Nosov Valentin A. (Moscow State University)

Constructing a Parametrical Families of Latin Squares in the Boolean Database.

Abstract.

In this article the construction of parametric classes of Latin Squares over Boolean n-vectors is demonstrated so that these Latin Squares are represented in analytical form by families of Boolean functions. This construction leads to the new property of Boolean functions which is named property. We deduce some classifying results about these families of functions.

Introduction.

Latin Squares are important object of Mathematics and Cryptology and have numerous applications in cryptographic practice. Ciphers on Latin Squares according to theory of C. Shannon [4] are so called perfect. But in most ciphering standards Latin Squares are not changeable and changeability of Latin Squares in ciphering system may raise the level of information security. There are many directions of research in the theory of Latin Squares and the main part of it is the modes of constructing classes of Latin Squares under some conditions. Practical adaptation of Latin Squares in computer ciphering systems requires them to have large dimension and to be changeable. Therefore there is necessity to determine Latin Square analytically and parametrically by functions of two variables, that determines element of square by number of row and column.

Latin Square over set S is the table of dimension $n \times n$, where $n = S$, consisting from elements of S, so that in each row and column all elements are different. There are many applications of Latin Squares in coding theory and cryptology ([4], [5]). In the literature there are many modes of constructing of Latin Squares in table form and this detail is an obstacle to the applications in the case of large $n = |S|$.

The aim of this paper is the presentation some results relating to the construction of parametric families of Latin Squares over set S where S is set of Boolean n—vectors in analytic form. When element of square is determined by function on number of row and column. Also we have some classifying results relating to the form of these functions.

Let E_n — the set of binary vectors of dimension n. In this case Latin Square over set E_n may be determined by family of n Boolean functions

$$\begin{array}{c} f_1(x_1, \ldots, x_n, y_1, \ldots, y_n) \\ f_2(x_1, \ldots, x_n, y_1, \ldots, y_n) \\ \ldots \\ f_n(x_1, \ldots, x_n, y_1, \ldots, y_n) \end{array} \tag{1}$$

of $2n$ variables, where $x_1, \ldots, x_n$ determins the number of row, $y_1, \ldots, y_n$ — the number of column, meaning of functions $f_1, \ldots, f_n$ determines corresponding element of square. By using results about the regularity of families boolean functions [6] it is easy to prove

Theorem 1 *The family of n Boolean functions $f_1, \ldots, f_n$ with $2n$ variables $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ determines the Latin Square if and only if, when in all products $f_{i_1}, \ldots, f_{i_k}$, $1 \leq i_1 < \ldots < i_k \leq n$, $k < n$ canonical polynome don't contains terms, including $x_1 \ldots x_n$ or $y_1 \ldots y_n$, but product $f_1 \ldots f_n$ contains both this terms and no other terms containing them.*

This proposition does not give the effective mode of constructing necessary functions but may be useful for finding sufficient conditions for solving this question.

Let us consider the mode of introduction the parameter in the family of Latin Square. Let we have the family of Boolean functions

$$g = (g_1(z_1, \ldots, z_n), \ldots, g_n(z_1, \ldots, z_n)) \tag{2}$$

with n variables $z_1, \ldots, z_n$. Let

$$\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n) \tag{3}$$

— system of Boolean functions with two variables. Let system of Boolean functions $f_1, \ldots, f_n$ with $2n$ variables $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ is defined by relations:

$$\begin{array}{c} f_1 = x_1 + y_1 + g_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ f_2 = x_2 + y_2 + g_2(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \\ \ldots \\ f_n = x_n + y_n + g_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)) \end{array} \tag{4}$$

Let us remind the definition from the article [1]. The family of Boolean functions $g = (g_1, \ldots, g_n)$ is named proper, if for all distinct n—collections of variables $z^{'} = \left(z_1^{'}, \ldots, z_n^{'}\right)$ and $z^{''} = \left(z_1^{''}, \ldots, z_n^{''}\right)$ exists $\alpha \in \overline{1, n}$ such that next relation is hold

$$z_\alpha^{'} \neq z_\alpha^{''}, \quad g_\alpha(z_1^{'}, \ldots, z_n^{'}) = g_\alpha(z_1^{''}, \ldots, z_n^{''}) \tag{5}$$

