MATHEMATICAL MODELING OF PROCESSES AND SYSTEMS

UDC 511.512 (045)

A. Ya. Beletsky,
E. A. Beletsky

GENERATORS OF PSEUDO RANDOM SEQUENCES OF GALOIS

Department of Electronics National Aviation University, Kyiv, Ukraine
E-mails: [1]abelnau@ukr.net, [2]ebeletskiy@gmail.com

***Abstract*—*The questions of Galois and Fibonacci random size n primitive matrices creation over the simple field $GF(p)$ is considered. The synthesis is based on usage of irreducible polynomial f_n of degree n and primitive elements of extended field $GF(p^n)$, which is generated by polynomial f_n. The ways of linked primitive matrices of Galois and Fibonacci are offered. The possibilities of such matrices application are described.*

Index Terms—Irreducible and primitive polynomials; primitive matrices; linear shift registers; generators of Galois sequences.

I. INTRODUCTION

There is a problem of binary pseudo random sequences (PRS) creation in theory and practice of cryptographic security system for sequences of maximal length $L = 2^n - 1$, with acceptable static characteristics. Usually PRS generators implement by means of linear shift registers (LSR) of maximal period with linear feedbacks [1]. We will extend the concept of PRS in these articles, assuming each digit (memory cell) can reside in of states $s \in GF(p)$, $p > 2$. Let's call such registers as "generalized linear shift register".

The main goal of research is an invention of algorithm for generalized matrix Galois and Fibonacci of order n over field $GF(p)$, $p \geq 2$, which is unambiguously define the structure of corresponding $n-$digit LSR of maximal period as long as PRS Galois created on their basis.

II. CONCEPTUAL-TERMINOLOGICAL DEFINITIONS

The main terms we need to clarify are: "primitive polynomial" and "primitive matrix". The definition for "linked Galois and Fibonacci matrices", "generalized generators of pseudo random Galois sequences" and others would be given later.

In Galois field theory which is the basis of noiseless coding, cryptography and creation of modern electronic circuits of data transfer, the crucial concept is irreducible polynomial (IP). A polynomial of one variable x degree n

$$f_n(x) = \sum_{i=0}^{n} u_{n-i} x^{n-i}, \quad u_i \in GF(p), \quad u_n = 1, \qquad (1)$$

is called *irreducible over field* $GF(p)$, if it can't be divided on any polynomial of less degree over the given field.

Polynomial (1) is written in so called *algebraic form*. It is also can be presented as a sequence of its coefficient

$$f_n = u_n u_{n-1} \ldots u_i \ldots u_1 u_0,$$

which we call as *vector form IP.*

The most important property of final extended fields of Galois $GF(p^n)$, which are generated by IP f_n and actually of simple fields $GF(p)$, is for each of its non-zero element g there should be an inverse element g^{-1}, which is $g\,g^{-1} (\mathrm{mod}\, f_n) = 1$. The described condition is true only if p is a prime number. From which it is follows the property p of Galois field, as simple and for extended $GF(p)$ should be a prime number.

For convenience, let's introduce for the polynomials a notion, which is called the *characteristic p of polynomial* f_n, which coinciding with characteristic p of simple Galois field.

The set IP contains important for cryptographic applications, informatics, electronics and other branches of science and technique, subset of so call *primitive polynomial* (PrP). There are different variants of "primitive polynomial" definition.

In algebra, numbers theory and Galois fields [2] irreducible polynomial f_n of degree n is called primitive over $GF(p)$ in the only case if it is – normalized polynomial, for which f_n is not equal to zero and

$$\mathrm{ord}\,(f_n) = p^n - 1.$$

In theory of noiseless coding [3] irreducible over

$GF(p)$ polynomial f_n is called primitive if its root α is a primitive element of extended field $GF(p^n)$.

And finally, in cryptographic [4] the primitive is such an irreducible polynomial $f_n(x)$, which can divide without leftover binomial $x^e - 1$, its true while the minimal e is given by

$$e = p^n - 1. \qquad (2)$$

The drawback of these definitions is that they do not reveal the physical sense to the full extent which makes it harder to give it engineering interpretation. For this purpose PrP may probably be more suitable.

The primitive is a such irreducible polynomial over $GF(p)$ polynomial f_n in degree n (*necessary conditions*), which generate an extended Galois field $GF(p^n)$ for which the minimal construction element ω coincide with the property of polynomial p (*sufficient conditions*).

The other possible definition is: the primitive over the field $GF(p)$ is called an irreducible polynomial f_n in degree n, which constructs a cyclic group of maximal order $p^n - 1$ while the minimal construction element ω of the group coincide with the property of field p.

Coefficients u_k, $k = \overline{0, n}$, of polynomial f_n belong to field $GF(p)$, i. e. $u_k \in GF(p)$. But for any radix of positional number system (PNS) m, including $m = p$ is the radix itself, i.e. the m digit is written as 10. So, for each $p-$PNS and as a result for each field $GF(p^n)$, generated by PrP f_n, $(k+1)-$ degree of minimal primitive element $\omega = 10$ field, which can be represented by ration $\omega^{k+1} = \omega^k \omega$, is constructed by offset of ω^k value to one digit (as a result of multiply in $p-$digit 10). If it turns, that the older non zero digit of value ω^{k+1} is moved to $n-$ digit (digits are enumerated from left to right starting from zero position), so the value ω^{k+1} lead to residue by mod f_n.

Now let's explain the "primitive matrix" definition. Let $A = (a_{i,j})$ is a positive non confluent matrix of $n > 1$ degree over the field of integral nonnegative numbers so as $a_{i,j} \in GF(p)$ for each $i, j = \overline{1, n}$, and $E = (\delta_{i,j})$, where $\delta_{i,j}$ – a Kronecker symbol is a singular matrix of the same degree as A. The A matrix is considered to be nonsingular in $GF(p)$ field if its determinant $\det A$ by module p is not equal to zero, i. e. $\det A (\mathrm{mod}\, p) \in \overline{1, p-1}$, where $p-$prime number. The operation of getting in degree d of matrix A is conducted in a loop of subtractions by p module while each element of A^d matrix starting from zero position for which $A^0 = E$ creates a cyclic group $\langle A \rangle$ of exponent e. The A matrix would be called *primitive* if the most minimal natural e fits ratio (2) while $A^e = E$. The essence of "primitive" matrix is more like the essence of "primitive element" of field $GF(p^n)$.

