbol{G}_f^{(n)}$ coincides with the degree of PrP f_n, which generates the $n-$bit generator Galois. Let's imagine the iterative procedure of changing Galois register states by the ratio

$$S(t) = S(t-1) \cdot \boldsymbol{G}_f^{(n)}, \qquad S(0) = \underbrace{00\ldots01}_{n}, \qquad t = 1, 2, \ldots \tag{1}$$

The vector $S(0)$ highlights the lower row (write it number 1) of the matrix $\boldsymbol{G}$. Consequently, in the bottom line of a matrix $\boldsymbol{G}_f^{(n)}$, it is necessary to write down the value $S(1)$, coinciding with a generating element (GE) $\theta = 10$ of a field $GF(2^n)$ over PrP f_n. Continuing transformation operations (1), we come to the final expression (2) for the classical Galois matrix. The upper line of the matrix $\boldsymbol{G}_f^{(n)}$ is a subtraction of the $(n+1)-$binary vector $\underbrace{10\ldots00}_{n+1}$ on the module f_n.

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

where α_k – the polynomial coefficients, the vector form of which is

$$f_n = 1\alpha_{n-1}\alpha_{n-2}\ldots\alpha_k\ldots\alpha_1 1, \qquad k = 1, 2, \ldots, n-1. \qquad (3)$$

The structure of the matrix (2) predetermines the general rule of synthesis of classical Galois matrices, the essence of which is as follows. In the right corner of the bottom line of the matrix $\boldsymbol{G}_f^{(n)}$ being synthesized, we will place the smallest primitive element $\theta = 10$ of the Galois field generated by PrP f_n. The subsequent matrix rows are formed from the previous rows as a result of their shift by one digit to the left. The digits released on the right are filled with zeros. If the unit of the row goes beyond the left border matrix $\boldsymbol{G}_f^{(n)}$, then this row is reduced to the remainder of the module f_n, resulting in it also becomes a $n-$bit. The formulated rule is called *the rule of synthesis of KMG* (classical Galois matrices).

In addition to the classic Galois matrices (2), you can also enter Fibonacci matrices $\boldsymbol{F}_f^{(n)}$ over PrP f_n that correspond to linear shift registers in the Fibonacci scheme (linear generators of pseudorandom Fibonacci sequences). Fibonacci matrices are mutually unambiguously related to Galois matrices by the right-hand transposition operator (transposition relative to the auxiliary diagonal) [5]

$$\boldsymbol{F} \xleftrightarrow{\perp} \boldsymbol{G}. \qquad (4)$$

Transposition, relative to the main matrix diagonal, indicated by the symbol T, will be called a left-hand inversion. According to (4) we have

$$\boldsymbol{F}_{f}^{(n)}=\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & \alpha_1 \\ 0 & 1 & \cdots & 0 & 0 & \alpha_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & \alpha_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & \alpha_{n-1} \end{pmatrix}. \quad (5)$$

The Fibonacci PRS generator, corresponding to the matrix (5) for PrP $f_8 = 101001101$, is shown in Fig. 2.

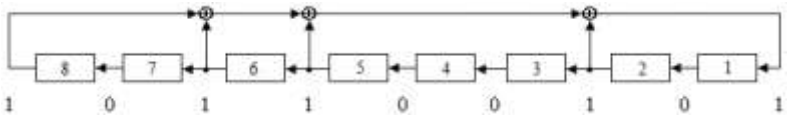

Fig. 2. Structural diagram of the classic Fibonacci generator over the PrP $f_8 = 101001101$

2 Expansion of the family of classic PRS generators

2.1 Conjugate generators Galois and Fibonacci

In group theory, an element a^* of a group A is a *conjugate* element a of the same group [], if there is an element $z \in A$ such that

$$a^* = z^{-1} \cdot a \cdot z \,. \quad (6)$$

Similar to (6), we will introduce a formal definition of the conjugate Galois and Fibonacci matrices by form

$$\boldsymbol{M}^* = \boldsymbol{P}^{-1} \cdot \boldsymbol{M} \cdot \boldsymbol{P} \,, \quad (7)$$

where $\boldsymbol{M}$ there is one of the matrices $\boldsymbol{G}$ or $\boldsymbol{F}$, and $\boldsymbol{P}$ – an unborn matrix of the same order as the matrix $\boldsymbol{M}$.