Theorem 2 *The system of Boolean functions $f_1, \ldots, f_n$ as (4) determines the Latin Square for any functions of two variables $\pi_1, \ldots, \pi_n$ if and only if when the family of functions $g = (g_1, \ldots, g_n)$ is proper.*

Proof. Let the functions $\pi_1, \ldots, \pi_n$ with two variables exist and family of functions $f_1, \ldots, f_n$, defined by (4), does not determine the Latin Square. Then we have

$$\begin{array}{c} f_1\left(x_1^{'}, \ldots, x_n^{'}, y_1, \ldots, y_n\right) = f_1\left(x_1^{''}, \ldots, x_n^{''}, y_1, \ldots, y_n\right) \\ \ldots \\ f_n\left(x_1^{'}, \ldots, x_n^{'}, y_1, \ldots, y_n\right) = f_n\left(x_1^{''}, \ldots, x_n^{''}, y_1, \ldots, y_n\right) \end{array} \tag{6}$$

for certain $x_1^{'}, \ldots, x_n^{'}$, $x_1^{''}, \ldots, x_n^{''}$, $y_1, \ldots, y_n$, where $\left(x_1^{'}, \ldots, x_n^{'}\right) \neq \left(x_1^{''}, \ldots, x_n^{''}\right)$, or

$$\begin{array}{c} f_1\left(x_1, \ldots, x_n, y_1^{'}, \ldots, y_n^{'}\right) = f_1\left(x_1, \ldots, x_n, y_1^{''}, \ldots, y_n^{''}\right) \\ \ldots \\ f_n\left(x_1, \ldots, x_n, y_1^{'}, \ldots, y_n^{'}\right) = f_n\left(x_1, \ldots, x_n, y_1^{''}, \ldots, y_n^{''}\right) \end{array} \tag{7}$$

for certain $x_1, \ldots, x_n$, $y_1^{'}, \ldots, y_n^{'}$, $y_1^{''}, \ldots, y_n^{''}$, where $\left(y_1^{'}, \ldots, y_n^{'}\right) \neq \left(y_1^{''}, \ldots, y_n^{''}\right)$. Let (6) is hold, then using (4) we get equations

$$\begin{array}{c} x_1^{'} + g_1(\pi_1(x_1^{'}, y_1), \ldots, \pi_n(x_n^{'}, y_n)) = x_1^{''} + g_1(\pi_1(x_1^{''}, y_1), \ldots, \pi_n(x_n^{''}, y_n)) \\ \ldots \\ x_n^{'} + g_n(\pi_1(x_1^{'}, y_1), \ldots, \pi_n(x_n^{'}, y_n)) = x_n^{''} + g_n(\pi_1(x_1^{''}, y_1), \ldots, \pi_n(x_n^{''}, y_n)) \end{array} \tag{8}$$

Let us put the signings $z^{'} = \left(z_1^{'}, \ldots, z_n^{'}\right)$, where $z_i^{'} = \pi_i\left(x_i^{'}, y_i\right)$, $i = \overline{1,n}$ and $z^{''} = \left(z_1^{''}, \ldots, z_n^{''}\right)$, where $z_i^{''} = \pi_i\left(x_i^{''}, y_i\right)$, $i = \overline{1,n}$ and consider the pair

$$g\left(z^{'}\right) = \left(g_1\left(z^{'}\right), \ldots, g_n\left(z^{'}\right)\right)$$

$$g\left(z^{''}\right) = \left(g_1\left(z^{''}\right), \ldots, g_n\left(z^{''}\right)\right)$$