The primitive is a such irreducible polynomial over $GF(p)$ polynomial f_n in degree n (necessary conditions), which generate an extended Galois field $GF(p^n)$ for which the minimal construction element ω coincide with the property of polynomial p (sufficient conditions).

The other possible definition is: the primitive over the field $GF(p)$ is called an irreducible polynomial f_n in degree n, which constructs a cyclic group of maximal order $p^n - 1$ while the minimal construction element ω of the group coincide with the property of field p.

Coefficients of polynomial f_n belong to field $GF(p)$. But for any positional base of counting system (PNS) m, including $m = p$ is the base itself, i. e. The m digit is written as 10. So, for each $p-$ PNS and as a result for each field $GF(p^n)$ generated by PrP f_n, $(k+1)-$ degree of minimal primitive element $\omega = 10$ field, which can be represented by ration $\omega^{k+1} = \omega^k \omega$ is constructed by offset of ω^k value to one digit (as a result of multiply in $p-$digit 10). If it happens the older non zero digit of value ω^{k+1} is moved to $n-$ digit (digits are enumerated from left to right starting from zero position), so the value ω^{k+1} lead to residue by mod f_n.

Now let's explain the "primitive matrix" definition. Let $A = (a_{i,j})$ is a positive non confluent matrix of degree $n > 1$ over the field of integral nonnegative numbers so as $a_{i,j} \in GF(p)$ for each $i, j = \overline{1, n}$, and $E = (\delta_{i,j})$, where $\delta_{i,j}$ – a Kronecker symbol is a singular matrix of the same degree as A. The A matrix is considered to be nonsingular in $GF(p)$ field if its determinant $\det A$ by module p is not equal to zero, i. e. $\det A (\mathrm{mod}\, p) \in \overline{1, p-1}$, where $p-$prime number. The operation of getting in d degree of A matrix is conducted in a loop of subtractions by p module while each element of A^d matrix starting from zero position, for which $A^0 = E$

creates a cyclic group $\langle A \rangle$ of degree e. The A matrix would be called *primitive* if the most minimal natural e fits ratio (2) while $A^e = E$. The essence of "primitive" matrix is more like the essence of "primitive element" of field $GF(p^n)$.

III. Classic Primitive Matrixes of Galois and Fibonacci

The terms "Galois matrix" and "Fibonacci matrix" are taken from theory of cryptography and coding [1], [4], where the generators of pseudo random sequences of Galois and Fibonacci are widely applicable and based on LRS with linear feedbacks. We will call them PRS generators of Galois and Fibonacci.

It is known, that the LSR to be the register of minimal period, the corresponding feedback polynomial shall be a primitive polynomial. The structural schema of generator and configuration of Galois is shown on Fig. 1, for which the linear feedback link are created PrP $f_8 = 101001101$. Galois generator confronts with each non zero element of field $GF(2^8)$ corresponding degree of primitive element $\omega = 10$ by module $f_8 = 101001101$.

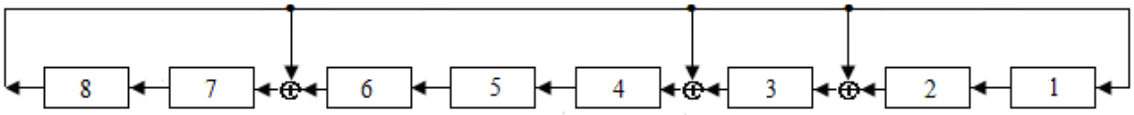

Fig. 1. Structural schema of Galois generator over PrP $f_8 = 101001101$

As elements of LSR memory discharge used usually D – triggers, the signal level at the output of which ("0" or "1") repeats the level of the input signal. The element $\oplus$ in LSR implements the addition operation by module 2 (XOR operation). As it seen from structural schema of generator (as an example shown in Fig. 1) the feedback links in simple (classical) Galois registers (generators) unambiguously defined by chosen PRP f_n and created like this: responses of each digit comes to inputs of subsequent digits for which they are stimulating functions. Besides, the response of older register digit is supplied (by XOR schema) to inputs of such and only such register digits the numbers of whose coincide with non-zero monomial PRP numbers. At that the lower monomial, which reside to the right of f_n polynomial corresponds number 1 as for the lower digit (D – trigger) of register.

Let's identify G_f matrix using which we will compute the state $S(t)$ of Galois registers at the moment of time t using formula:

$$S(t) = S(t-1)G_f, \quad S(0) = 00000001, \quad t = 1, 2, \ldots.$$

The very low row is selected by vector $S(0)$ (let's give it a number 1) of matrix G_f. Consequently in the very low row of matrix G_f it is required to write a $S(1)$ value which coincide with minimal creational element (CE) $\omega = 10$ of field $GF(2^8)$ over PrP $f_8 = 101001101$. Doing the same operation we come to the final matrix:

$$G_f = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (3)$$

According to (3), the algorithm of Galois matrices G_f synthesis can be described as following. Let's f_n – is a vector form of PrP in degree n so as $f_n = \{1, u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1\}$, $u_i \in \{0, 1\}$, $i = \overline{1, n-1}$, and $\omega = 10$ – is the minimal CE of field $GF(2^n)$. Now reside the CE to the right of the very low row of G_f matrix and fill elements of it using the strict rule. Place identities for elements which reside in diagonal lower from main diagonal of the matrix, and place zeroes for elements which are left, except elements of top row. It is assumed to get $(n+1)$ – byte vector in the top row of matrix G_f. This is unacceptable because the degree is equal to n.. Taking this $(n+1)$ – byte vector to remainder by module f_n we come to the state where PRP f_n is placed in the top row of matrix G_f excluding its top unity, i. e. n – bits vector $u_{n-1}, u_{n-2}, \ldots, u_2, u_1, 1$.