As follows from the ratio (7), they are matrices $\boldsymbol{M}^*$ similar to $\boldsymbol{M}$, preserving the basic properties of matrices $\boldsymbol{M}$. The matrix $\boldsymbol{P}$ is the inverse permutation matrix (IPM), which is conventionally designated by a numeral **1**. Below is an example of the fourth- order IPM

$$\mathbf{1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

In this way

$$\begin{aligned} \boldsymbol{G}^* &= \mathbf{1} \cdot \boldsymbol{G} \cdot \mathbf{1}; \qquad \boldsymbol{G} = \mathbf{1} \cdot \boldsymbol{G}^* \cdot \mathbf{1}; \\ \boldsymbol{F}^* &= \mathbf{1} \cdot \boldsymbol{F} \cdot \mathbf{1}; \qquad \boldsymbol{F} = \mathbf{1} \cdot \boldsymbol{F}^* \cdot \mathbf{1}. \end{aligned} \tag{8}$$

Multiplication square matrix by the IP matrix $\boldsymbol{M}$ on the left is equivalent to an inversion of matrix rows $\boldsymbol{M}$, and on the right – a reversal of columns of this matrix. So it follows that the conjugate matrix $\boldsymbol{M}^*$ is formed from the matrix $\boldsymbol{M}$ as a result of joint inversions of its rows and columns equivalent to the joint operations of left- and right-side transposition, i.e. $\boldsymbol{M}^* = \boldsymbol{M}^{T\perp} = \boldsymbol{M}^{\perp T}$.

The general forms of the classical conjugate matrices of Galois and Fibonacci, in which the indices f and n are omitted for simplicity and, according to (2), (4) and (8), look like:

$$\boldsymbol{G}^* = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & \alpha_1 & \alpha_2 & \cdots & \alpha_{n-2} & \alpha_{n-1} \end{pmatrix}, \tag{9}$$

$$\boldsymbol{F}^* = \begin{pmatrix} \alpha_{n-1} & 1 & 0 & \cdots & 0 & 0 \\ \alpha_{n-2} & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_2 & 0 & 0 & \cdots & 1 & 0 \\ \alpha_1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{10}$$

Based on the relations (9) and (10), we come to the structural schemes of the conjugate generators Galois and Fibonacci, which are presented in Fig. 3 and 4.

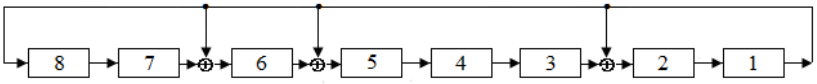

Fig. 3. Structural diagram of the mating Galois generator over the PrP $f_8 = 101001101$

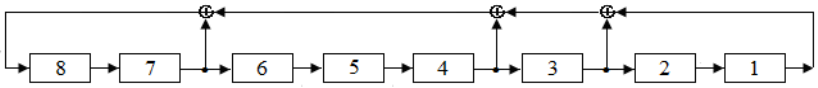

Fig. 4. Structural diagram of the mating Fibonacci generator over the PrP $f_8 = 101001101$

2.2 Galois and Fibonacci inverse generators

Let us explain the way of calculating the inverse matrixes of Galois $\bar{G}$ [6, 7], to which we come, solving the equation

$$\boldsymbol{G} \cdot \bar{\boldsymbol{G}} = \boldsymbol{E}, \tag{11}$$

where $\boldsymbol{E}$ – the single matrix is.

For example, for the fourth-order matrices, according to (2) and (11), we have

$$\begin{pmatrix} \alpha_3 & \alpha_2 & \alpha_1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{12}$$

For simplicity, the unknown components of the reverse matrix are represented in (12) by their indices. Summarizing the solution of the matrix equation (12), we come to the classical inverse matrix of the Galois $n-$order above the PrP f_n:

$$\bar{\boldsymbol{G}} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_2 & \alpha_1 \end{pmatrix}, \tag{13}$$

which unequivocally defines the structural scheme of the PRS generator generated by the selected PrP $f_8 = 101001101$

Fig. 5. Galois reverse oscillator diagram over the PrP $f_8 = 101001101$

Using the relations (4) and (8), we can easily find both the inverse Fibonacci matrix $\bar{F}$ and the conjugate matrices $\bar{G}^*$, $\bar{F}^*$ and then the corresponding structural schemes of PRS generators.