If for all $\alpha \in \overline{1,n}$ is hold $g_\alpha\left(z^{'}\right) \neq g_\alpha\left(z^{''}\right)$, then the condition of property for family $g = (g_1, \ldots, g_n)$ is not hold on pair $z^{'}$ and $z^{''}$. If exists $\alpha \in \overline{1,n}$, such, that $g_\alpha\left(z^{'}\right) = g_\alpha\left(z^{''}\right)$ is hold then from relation (8) we get $x_\alpha^{'} = x_\alpha^{''}$. And then $\pi_\alpha\left(x_\alpha^{'}, y_\alpha\right) = \pi_\alpha\left(x_\alpha^{'}, y_\alpha\right)$ so we have $z_\alpha^{'} = z_\alpha^{''}$. Consequently in this case the condition of property of family $g_1, \ldots, g_n$ is not hold on pair $z^{'}$ and $z^{"}$. The case (7) is proved by similar way. So we have if system of functions (4) does not determine the Latin Square for any functions $\pi_1, \ldots, \pi_n$ then the family $g_1, \ldots, g_n$ is not proper. Let now the family $g_1, \ldots, g_n$ is not proper. This means that exists pair of variables $z^{'} = \left(z_1^{'}, \ldots, z_n^{'}\right)$ and $z^{''} = \left(z_1^{''}, \ldots, z_n^{''}\right)$, such that for all $\alpha \in \overline{1,n}$ with condition $z_\alpha^{'} \neq z_\alpha^{''}$ we have $g_\alpha\left(z^{'}\right) \neq g_\alpha\left(z^{''}\right)$. Let us consider any $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$. Consider the pair $x_1^{'}, \ldots, x_n^{'}$ and $x_1^{''}, \ldots, x_n^{''}$, where

$$\begin{array}{c} x_i^{'} = x_i + g_i\left(z^{'}\right),\ i \in \overline{1,n} \\ \ldots \\ x_i^{''} = x_i + g_i\left(z^{''}\right),\ i \in \overline{1,n} \end{array} \tag{9}$$

Now determine the functions $\pi_1, \ldots, \pi_n$ so that is hold

$$\begin{array}{c} \pi_i\left(x_i^{'}, y_i\right) = z_i^{'},\ i \in \overline{1,n} \\ \ldots \\ \pi_i\left(x_i^{''}, y_i\right) = z_i^{''},\ i \in \overline{1,n} \end{array} \tag{10}$$

This is impossible only in the case when $x_i^{'} = x_i^{''}$, but $z_i^{'} \neq z_i^{"}$ for some $i \in \overline{1,n}$. But if $x_i^{'} = x_i^{''}$, then from (9) we have $g_i\left(z^{'}\right) = g_i(z^{''})$ and with condition on $z^{'}$ and $z^{''}$ we have $z_i^{'} = z_i^{''}$. Now it is easy to see from (4), that elements of the square corresponding $\left(x_1^{'}, \ldots, x_n^{'}, y_1, \ldots, y_n\right)$ and $\left(x_1^{''}, \ldots, x_n^{''}, y_1, \ldots, y_n\right)$ equal $(x_1, \ldots, x_n)$, and the square (4) is not Latin for given functions $\pi_1, \ldots, \pi_n$. ■

Remark 1 *The notion of property for family Boolean functions was introduced in [1] in connection of study regularity (substitution property) of boolean automata. There it is proved following criteria.*

Theorem 3 *A family of Boolean functions $f_1, \ldots, f_n$ with variables $x_1, \ldots, x_n$ is proper if and only if when in all products $f_{i_1} \ldots f_{i_k}$ there are not terms $x_{i_1} \ldots x_{i_k}$ in corresponding canonical polynoms.*

Let us consider the connection of proper and regular families of Boolean functions. It is easy to prove

Theorem 4 *A family of Boolean functions $f = (f_1, \ldots, f_n)$ is proper if and only if when the family $g_1, \ldots, g_n$, where $g_i = a_i f_i + x_i$ for all constant a_i, is regular, $i = \overline{1,n}$.*