Using this simple rule, let's call it *the simple rule*

of diagonal completion; we get the general formula of Galois matrix of order n

$$G_f = \begin{pmatrix} u_{n-1} & u_{n-2} & \cdots & u_2 & u_1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}. \quad (4)$$

From matrix (3) and corresponding structural schema LSR (see Fig. 1) comparison we get values of function initiation $\nu_k(t)$ of classical PrP generators for Galois configuration at any point of time t. Let's $s_k(t)$ – is a state of k – digit (D – trigger) of Galois register. The register's state $S(t) = \{s_n(t), s_{n-1}(t), \cdots, s_2(t), s_1(t)\}$ in initial point of time $t = 0$ is $S(0) = \{0, 0, \ldots, 0, 1\}$. So for each moment of time $t \geq 1$ the function of initiation $\nu_k(t)$ k – digit of register would be defined by

$$v_1(t) = s_n(t-1); v_k(t) = s_{k-1}(t-1) \oplus u_k s_n(t-1),$$
$$k = \overline{2, n} \quad t = 1, 2, \ldots$$

In addition to Galois matrixes we can introduce *Fibonacci matrixes* F_f over PRP f_n which correspond to LSR using the Fibonacci schema (Fibonacci PRP generators). Fibonacci matrixes F_f self-including mutually unambiguously connected with Galois matrixes G_f by *operator of right-hand transposition* $\perp$ *(transposition relatively to helper diagonal), i. e.*

$$F_f \xleftrightarrow{\perp} G_f. \quad (5)$$

It is possible to come to Fibonacci matrixes of n – degree according to ratio (5), as a result of right-hand transposition of matrix (4) we have:

$$F_f = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & u_1 \\ 0 & 1 & \cdots & 0 & 0 & u_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 & u_{n-2} \\ 0 & 0 & \cdots & 0 & 1 & u_{n-1} \end{pmatrix}. \quad (6)$$

The special case (6) is Fibonacci matrix over PRP in degree eight $f_8 = 101001101$, which created by right-hand transposition of matrix (3), i. e.

$$F_f = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \quad (7)$$

The structural schema of PrP generators in Fibonacci configuration which correspond to matrix (7) is shown on Fig. 2.

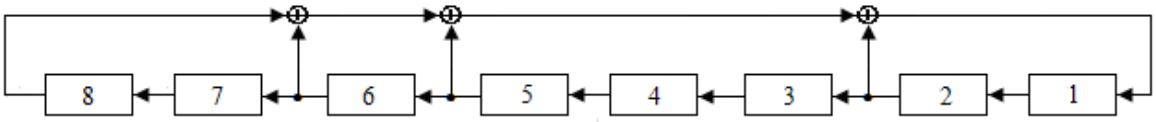

Fig. 2. The structural schema of Fibonacci generator over PRP $f_8 = 101001101$

IV. Conceal Generators of Galois and Fibonacci

An x^* element of some group X is concealed to element x of the same group in group theory if there is some element $z \in X$ which is

$$x^* = z^{-1} x z. \quad (8)$$

By analogy with (8) let's introduce formal definition of conceal matrixes of Galois and Fibonacci using

$$M^* = P^{-1} M P, \quad (9)$$

where M is matrix G or F, and P – matrix which is called a *transition matrix* from M to M^*.

As it follows from ratio (9) matrixes M^* are the matrixes which are alike M and thereby have properties of matrix M. It is signification the matrixes G^* and F^* is called *concealed matrixes* G and F correspondingly using just formal similarity of (8) and (9). For the matrix P the *matrix of inverse rearrangement (IR)* is chosen in this article which we symbolically mark with 1 digit, where 1 – symbol of the operator inverse permutation is an involute square matrix of order n, on the auxiliary diagonal which is ones and zero in other elements.

IR matrix is *involute,* i. e. matrix which is

self-inverse. This means $1\cdot 1 = 1^2 = E$. So

$$G^* = 1\cdot G\cdot 1, \quad G = 1\cdot G^*\cdot 1; \qquad F^* = 1\cdot F\cdot 1, \quad F = 1\cdot F^*\cdot 1. \tag{10}$$

and, as a result

$$M^* \xleftrightarrow{1} M, \quad M \in \{G, F\}. \tag{11}$$

Multiplication of square matrix M times IR matrix from the left is equal to rows of M matrix inversion, and from the right – to columns inversion of the same matrix. So, conceal matrix M^* can be obtained from M matrix by means of mutual inversion of its rows and columns conducted in any order.

According to mutual unambiguously compliance (11) any of described Galois and Fibonacci matrixes (base M and conceal M^*) can be obtained by means of *similarity transformation* from another matrix. The combined forms of classical conceal matrixes of n – degree, according to (4), (6) and (10) are:

$$G_f^* = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & u_1 & u_2 & \cdots & u_{n-2} & u_{n-1} \end{pmatrix}; \qquad F_f^* = \begin{pmatrix} u_{n-1} & 1 & 0 & \cdots & 0 & 0 \\ u_{n-2} & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ u_2 & 0 & 0 & \cdots & 1 & 0 \\ u_1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

According to (12) for conceal matrixes G_f^* and F_f^* over PrP $f_8 = 101001101$ we came to structural eight digit PRS Galios and Fibonacci generators, depicted on Figs 3 and 4 respectively:

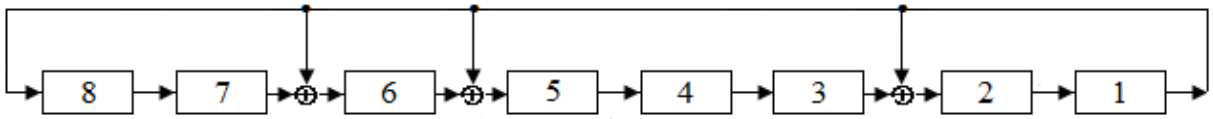

Fig. 3. Structural schema of conceal Galois generator over PrP $f_8 = 101001101$

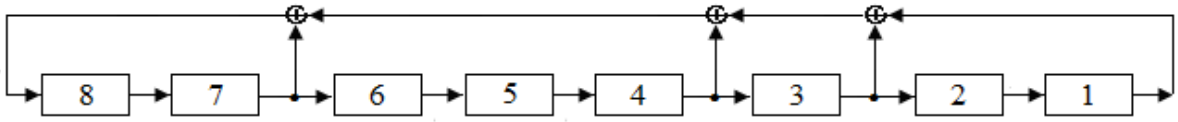

Fig. 4. Structural schema of conceal Fibonacci generator over PrP $f_8 = 101001101$

Initiation functions of D – triggers for classical n – digit linked PRS Galois and Fibonacci generators (the initial states for both generators are the following: $s_1(0) = 1, \quad s_k(0) = 0, \quad k = \overline{2, n}$, where $n = 8$) is described by:

$$\nu_n(t) = s_1(t-1); \quad \nu_k(t) = s_{k+1}(t-1) \oplus u_{n-k} s_1(t-1), \quad k = \overline{1, n-1} \qquad t = 1, 2, ...;$$

and

$$\nu_k(t) = s_{k+1}(t-1), \quad k = \overline{1, n-1};$$

$$\nu_n(t) = s_1(t-1) \overset{n}{\underset{k=2}{\oplus}} u_{k-1} s_k(t-1), \qquad t = 1, 2, \ldots.$$

V. Linear Transformations in PRS Generators

Using the comparison of base Galois G (4) and Fibonacci F (6) matrixes as well as from conceal variants G^* and F^* (12) and could be easily defined (Table 1) operators of one well known matrix transformation into another.

Table 1

Operators of matrixes transformation

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

According to Table 1, if two matrixes belong to different subgroups (let's call them subgroups of Galois and Fibonacci), at that one of matrixes is conceal, so they linked by operator of classical transposition T.

By analyzing structural schemas of simple special LRS generators over PrP $f_8 = 101001101$ generators, shown on Figs 1–4, we came to general transformation rules, gathered in Table 2, the schemas of linear feedbacks (LF) of well known PRS generator over given PrP f_n to schemas LF for any of three types of left generators. Unlike from Table 1, in which by G, F, G^* and F^* symbols are used to define primitive matrixes of PRS generators, the same symbols in Table 2 is used for symbolically define *schemas of feedbacks* in corresponding generators.

TABLE 2

OPERATORS OF FEEDBACKS TRANSFORMATION

	G	F	G^*	F^*
G	—	$1\circ 1$	$\circ 1$	$1\circ$
F	$1\circ 1$	—	$1\circ$	$\circ 1$
G^*	$\circ 1$	$1\circ$	—	$1\circ 1$
F^*	$1\circ$	$\circ 1$	$1\circ 1$	—

The sense of "schemas of feedbacks" in G, F, G^* or F^* PRS generators can be explained by looking at their styled graphical representation shown on Fig. 5. Please notice on such F distinctions. While in base G and F PRS generators their feedbacks are conducted clockwise so in conceal G^* and F^* – counterclockwise.

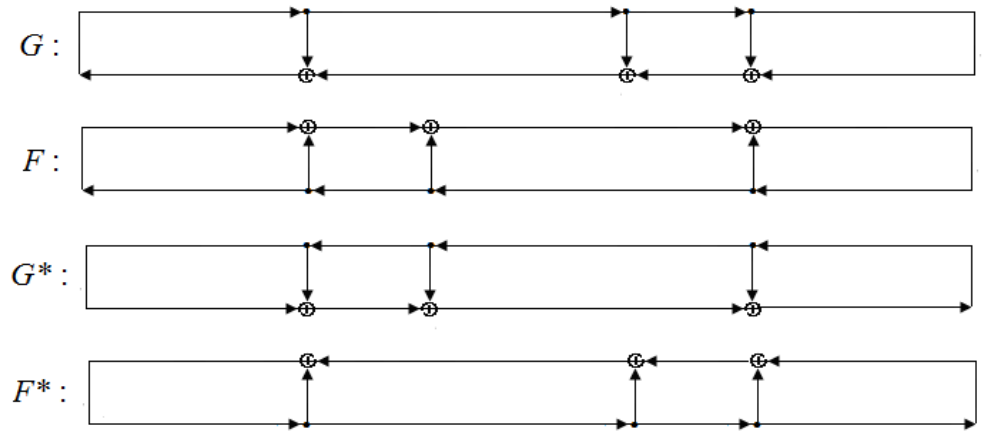

Fig. 5. Styles representation of feedbacks in PRS generators

Let's make it exact the physical sense of transformation operators from tables 2. Operator $\circ 1$ means the schema LF, which is marked by $\circ$, symbol, is being rotated by 180° relatively to vertical axis. Such transformations happen, as it stands from Fig. 5, in generator pairs (G, G^*) or (F, F^*). Operation $\circ 1$ is alike operation of inverse shifting of columns of matrix M, which is implemented if it would be multiplied times matrix of inverse transformation 1. By $1\circ$ operator the rotation of F schema is conducted relatively to horizontal axes. Thus, operation $1\circ$ is alike operation of inverse transformation of rows of matrix M if it would be multiplied times matrix of inverse transformation from the left. Mentioned transformations of feedbacks are having place in generator pairs (G, F^*) or (F, G^*). And finally operator $1\circ 1$ means the F is being rotated on 180° relatively to both vertical and horizontal axes. Such transformations are being executing in generator pairs (G, F) or (G^*, F^*).

VI. GENERALIZED PRIMITIVE GALIOS MATRIXES OVER $GF(2)$

In this section we will describe the algorithm for primitive Galois matrixes construction and others related matrixes where primitive elements $\omega > p = 2 = 10$ of field $GF(2^n)$ over random irreducible polynomial f_n in degree n is used as the base construction elements.