2.3 Relationship between classical Galois and Fibonacci generators

From the comparison of Galois (4) and Fibonacci (6) matrices, as well as their conjugate variants (9) and (10), we come to the operators of a transformation of one of the known matrices into any other matrix.

Table 1: Matrix conversion operators

	G	F	G^*	F^*
G	—	⊥	T ⊥	T
F	⊥	—	T	T ⊥
G^*	T ⊥	T	—	⊥
F^*	T	T ⊥	⊥	—

From the analysis of the structural schemes of simple generators over PrP $f_8 = 101001101$, shown in Figs. 1 - 4, we come to the general rules of change, summarized in Table 2, the schemes of linear feedback of the known PRS generator over a given f to the schemes of any of the remaining three types of generators. In contrast to Table 1, in which the symbols G, F, G^* and F^* the primitive matrixes of PRS generators are designated, in Table 2 the same symbols conventionally denote the scheme of feedback in the corresponding generators.

Table 2. Operators of the feedback schemes

	G	F	G^*	F^*
G	—	1 ∘ 1	∘1	1 ∘
F	1 ∘ 1	—	1 ∘	∘1
G^*	∘1	1 ∘	—	1 ∘ 1
F^*	1 ∘	∘1	1 ∘ 1	—

The meaning of the term "feedback scheme" in G, F, G^* or F^* of PRS generators can be explained by referring to their stylized graphical representation shown in Fig. 6. Let's pay attention to such peculiarities of feedback. If the generators G and F feedback are clockwise, the generators G^* and F^* are counter-clockwise.

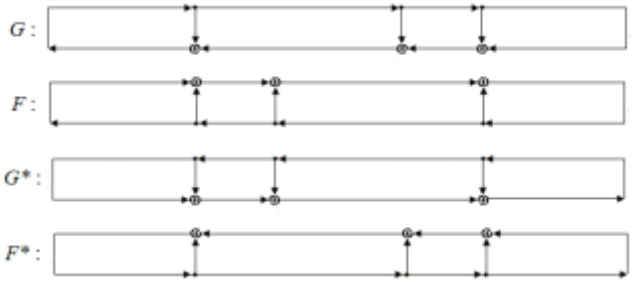

Fig. 6. A stylized representation of feedback schemes in PRS generators

Let's specify the physical meaning of transformation operators in Table 2. The operator $\circ 1$ means that the feedback scheme marked with the symbol $\circ$ undergoes rotation on 180° a relatively vertical axis. Such transformations occur, as it follows from Fig. 6, in pairs of generators $(\boldsymbol{G}, \boldsymbol{G}^*)$ or $(\boldsymbol{F}, \boldsymbol{F}^*)$. The operation $\circ 1$ is similar to the process of inverse shifting of matrix columns $\boldsymbol{M}$, which is realized by multiplying it by the IPM on the right side. The operator $1\circ$ rotates the feedback scheme relative to the horizontal axis. Thus, the process is similar to the operation $1\circ$ of inverse permutation of matrix rows, if you multiply it by IPM on the left side. The specified conversions 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 both vertical and horizontal axes rotate the feedback scheme. Such transformations of feedback circuits are performed in pairs of generators $(\boldsymbol{G}, \boldsymbol{F})$ or $(\boldsymbol{G}^*, \boldsymbol{F}^*)$.

The feedback diagrams in reverse PRS generators are formed as a result of turning on the relatively $180°$ vertical axis of the charts shown, as an example, in Fig. 6 for the generators, generated by the PrP $f_8 = 101001101$. The way of formation of matrixes of a full set of LFSR generators of PRS (and among them - classical, conjugate, and return generators) is shown in Fig. 7.