Now we give some classifying results about the proper families functions. For effective application of this construction of Latin Squares we need to describe some classes of proper families of Boolean functions. For any families functions $f = (f_1, \ldots, f_n)$ of variables $x_1, \ldots, x_n$ define the oriented graph G_f of essential variable as $G_f = (V, E)$, where $V = \{1, \ldots, n\}$, $(i, j) \in E$ when variable x_i is essential for f_j. It is easy to see that if $G_f = (V, E)$ has no cycles then the family $f = (f_1, \ldots, f_n)$ is proper. Inverse assertion is not true. Let us consider the family $f = (f_1, \ldots, f_n)$ where

$$\begin{array}{c} f_1 = (x_2 + 1)x_3 \ldots x_n \\ \ldots \\ f_n = (x_1 + 1)x_2 \ldots x_{n-1} \end{array} \tag{11}$$

It is easy to see that graph G_f, is complete but the family $f = (f_1, \ldots, f_n)$ is proper. Let M be class multyaffine functions. That is every function $f \in M$ is conjunction of lineal functions. Let f is the family of multyaffine functions. This means that $f = (f_i \; i \in \overline{1, n})$ may be presented as

$$\begin{array}{c} f_1 = \prod\limits_{i=1}^{k_1} l_i^1(x_1 \ldots x_n) \\ f_2 = \prod\limits_{i=1}^{k_2} l_i^2(x_1 \ldots x_n) \\ \ldots \\ f_n = \prod\limits_{i=1}^{k_n} l_i^n(x_1 \ldots x_n) \end{array} \tag{12}$$

where $k_i \; i \in \overline{1, n}$ — number of linear functions in f_i, and $l_i^t = a_1^t x_1 + \ldots + a_n^t x_n + b_t$ — lineal function over the field F_2, $1 \leq t \leq n$. Define oriented graph G_f^0 of entering variables in family f, by putting

$$G_f^0 = (V, E) \tag{13}$$

where $V = \{1, 2, \ldots, n\}$, $(i, j) \in E \Leftrightarrow \exists s \mid$ the function l_s^j contains x_i (that is $a_s^j = 1$).

Remark 2 *The graph G_f^0 of entering variables contains as subgraph graph G_f of essentiality variables of family f. Designing of graph G_f^0 is simple, designing of graph G_f is NP—hard problem for many classes of functions ([2]).*

The cycle for which no proper subset of vertexes do not contain cycle we will name as simple.

Theorem 5 *The family of multyaffine functions $f = (f_i) \; i \in \overline{1, n}$, is proper if and only if when for every simple cycle C of the graph of entering variables G_f^0 of family f is hold*

$$\prod_{i \in C} f_i(x_1, \ldots, x_n) \equiv 0 \tag{14}$$

Proof. Let the simple cycle C of the graph G_f exists and condition (14)is not hold, that is

$$\prod_{i \in C} f_i(x_1, \ldots, x_n) \neq 0 \tag{15}$$

Let $C = i_1, \ldots, i_s,\ i_k \in \overline{1,n}$. This means that function f_{i_1} contains entering variable x_{i_2} and does not contain entering variables $x_{i_1}, x_{i_3}, \ldots, x_{i_s}$ Similarly it is true about functions $f_{i_2}, \ldots, f_{i_s}$. The functions $f_{i_1}, \ldots, f_{i_s}$ may be presented as

$$\begin{array}{c} f_{i_1} = (\ldots + x_{i_2} + \ldots) \ldots (\ldots + x_{i_2} + \ldots)\varphi_{i_1}(x_1, \ldots, x_n) \\ \ldots \\ f_{i_s} = (\ldots + x_{i_1} + \ldots) \ldots (\ldots + x_{i_1} + \ldots)\varphi_{i_s}(x_1, \ldots, x_n) \end{array} \tag{16}$$

here φ_{i_1}—multyaffine function, not containing the entering x_{i_2}. Similarly, φ_{i_s}—multyaffine function, not containing the entering x_{i_1}, multipliers by φ_{i_1} are linear functions, containing entering x_{i_2}, multipliers by φ_{i_s} are linear functions, containing entering x_{i_1}. According to (15) there is n—collection $x = (x_1^0, \ldots, x_n^0)$, such that $\prod\limits_{i \in C} f_i(x_1^0, \ldots, x_n^0) = 1$. Consequently we have

$$f_{i_1}\left(x_1^0, \ldots, x_n^0\right) = \ldots = f_{i_s}\left(x_1^0, \ldots, x_n^0\right) = 1 \tag{17}$$