To solve the task of synthesis of primitive matrixes let's use the *generalized rule of diagonal completion* the sense of which is in following. First of all for the very low row of G matrix fill the construction element ω which is a primitive of $GF(p^n)$ field over chosen IP f_n. The row elements to the left of ω are filled with zero. The following rows of the matrix (in direction from bottom to top) is constructed by means of previous row shifting for one digit to the left. If it happens the oldest nonzero digit of the row goes off the matrix's limits, the

vectors responsible from such rows, gives a residue by module CE f_n and the row is getting $n-$ digit.

Let's $n=8$ and $f_8=101001101$. Choose, as for example, IP $\omega=2D=101101$. Here we go to primitive Galois matrix which is depicted as:

$$G_f=\begin{pmatrix}1&1&0&0&1&0&1&0\\0&1&1&0&0&1&0&1\\1&0&0&1&0&1&0&0\\0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\1&0&1&1&0&1&0&0\\0&1&0&1&1&0&1&0\\0&0&1&0&1&1&0&1\end{pmatrix}. \quad (13)$$

Generalized Galios G matrix corresponds to *generalized Fibonacci* F *matrix*, which is created by means of right-hand transposition $\perp$ operator of matrix (13), i. e.

$$F_f=\begin{pmatrix}1&0&0&1&0&0&1&0\\0&1&0&0&1&0&0&1\\1&0&1&1&0&1&1&0\\1&1&0&0&1&0&0&1\\0&1&1&0&0&1&0&0\\1&0&1&1&0&0&1&0\\0&1&0&0&1&0&1&1\\0&0&1&0&0&1&0&1\end{pmatrix}. \quad (14)$$

Using the $1\circ 1$ operator matrixes (13) and (14) transformed into generalized conceals matrixes G^* and F^* described as:

$$G_f^*=\begin{pmatrix}1&0&1&1&0&1&0&0\\0&1&0&1&1&0&1&0\\0&0&1&0&1&1&0&1\\1&0&1&0&0&1&0&0\\0&1&0&1&0&0&1&0\\0&0&1&0&1&0&0&1\\1&0&1&0&0&1&1&0\\0&1&0&1&0&0&1&1\end{pmatrix}; \quad F_f^*=\begin{pmatrix}1&0&1&0&0&1&0&0\\1&1&0&1&0&0&1&0\\0&1&0&0&1&1&0&1\\0&0&1&0&0&1&1&0\\1&0&0&1&0&0&1&1\\0&1&1&0&1&1&0&1\\1&0&0&1&0&0&1&0\\0&1&0&0&1&0&0&1\end{pmatrix}.$$

Let's examine an example of synthesis of generalized primitive matrixes and generators of Galois. Choose a polynomial of fourth degree of $f_4=11111$ degree which is not a primitive and a primitive CE ω of G_f matrix equal to 111. Matrixes which fit chosen generators properties look like

$$G1=\begin{pmatrix}0&1&1&0\\0&0&1&1\\1&1&1&0\\0&1&1&1\end{pmatrix}; \quad F1=\begin{pmatrix}1&0&1&0\\1&1&1&1\\1&1&0&1\\0&1&0&0\end{pmatrix}; \quad G1^*=\begin{pmatrix}1&1&1&0\\0&1&1&1\\1&1&0&0\\0&1&1&0\end{pmatrix}; \quad F1^*=\begin{pmatrix}0&0&1&0\\1&0&1&1\\1&1&1&1\\0&1&0&1\end{pmatrix}. \quad (15)$$

Structural schema of generalized base fourth digit Galois generator which coincides with generalized schema of base Fibonacci generator is shown in Fig. 6. The registers of generators are located vertically and marked with $\otimes$ symbol. They implement multiplication operation. Registers, marked with $\otimes-$ symbol, $-$ addition operation of register content by module 2.

If we would place the columns elements of $G1$ matrix from system (15) we would get the PRS generator by Galois schema. For the case if using the same registers we would use elements from $F1$ matrix, so we would get the PRS by Fibonacci schema. Schema of conceal PRS generators is shown on Fig. 7.

In much the same way as PRS generators, if for the multiplication registers of structural schema on Fig. 7 we would reside elements of $G1^*$ matrix we would get the generalized conceal PRS generator by Galois schema. If using the same registers we would use elements from $F1^*$ matrix so we would get PRS by Galois schema.

The generalized primitive matrixes which belong to the same groud (Galois or Fibonacci) have amazing *commutatively* properties which can be explained as following. Let's $\omega_2=1011-$ is second primitive element of $GF(2^4)$, fields which is different from CE $\omega_1=111$. The following group of primitive matrixes correspond to creation element ω_2:

$$G2=\begin{pmatrix}0&1&0&1\\1&1&0&1\\1&0&0&1\\1&0&1&1\end{pmatrix};\quad F2=\begin{pmatrix}1&1&1&1\\1&0&0&0\\0&0&1&1\\1&1&1&0\end{pmatrix};\quad G2^*=\begin{pmatrix}1&1&0&1\\1&0&0&1\\1&0&1&1\\1&0&1&0\end{pmatrix};\quad F2^*=\begin{pmatrix}0&1&1&1\\1&1&0&0\\0&0&0&1\\1&1&1&1\end{pmatrix}. \qquad (16)$$