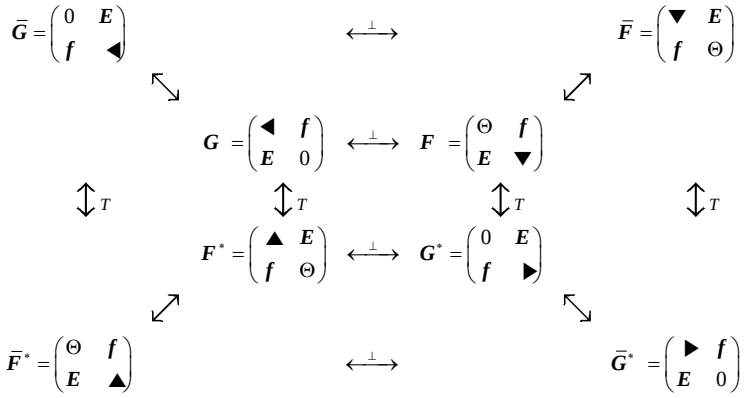

Fig. 7. The interrelation of classic LFSR matrixes of PRS generators

In this figure, a pair of symbols (f ◂) define a binary vector (row or column), in which f is replaced by the digit 1, and a shaded triangle - a sequence of polynomial coefficients α_k, and the top of the triangle indicate the location of the senior factor. For example, f ◂ it means a vector $1\alpha_{n-1}\alpha_{n-2}\ldots\alpha_1$, while f ▸ it implies a vector $1\alpha_1\alpha_2\ldots\alpha_{n-1}$. Besides, symbols **0** and Θ also suggest zero vector-column and vector-line, respectively. And finally, the symbols $\overline{T\perp}$ indicate not only the two-way transposition but also the inversion of the polynomial coefficients α_k.

3 Research methods

3.1 Generalized generators Galois and Fibonacci

Based on the construction of generalized generators of Galois (as well as Fibonacci), we will put the generalized matrices corresponding to them.

Definition. *The generalized matrix of Galois* (GMG) will be called the matrix, formed by the primitive element $\theta > 10$ of the field $GF(2^n)$ over the IP f_n, which is not necessarily primitive.

We come to the algorithm of GMG construction, expanding the Rule of synthesis of KMG, formulated in paragraph 1.2. The essence of the algorithm of GMG formation is as follows. Let's choose some primitive element $\theta > 10$ of the field $GF(2^n)$ generated by the IP f_n, which we will place in the right corner of the bottom line of the synthesized matrix $\boldsymbol{G}_f^{(n)}$. Subsequent matrix rows (in the direction from bottom to top) are formed from the previous rows as a result of their shift by one digit to the left. The numbers released on the right are filled with zeros. If a higher unit shifted, row goes beyond the left border of the matrix. This row is reduced to the remainder of the module f_n, which also results in it becoming a digit. The row returns to matrix boundaries, and the process of filling in its rows continues as described above. The formulated rule is called the *rule of GMG synthesis*.

$$\boldsymbol{G} = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}; \qquad \boldsymbol{F} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$\boldsymbol{G}^* = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}; \qquad \boldsymbol{F}^* = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \tag{14}$$

Let's consider an example of the synthesis of generalized primitive matrices and LFSR generators of PRS, choosing as an irreducible binary polynomial $f_n = 11111$ of the fourth degree, which is not primitive, and primitive forming element. Matrixes corresponding to the selected parameters are represented by expressions (14).

Let's $h_{i,j}$ denote the element of $i-$th row and $j-$th column, $i, j = \overline{1, n}$, any of the matrices $\boldsymbol{G}, \boldsymbol{F}, \boldsymbol{G}^*$ or $\boldsymbol{F}^*$ underlying the construction of LFSR with generalized linear relations. The state of the $k-$th discharge LFSR $s_k(t+1)$ at the moment $t+1$ coincides with the excitation function of this discharge $\nu_k(t)$ at the moment t and is determined by the expression:

$$s_k(t+1) = \nu_k(t) = \bigoplus_{i=1}^{n} h_{i,k} \cdot s_i(t) .$$

The structural scheme of the generalized primary four-digit Galois generator is shown in Fig. 8. Vertically arranged generator records marked with a symbol $\otimes$ at the top implement the digit multiplication operation, and registers marked with a symbol $\oplus-$ addition operation on module 2.