Let us consider collection $\tilde{x} = \left(x_1^0, \ldots, \bar{x}_{i_1}^0, \ldots, \bar{x}_{i_s}^0, \ldots, x_n^0\right)$, which is took from $x = (x_1^0, \ldots, x_n^0)$ by negotiating of variables with indexes from C.

Then from (16) we conclude that it is hold

$$f_{i_1}(\tilde{x}) = f_{i_2}(\tilde{x}) = \ldots = f_{i_s}(\tilde{x}) = 0 \tag{18}$$

From (17) and (18) we see that family f is not proper if we take two collections $x = (x_1^0, \ldots, x_n^0)$ and $\tilde{x} = \left(x_1^0, \ldots, \bar{x}_{i_1}^0, \ldots, \bar{x}_{i_s}^0, \ldots, x_n^0\right)$. Conversely, let for any simple cycle C of graph G_f^0 the relation (14) is hold. For family $f = (f_i)$ i $\in \overline{1,n}$ let us consider the family $\check{f} = \left(\check{f}_i\right)\ i \in \overline{1,n}$, where

$$\check{f}(x_1, \ldots, x_n) = x_i + f_i(x_1, \ldots, x_n),\ \forall i \in \overline{1,n}. \tag{19}$$

Let $I\ i \in \overline{1,n}$ — the set of indexes, $\varepsilon_I = (\varepsilon_\alpha),\ \alpha \in I, \varepsilon \in \{0,1\}$ — family of constants. For any function $g = (g_1, \ldots, g_n)$ we put

$$g^{\varepsilon_I}\left(x_i, i \in CI\right) = g_(x_1, \ldots, x_n) \mid_{x_\alpha = \varepsilon_\alpha, \alpha \in I}$$

That is the variables with indexes from I are substituted by constants ε_I, CI—the complement I in $i \in \overline{1,n}$. It is proved (see.[1], Lemma 2), that f is proper family if and only if when the family

$$\check{f}^{\varepsilon_I} = \left(\check{f}_i^{\varepsilon_I}\right),\ i \in CI$$

is regular for all $I \neq \overline{1,n}$ and all ε_I.

For proving regularity any family of Boolean functions $g = (g_1, g_2, \ldots, g_n)$ with variables $x_1, x_2, \ldots, x_n$ we will use criteria of Huffman (see. [6]), according to which the family $g = (g_1, g_2, \ldots, g_n)$ is regular if and only if when for any indexes $i_1, i_2, \ldots, i_k,\ k \leq n-1$ the product $g_{i_1} g_{i_2} \ldots g_{i_k}$ does not contain term $x_1 x_2 \ldots x_n$ in canonical polynom, but the product $g_1 g_2 \ldots g_k$ contain this term. Let the set I is empty. Prove the regularity of family $\check{f} = \left(\check{f}_i\right)\ i \in \overline{1,n}$ We have

$$\check{f}_1 \ldots \check{f}_n = x_1 \ldots x_k + \sum \prod_{i \in p_1} x_i \prod_{j \in p_2} f_j \tag{20}$$

Summation over all partitions (p_1, p_2) the set $i \in \overline{1,n}$, where $p_2 \neq 0$. Prove that $\sum \prod\limits_{i \in p_1} x_i \prod\limits_{j \in p_2} f_j$ for all (p_1, p_2), $p_2 \neq 0$ does not contain the term $x_1 x_2 \ldots x_n$. If on the

contrary for any (p_1, p_2), $p_2 \neq 0$ there is the term $x_1 x_2 \dots x_n$, then it is hold $f_j \neq 0$ if $j \in p_2$ and $\prod\limits_{j \in p_2} f_j(x_1 \dots x_n)$ contains term $\prod\limits_{j \in p_2} x_j$.