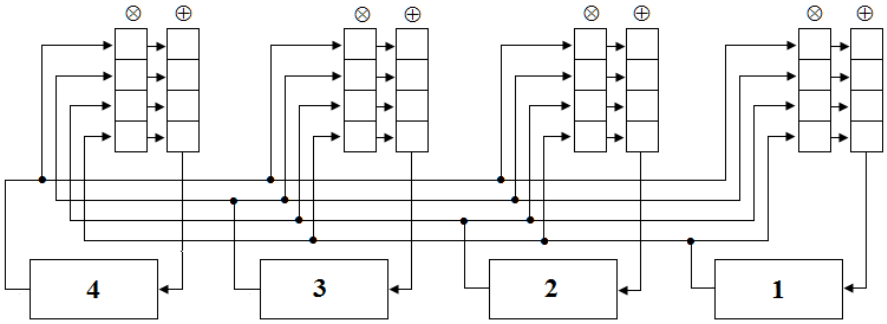

Fig. 6. Structural schema of generalized base PRS generators of Galois/Fibonacci

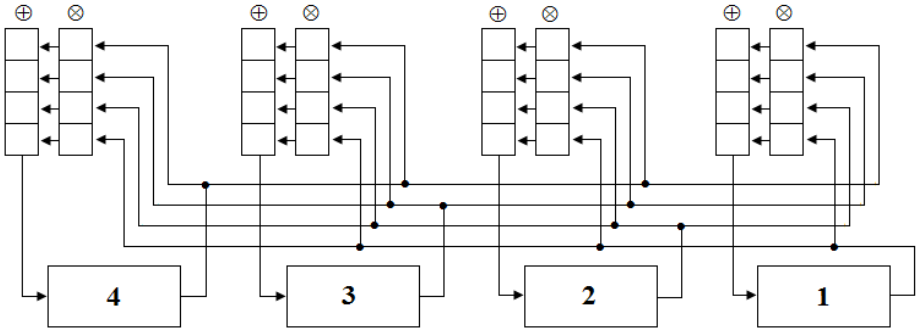

Fig. 7. Structural schema of generalized conceal PRS generators of Galois/Fibonacci

For many primitive matrixes (15) or (16) we can select commutative and non-commutative matrixes. Commutative are the any pair of matrixes, which belong to one of two groups of *monotonous primitive matrixes*. The first monotonous group consists of Galois matrix ($G-$group) which include primitive matrixes $G=\{G1,\ G2,\ G1^*,\ G2^*\}$. The second ($F$–group) include primitive Fibonacci matrixes $F=\{F1,F2,F1^*,F2^*\}$. Thus, for example, matrix $G1$ is commutative with each of three $G2$, $G1^*$ or $G2^*$ matrix, but is not commutative with any of primitive matrixes from $F-$group.

Besides such an interesting property of primitive base Galois matrixes G over IP f_n and CE $\omega \geq 10$. The structure of degrees of $G-$ matrixes, i. e. G^k matrixes the same as structure of base G matrix, i.e. the concept of diagonal rows completion is also applied. This means in order to compute the G^k matrix it is enough to take CE ω in $k-$degree and take remainder of ω^k value by f_n module and then apply the rule of diagonal completion using the CE $\omega_k=(\omega^k) \bmod f_n$. This matrixes property would be considered in unit 6 where the isomorphism of Galois matrixes is described.

VII. Synthesis of primitive Galois matrixes over $GF(p),\ p>2$

Primitive matrixes over $GF(p),\ p>2$ are synthesized using the same rules (diagonal completion) as matrixes over $GF(2)$ do. Let's choose, just for example, $n=4,\ p=3$ and irreducible over $GF(3)$ polynomial $f_4=12101$. Let's $\omega=1102$.. Base G, F and conceal G^*, F^* generalized Galois and Fibonacci matrixes which correspond to chosen parameters $n,\ \omega$ and f_4, look like:

$$G=\begin{pmatrix}1&1&1&2\\1&0&2&1\\2&2&2&2\\1&1&0&2\end{pmatrix};\quad F=\begin{pmatrix}2&2&1&2\\0&2&2&1\\1&2&0&1\\1&2&1&1\end{pmatrix};\quad G^*=\begin{pmatrix}2&0&1&1\\2&2&2&2\\1&2&0&1\\2&1&1&1\end{pmatrix};\quad F^*=\begin{pmatrix}1&1&2&1\\1&0&2&1\\1&2&2&0\\2&1&2&2\end{pmatrix}. \qquad (17)$$

Structural schemas of generalized LSR are invariant to the property of p field. In particular, the structural schemas of fourth digit Galois LSR the feedbacks in which are given by G matrix of (17) are shown on Fig. 8, moreover $\oplus$ is an addition operator by module $p = 3$.

The structural schema of fourth digit conceal Fibonacci LSR the feedback of which is given by F^* matrix of (17) is shown on Fig. 9.

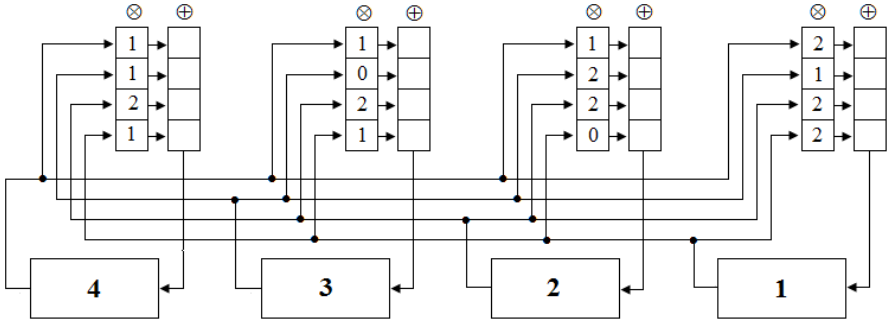

Fig. 8. Structural schema of LSR generalized Galois

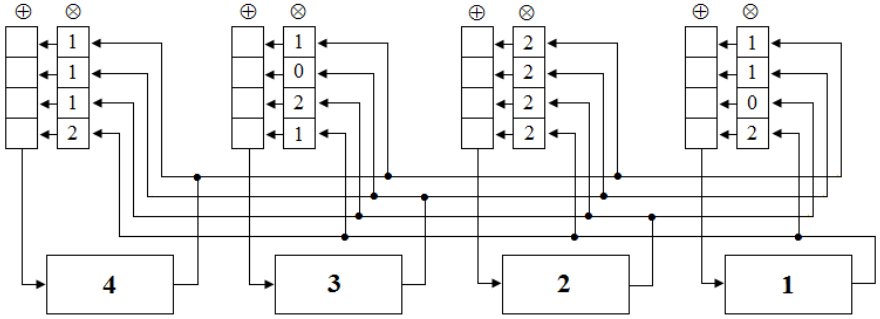

Fig. 9. Structural schema of LSR generalized Fibonacci

It is followed from Figs. 6 to 9 comparison structural schemas of base and conceal generators are *invariant to operators of right hand transposition.*

At the finish line of the section need to pay your attention to the following facts. First of all, if even the only one matrix over the chosen IP is not primitive (this can happen only if chosen CE of matrix the Galois element is not primitive), the primitive property and commutative property are lost. Secondary, according to (17) conceal Galois and Fibonacci matrixes are matrixes which are created by similarity transformation of initial (base) G and F matrixes. The matrixes of inverse shifting 1 are used in the role of transformation matrixes P. As it is knows, similar matrixes keep all properties of source matrixes. Up to this property, if G and F matrixes (simple and generalized) are primitive, so the G^* and F^* are.