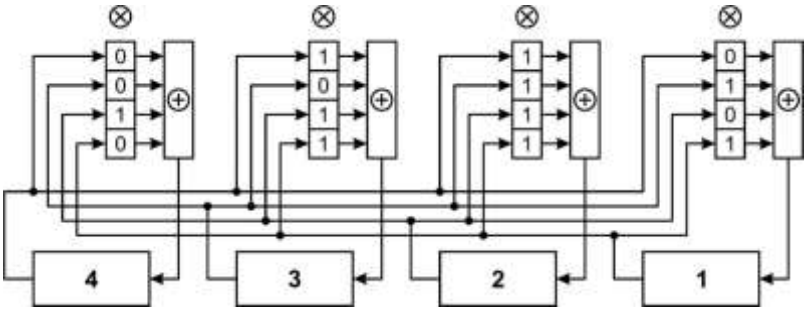

Fig. 8. Structural scheme of generalized PRS Galois/Fibonacci generators

Galois generator (Fig. 8) is converted into a Fibonacci generator by replacing the register contents with the system matrix $\boldsymbol{F}$ (14). If we place matrix column elements in the multiplication registers $\boldsymbol{G}^*$ or $\boldsymbol{F}^*$ from the system (14), we get a paired generator in the Galois or Fibonacci configuration. The scheme of the matched Galois/Fibonacci PRS generator is shown in Fig. 9.

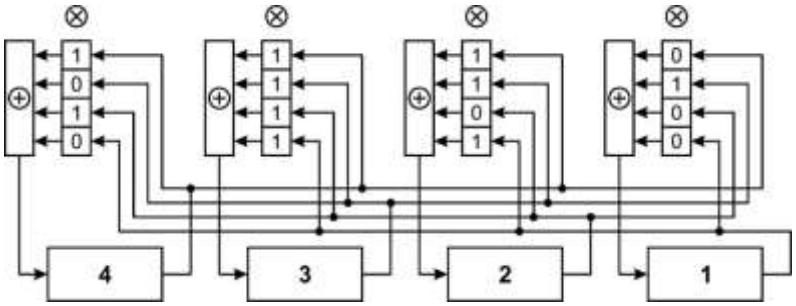

Fig. 9. Structural scheme of generalized conjugate generators of PRS Galois/Fibonacci

3.2 Isomorphism of Galois matrixes

From the theory of polynomials is known, that multiplication of an arbitrary degree k polynomial $\omega_k(x)$ by x the equivalent of a shift of a polynomial by one digit to the left and, consequently, an increase by 1 degree of a polynomial

$$x \cdot \omega_k(x) \to \omega_{k+1}(x). \tag{15}$$

Using the ratio (15) and taking into account the way OMG is formed, let's write down the chain of transformations:

$$\boldsymbol{G}_{f,\omega}^{(n)} \Rightarrow \begin{pmatrix} x^{n-1} \cdot \omega \\ x^{n-2} \cdot \omega \\ \cdots \\ x \cdot \omega \\ \omega \end{pmatrix} \bmod f_n = \omega \cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} \bmod f_n . \tag{16}$$

Elements of the right vector-column in the ratio (16) are monomers, which, being represented in the binary form, turn the vector-column into a single matrix, i.e.

$$\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = \boldsymbol{E}, \tag{17}$$

which makes it possible to formulate the following

The postulate. The generalized binary matrix of Galois $\boldsymbol{G}_{f,\omega}^{(n)}$ isomorphous to its forming element ω

$$\boldsymbol{G}_{f,\omega}^{(n)} \leftrightarrow \omega . \tag{18}$$

Therefore, according to the expressions (16) and (17), there is a mutually unambiguous correspondence (*isomorphism*) between GMG $\boldsymbol{G}_{f,\omega}^{(n)}$ and its forming element ω, which is displayed by the ratio (18). Also, it is easy to establish that isomorphism (18) leads to such consequences.

Consequence 1. The generalized Galois matrices $\boldsymbol{G}_{f,\omega}^{(n)}$ are nondegenerate for all parameters f_n and ω are linearly independent rows of matrices, as can be readily ascertained from the ratio (17).

Consequence 2. To elevate the matrix $\boldsymbol{G}_{f,\omega}^{(n)}$ in degree k, it is enough to calculate forming elements $\omega_k = \omega^k (\mathrm{mod}\, f_n)$ and then calculate matrix $\boldsymbol{G}_{f,\omega_k}^{(n)}$.

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

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

Consequence 5. Matrixes $\boldsymbol{G}_{f,\omega_1}^{(n)}$ and $\boldsymbol{G}_{f,\omega_2}^{(n)}$, $\omega_1 \neq \omega_2$, are commutative, because commutatively the product of the elements forming them.

Consequence 6. Algebraic transformations over the totality of Galois matrices are isomorphic to the same transformations over the forming elements of matrices.