VIII. Isomorphism of Matrixes Galois

It was stated in unit four that in order to compute $k-$ degree of Galois matrix it is enough to take CE ω of this matrix in $k-$ degree then compute the remainder by f_n module using ω^k and afterwards apply the generalized rule of diagonal completion using $\omega_k = (\omega^k) \bmod f_n$ as creation element.

Let's examine another interpretation of "diagonal completion" rule which is used for Galois matrix over $GF(p^n)$ field synthesis. According to offered rule on the initial stage of G_f matrix synthesis the creational element ω resides in lower (right) digits of the very bottom row of $n-$ degree matrix. All following matrix's rows are created by means of shifting to one digit to the left of previous row, besides after this shifting the 0 is filled to the right released position. For the case when none zero older (left) element of the row under a shifting is moved out of matrix's limits then $(n+1)-$ digit $p-$ vector is taken to remainder by $\bmod f_n$. By this procedure such a row returns back to matrix's limit and the process of its completion of remained top rows is going using just described rule.

The creational element ω of Galois G_f matrix which contains $k+1$ digits which belong to $GF(p)$ field can be depicted as polynomial in $k-$ degree of one of variable x, i. e. like $\omega_k(x)$. As it is known from polynomial theory, the multiplication of random polynomial $\omega_k(x)$ of k degree x is equal to poly-

nomial shifting for one digit to the left and thereafter equal to polynomial's degree increment by 1. Another word

$$x\omega_k(x) \to \omega_{k+1}(x). \qquad (18)$$

Using (18) we can express the Galois G_f matrix of n degree as

$$G_f = \begin{pmatrix} x^{n-1}\cdot\omega \\ x^{n-2}\cdot\omega \\ \cdots \\ x\cdot\omega \\ \omega \end{pmatrix} (\mathrm{mod}\, f) = \omega\cdot \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} (\mathrm{mod}\, f). \qquad (19)$$

Elements x^l, $l = \overline{0, n-1}$, of right vector-column in (19) are polynomials of l – degree of single variable the vector form of which is

$$x^l \to \underbrace{1, 0, \ldots 0, 0}_{(l+1)}, \quad l = \overline{0, n-1}. \qquad (20)$$

Taking replacement in (20) into consideration we have the vector-column as

$$\begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \cdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = E, \qquad (21)$$

where E – is a single matrix of n–degree.

Correlations (19) – (21) makes us able to formulate the conclusion: Galois G_f matrix of n degree over IP f_n unambiguously defined of its creational element ω. Consequently Galois G_f matrixes of n degree over $GF(p)$ is isomorphs' to it creational element ω, which belong to $GF(p^n)$ field. That means that there is a mutually unambiguously correlation between G_f matrix and its CE, i. e. $G_f \leftrightarrow \omega$.

IX. Characteristic Polynomials of Galois Matrixes

The characteristic polynomial (CP) of nonsingular square matrix A of order n is a polynomial of n–degree

$$\chi(\lambda) = \det(A - \lambda E),$$

where E–the unity matrix of the same n degree, as A matrix [6].

An amazing property CP of matrix is: if the some matrices A and B are similar, then they CP coincide. The reverse is also true: if the matrices have identical CP, consequently the matrix similar.

Let's have a look on analyses of characteristic polynomials of Galois, Fibonacci and conjugate matrixes. The following is true

***Statement*:** *Characteristic polynomials of Galois and Fibonacci (both basic and conjugate) over* $GF(p)$, $p \geq 2$, *with a generating element* $\omega = 10$ *are coincide with irreducible polynomials, which generate by data matrixes.*

The main point of the approval is

$$\chi(x) = \det(M_{f_n} - xE) \equiv f_n(x), \qquad (22)$$

where M_{f_n} – matrix G, F, G^* or F^*, generated IP $f_n(x)$ and the generating element $\omega = 10$..

The proving of the statement can be conducted by method of direct verification. Indeed, let's choose, just for example, PRS of third degree $f_3(x) = 1011$, $p = 2$, for which

$$\chi_G(x) = \begin{vmatrix} -x & 1 & 1 \\ 1 & -x & 0 \\ 0 & 1 & -x \end{vmatrix}; \quad \chi_F(x) = \begin{vmatrix} -x & 0 & 1 \\ 1 & -x & 1 \\ 0 & 1 & -x \end{vmatrix}; \quad \chi_{G^*}(x) = \begin{vmatrix} -x & 1 & 0 \\ 0 & -x & 1 \\ 1 & 1 & -x \end{vmatrix}; \quad \chi_{F^*}(x) = \begin{vmatrix} -x & 1 & 0 \\ 1 & -x & 1 \\ 1 & 0 & -x \end{vmatrix},$$

where $|A|$ – determinant of matrix A.

It is easy to make sure, that for all four matrixes the CP is the same, so they $\chi(x) = x^3 + x + 1$ are coincide with PrP $f_3(x)$.

Using the same approach the verification of (22) equation can be conducted for matrixes, which are generated by irreducible polynomials, but with the proviso, that their GE are equal to 10.

At the same time for generalized matrixes G, F, G^* and F^*, so those for which GE $\omega > 10$, the statement is not always true. Let's have a look on the example. Let's $p = 2$, $f_3(x) = 1011$ and $\omega = 101$. So, we have

$$G = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix};$$

$$\chi_G(x)=\begin{vmatrix} -x & 1 & 0 \\ 0 & -x & 1 \\ 1 & 0 & 1-x \end{vmatrix} = x^3+x^2+1 \Rightarrow 1101,,$$

i. e. $\chi_G(x)$ does not coincide with $f_3(x)$.

CONCLUSIONS

The main result of the current research is an invention of algorithm for generalized base and conceal Galois and Fibonacci matrixes the elements of which belong to simple field $GF(p)$ of $p \geq 2$ property. Those matrixes have amazing properties such as primitiveness and commutations which made it possible to create linear registers of maximal period and corresponding generators of pseudo random sequences. Structural schemas of generalized LSR are happened to be similar and invariant to registers n orders as well as to p properties of Galois field.

It is worth mentioning the generalized LSR with linear feedback do not introduce any new properties to sequences which created by generalized PRS generators because Golomb's postulates are kept the same way as for classical generators.

REFERENCES

[1] Ivanov, M. A.; Chugunkov, I. V. Theory, application and evaluation of the quality of pseudo-random sequences. Moscow: Kudits-OBRAZ, 2003. (In Russian).

[2] Lidl, R.; Niederreiter, H. Finite fields. Monograph in 2 vols. Addison Wesley, 1983.

[3] Volkovich, S. L.; Geranin, V. O.; Movchan, T. V.; Pisarenko, L. D. Introduction to algebraic theory of noiseproof coding. Kyiv: UkrINTEI, 2002. (In Russian).

[4] Ivanov, M. A. Cryptographic methods of information security in computer systems and networks. Moscow: Kudits-OBRAZ, 2001. (In Russian).

[5] Beletsky, A. Ja.; Beletsky, A. A.; Beletsky, E. A. Gray Transformations. Monograph in 2 vols. vol.1. Fundamentals of the theory. Kyiv: NAU Publishing House, 2001. (In Russian).

[6] Gantmakher, F. R. Theory of Matrices. – Moscow: Nauka, 1968. (In Russian).

[7] Fomichev V. M. Discrete mathematics and cryptology. Moscow.: Dialog-MIFI, 2003. 400 p.

Received 05 October 2014.

Beletsky Anatoliy. Doctor of Science (Engineering), PhD, Professor.
Institute of Air Navigation, National Aviation University, Kyiv, Ukraine.
Education: Kiev Institute of Civil Aviation, Kiev, Ukraine (1961).
Research area: noiseless coding and data protection.
Publications: more than 350 papers.
E-mail: abelnau@ukr.net

Beletsky Evgeniy. Junior Researcher.
Institute of Air Navigation, National Aviation University, Kyiv, Ukraine.
Education: National Aviation University, Kyiv, Ukraine (2003).
Research interests: noiseless coding and data protection.
Publications: 24.
E-mail: ebeletskiy@gmail.com

А. Я. Білецький, Е. А. Білецький. Примітивні матриці та генератори псевдовипадкових послідовностей Галуа

Розглянуто питання формування узагальнених примітивних матриць Галуа і Фібоначчі довільного порядку n над простим полем $GF(p)$. Синтез матриць базується на використанні незвідних поліномів f_n ступеня n і примітивних елементів розширеного поля $GF(p^n)$, що породжується поліномом f_n. Запропоновано способи побудови сполучених примітивних матриць Галуа і Фібоначчі. Обговорюються можливості застосування таких матриць при вирішенні задачі побудови узагальнених генераторів псевдовипадкових послідовностей Галуа.
Ключові слова: незвідні та примітивні поліноми; примітивні матриці; лінійні регістри зсуву; генератори послідовностей Галуа.

Білецький Анатолій Якович. Доктор технічних наук. Професор.
Кафедра електроніки, Національний авіаційний університет, Київ, Україна.
Освіта: Київський інститут цивільного повітряного флоту, Київ, Україна (1961).
Напрям наукової діяльності: завадостійке кодування та криптографічний захист інформації.
Кількість публікацій: більше 350 наукових робіт.
E-mail: abelnau@ukr.net

Білецький Євген Анатолійович. Молодший науковий співробітник.
Кафедра електроніки, Національний авіаційний університет, Київ, Україна.
Освіта: Національний авіаційний університет, Київ, Україна (2003).
Напрямок наукової діяльності: завадостійке кодування та криптографічний захист інформації.
Кількість публікацій: 24.
E-mail: ebeletskiy@gmail.com

А. Я. Белецкий, Е. А. Белецкий. Примитивные матрицы и генератори псевдослучайных последовательностей Галуа

Рассмотрены вопросы формирования обобщенных примитивных матриц Галуа и Фибоначчи произвольного порядка n над простым полем $GF(p)$. Синтез матриц базируется на использовании неприводимых полиномов f_n степени n и примитивных элементов расширенного поля $GF(p^n)$, порождаемого полиномом f_n. Предложены способы построения сопряженных примитивных матриц Галуа и Фибоначчи. Обсуждаются возможности применения таких матриц при решении задачи построения обобщенных генераторов псевдослучайных последовательностей Галуа.

Ключевые слова: неприводимые и примитивные полиномы; примитивные матрицы; линейные регистры сдвига; генераторы последовательностей Галуа.

Белецкий Анатолий Яковлевич. Доктор технических наук. Профессор.
Кафедра электроники, Национальный авиационный университет, Киев, Украина.
Образование: Киевский институт гражданского воздушного флота, Киев, Украина (1961).
Направление научной деятельности: помехоустойчивое кодирование и криптографическая защита информации.
Количество публикаций: более 350 научных работ.
E-mail: abelnau@ukr.net

Белецкий Евгений Анатольевич. Младший научный сотрудник.
Кафедра электроники, Национальный авиационный университет, Киев, Украина.
Образование: Национальный авиационный университет, Киев, Украина (2003).
Направление научной деятельности: помехоустойчивое кодирование и криптографическая защита информации.
Количество публикаций: 24.
E-mail: ebeletskiy@gmail.com