Consequence 7. GMG $\bar{\boldsymbol{G}}_{f,\omega}^{(n)}$, inverse matrix $\boldsymbol{G}_{f,\omega}^{(n)}$, can be constructed according to the rule of synthesis of generalized Galois matrices, formulated in item 3.1. The forming element of the matrix $\bar{\boldsymbol{G}}_{f,\omega}^{(n)}$ is the inverse element $\bar{\omega}$ of the forming element matrix $\boldsymbol{G}_{f,\omega}^{(n)}$.

Consequence 8. A lot of GMGs can be expanded by introducing similar Galois matrices $\hat{\boldsymbol{G}}_{f,\omega}^{(n)}$ defined by the

$$\hat{\boldsymbol{G}}_{f,\omega}^{(n)} = \boldsymbol{P}^{-1} \cdot \boldsymbol{G}_{f,\omega}^{(n)} \cdot \boldsymbol{P} . \tag{19}$$

As $\boldsymbol{P}-$ matrices in transformation (19), it is preferable to consider permutation matrices of the $n-$order, because, for them, the inverse matrices are simply enough calculated, namely $\boldsymbol{P}^{-1} = \boldsymbol{P}^{-T}$. Unlike the GMG $\boldsymbol{G}_{f,\omega}^{(n)}$ matrixes $\hat{\boldsymbol{G}}_{f,\omega}^{(n)}$, they remain commutative and lose their isomorphism property. This feature of such matrices of Galois, first of all, provides an opportunity to build on their one-way basis functions, widely used in cryptography and other applications. And, secondly, it is possible to construct one-sided functions based on them, which are widely used in cryptography and other applications, LFSR generators of PRS are free from Berlekemp-Messi attack.

The complete set of generalized Galois and Fibonacci matrices can be represented in the form of a graph (Fig. 10), similar to the chart of many classical matrices shown in Fig. 7.

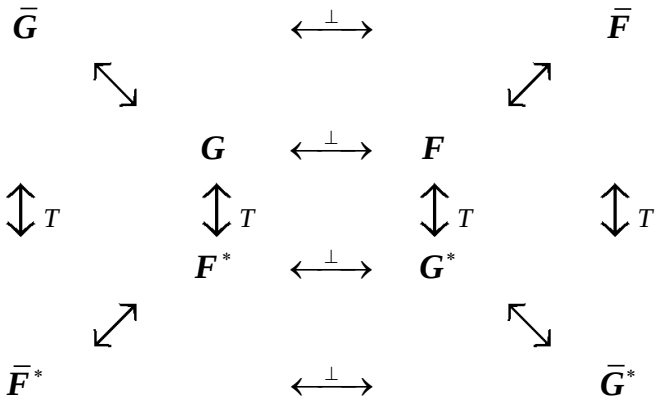

Fig. 10. The interrelation of generalized matrixes of LFSR generators of PRS

The location of the vectors of FE generalized matrices, all of them for simplicity, will be called Galois matrices, is shown in Fig. 11. The vector arrows are directed towards the higher classes of the forming elements.

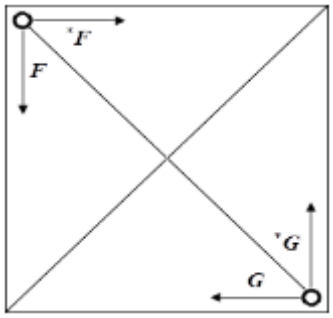

Fig. 11. Conditional and graphical representation of vectors of FE matrices of Galois

3.3 Calculating inverse elements of the Galois field

The generalized matrixes located in the corners of the outer contour of the graph in Fig. 10 are calculated elementary. In fact, the arbitrary GMG $\boldsymbol{G}_{f,\omega}^{(n)}$, including the inverse matrix $\bar{\boldsymbol{G}}_{f,\omega}^{(n)}$, is unambiguously determined by its FE $\bar{\omega}$. Therefore, for the construction of GMG $\bar{\boldsymbol{G}}_{f,\omega}^{(n)}$, it is necessary to calculate the element $\bar{\omega}$ and then, using the rule of synthesis GMG, to make a matrix $\bar{\boldsymbol{G}}_{f,\bar{\omega}}^{(n)}$. The remaining matrices of the

external contour of the graph are connected with the operators of left- and right-hand transposition.

The main problem in the designated calculation chain is the definition of the element $\bar{\omega}$. There are different ways of finding the inverse elements of the Galois field [7, 8]. Among them, the most frequently used method is based on the extended Euclidian algorithm [9-11].

Below is an alternative approach to calculation $\bar{\omega}$ — it is more straightforward in the program implementation than the Euclid algorithm. The essence of the alternative algorithm is explained in Table 3, in which it is indicated: $n-$ the degree of IP f; $k-$ step of iteration; $L_n = (2^n - 1) -$ the order of the multiplicative group of the field $GF(2^n)$, generated by IP f_n; $VI-$ vector of initialization. Writing $\Delta_k = (a)_f$ means the calculation of the residual Δ value a of the module f_n on the $k-$th iteration step.

Table 3: Calculation procedure of extended inverse elements of the Galois field

n	L_n	k	Residue		n	L_n	k	Residue
VI		1	$\Delta_1 = (\omega^2)_f$		6	63	8	$\Delta_8 = (\Delta_7 \cdot \omega)_f$
3	7	2	$\Delta_2 = (\Delta_1 \cdot \omega)_f$				9	$\Delta_9 = (\Delta_8^2)_f$
		3	$\Delta_3 = (\Delta_2^2)_f$		7	127	10	$\Delta_{10} = (\Delta_9 \cdot \omega)_f$
4	15	4	$\Delta_4 = (\Delta_3 \cdot \omega)_f$				11	$\Delta_{11} = (\Delta_{10}^2)_f$
		5	$\Delta_5 = (\Delta_4^2)_f$		8	255	12	$\Delta_{12} = (\Delta_{11} \cdot \omega)_f$
5	31	6	$\Delta_6 = (\Delta_5 \cdot \omega)_f$				13	$\Delta_{13} = (\Delta_{12}^2)_f$
		7	$\Delta_7 = (\Delta_6^2)_f$		• • •			

It is known, that for any non-zero field element the equality of

$$(\omega^{L_n})_f = (\omega^{2^n - 1})_f = 1. \tag{20}$$

Introducing (20) in the form

$$(\omega \cdot (\omega^{2^n - 2}))_f = (\omega \cdot \bar{\omega})_f = 1,$$

we'll get

$$\bar{\omega} = (\omega^{2^n - 2})_f. \tag{21}$$

According to formula (21), the inverse element $\bar{\omega}$ is determined by residue Δ an even degree $2^n - 2$ of the field element ω from the IP module f_n. These residues are placed in odd lines in Table 3.

Based on Table 3, we quickly come to the expression for the number of iterations k, performed when calculating the inverse field elements $\bar{\omega}$ over the IP degree n

$$k = 2n - 3.$$

Let's consider a numerical example. Suppose $n = 4$, $f = 10011$ and $\omega = 1101$. According to Table 3, the first step is to perform the following calculations

$$\Delta_1 = (\omega^2)_f = (1101 \cdot 1101)_f = (1010001)_{10011} = 1110.$$

For the next step, we find

$$\Delta_2 = (\Delta_1 \cdot \omega)_f = (1110 \cdot 1101)_f = (1000110)_{10011} = 1010;$$
$$\Delta_3 = (\Delta_2^2)_f = (1010 \cdot 1010)_f = (1000100)_{10011} = 1000;$$
$$\Delta_4 = (\Delta_3 \cdot \omega)_f = (1000 \cdot 1101)_f = (1101000)_{10011} = 10;$$
$$\Delta_5 = (\Delta_4^2)_f = (10 \cdot 10)_f = 100.$$

The residue $\Delta_5 = 100$ is the opposite of the subtraction element $\omega = 1101$.

The vector of initialization starts $VI = \Delta_1 = (\omega^2)_f$ the computational process (according to Table 3). The further procedure consists $n - 2$ cycles, each of which includes two iteration steps. We find the auxiliary vector $\Delta_{2(n-2)}$ as the first one (on the even step k), and the second one (on the odd stage of iteration) — the inverse element $\overline{\omega} = \Delta_{2n-3}$.

4 Discussion

Visual perception of the FE vectors presented in Fig. 11 can create an assumption about the possible existence of an alternative set of matrices, the vectors of forming elements which are located in the vicinity of the vertices of the auxiliary diagonal of the square (fig. 12).

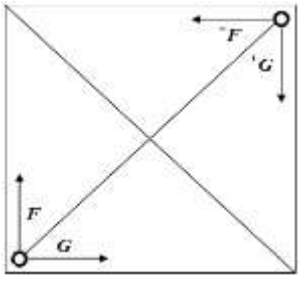

Fig. 12. Alternative arrangement of vectors FE matrices of Galois

However, this is a false assumption, as none of the FE $\omega \geq 10$ fields $GF(2^n)$ above the IP f_n leads to the formation of a primitive Galois matrix. And this excludes the possibility of building PRS generators of the maximum period [12-14].

5 Conclusions

The main scientific results of this study include the following:

1. Algorithms for the synthesis of the so-called generalized Galois matrices have been developed. Generalized matrices are those formed by primitive elements $\theta > 10$ over IP f_n, which are not necessarily primitive. In addition to Galois matrices, many generalized matrices also include other matrices (Fibonacci, conjugate, and backward matrixes). All the above matrices are interconnected by a set of linear transformations (left- and right-hand transposition). The generalized matrixes of Galois (as well as classical ones) are intended for the construction of LFSR generators of PRS of the maximum period. The advantage of the widespread PRS generators is that they, unlike the classic LFSR generators, are free from the Berlekemp-Messi attack.

2. The postulate, according to which the generalized Galois matrices appear to be isomorphic elements forming them, is formulated and confirmed [15, 16].

3. A new algorithm for calculating the inverse field elements $GF(2^n)$ over IP f_n is proposed, which is simpler in comparison with the widely used generalized Euclidean algorithm.

References

1. Stream Ciphers, 1997, http//www/ssl/stu/neva/ru/psw/crypto/potok/str_ciph.htm.
2. Ivanov V.A., Chugunkov I.V.: Theory, Appl. and Evaluation of the Quality of Pseudorandom Sequences. KUDIC-OBRAZ, Moscow, 2003.
3. Asoskov A., Ivanov A., Mirskiy A. Stream ciphers. KUDIC-OBRAZ, Moscow, 2003.
4. Beletsky A., Ya. Generators of pseudo random sequences of Galois, Electronics and Control Systems, 4(42), pp. 116-127 (2014).
5. Mullozhanov R.V. Generalized transposition of matrices and linear structure of large-scale systems, http://nbuv.gov.ua/j-pdf/dnanu2009106.pdf
6. Lidl R., Niederreiter H. Introduction to finite fields and their application, Cambridge University, Press, 1994.
7. Smart, N.: Cryptography: An Introduction, 3rd ed. McGraw-Hill College, 2013.
8. Aschbacher M. Finite Group Theory, 2nd ed. Cambridge, England: Cambridge University Press, 2000.
9. Van der Warden, B., L.: Mathematics Statistic. Moscow, IL, 1960.
10. Pankratyev E., V.: Elements of computer algebra. Moscow, 2007.
11. I. Gorbenko, A. Kuznetsov, Y. Gorbenko et al, Random S-Boxes Generation Methods for Symmetric Cryptography, IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 947-950.
12. Mohammed Abdul Samad AL-Khatib, Auqib Hamid Lone, Acoustic Lightweight Pseudo Random Number Generator based on Cryptographically Secure LFSR, International Jour-

nal of Computer Network and Information Security (IJCNIS), Vol.10, №2, pp. 38-45, 2018.
13. Zodpe H., Sapkal A. “FPGA-Based High-Performance Computing Platform for Cryptanalysis of AES Algorithm”, Advances in Intelligent Systems and Computing, Springer, vol. 1025, pp. 637-646, 2020.
14. Hu Z., Gnatyuk S., Okhrimenko T., Tynymbayev S. and Iavich M. High-speed and secure PRNG for cryptographic applications, International Journal of Computer Network and Information Security, Issue 12 (3), pp. 1-10, 2020.
15. Yeoh, W., Teh, J. S. and Sazali, M. I. “μ^2: A lightweight block cipher”, Lecture Notes in Electrical Engineering, vol. 603, pp. 281-290, 2020, doi:10.1007/978-981-15-0058-9_27
16. Liu H., Kadir A. and Xu C. “Cryptanalysis and constructing S-box based on chaotic map and backtracking”, Applied Mathematics and Computation, vol. 376, 125153, 2020, doi:10.1016/j.amc.2020.125153