Let us consider subgraph $H_f(p_2)$ of the graph G_f, which contains the vertexes of the set p_2. By the definition we have that from every vertex goes out at least one edge. It is easy to see that in this case $H_f(p_2)$ contains the simple cycle C and by the condition we must have

$$\prod_{j \in C} f_j(x_1 \dots x_n) = 0$$

But the set p_2 contains the vertexes C as subset. Consequently we have $\prod\limits_{j \in p_2} f_j(x_1 \dots x_n) \equiv 0$. Then the term $\prod\limits_{i \in p_1} x_i \prod\limits_{j \in p_2} f_j$ if $p_2 \neq 0$ does not contain the term $x_1 x_2 \dots x_n$ and therefore, by (20) the product $\check{f}_1 \dots \check{f}_n$ contains such term. Let now such $k < n$ and indexes $1 \leq i_1 < \dots < i_k \leq n$ exist that product $\check{f}_{i_1} \dots \check{f}_{i_k}$ contains the term $x_1 x_2 \dots x_n$. We have

$$\check{f}_{i_1} \dots \check{f}_{i_k} = x_{i_1} x_{i_2} \dots x_{i_n} + \sum \prod_{i \in p_1} x_i \prod_{j \in p_2} f_j \tag{21}$$

Summation over all partitions (p_1, p_2), $p_2 \neq 0$ the set $i_1, i_2, \dots, i_k$. This means that exists the partition (p_1, p_2), $p_2 \neq 0$, such that the term $\prod\limits_{i \in p_1} x_i \prod\limits_{j \in p_2} f_j$ contains the term $x_1 x_2 \dots x_n$. Consequently the term $\prod\limits_{j \in p_2} f_j$ contains the term $\prod\limits_{i \in Cp_1} x_i$, where Cp_1 is the complement of the set p_1 in $\overline{1,n}$. Consider the subgraph $H_f(p_2)$ on vertexes of the set p_2. Since the functions with indexes from the set p_2 give the term $\prod\limits_{i \in Cp_1} x_i$ then by the definition of the graph G_f from each vertex of Cp_1 at least one edge goes out with the end in p_2. By the condition we have $p_2 \subset Cp_1$ and therefore the graph $H_f(p_2)$ contains the cycle. Then we have the consequence $\prod\limits_{j \in p_2} f_j(x_1 \dots x_n) \equiv 0$ and the term $x_1 x_2 \dots x_n$ does not appear in (21). Hence it is proved that the family $\check{f}_1 \dots \check{f}_n$ is regular according to Huffman's criteria.

Let $I \subset \overline{1,n}$—strictly subset, ε_I—arbitrary family of the constants. Regularity of the family $f^{\varepsilon_I} = (f^{\varepsilon_I})$, $i \in CI$ (with variables x_i, $i \in CI$) may be proved by the similar arguments. This is possible because by the substitution the variables by the constants the multyaffine function is also multyaffine and the condition (19) is hold by substitution of variables with the constants. ■

Now we give recursive mode constructing the proper families of functions. Let there is the family f' functions with variables $z_{i0}, \dots, z_{in}$. Define family of $n + s_1 + \dots + s_n$ functions $f = (f_{ij})$ with variables z_{ij}, $i = 1, \dots, n$, $j = 1, \dots, s_i$ ($s_1, \dots, s_n$—any natural numbers ≥ 0) by relations

$$\begin{gathered} f_{i1} = \Phi_{i_1}(f'_{i0}, x_{i0}) \\ f_{i2} = \Phi_{i_2}(f'_{i0}, x_{i0}, z_{i1}) \\ \dots \\ f_{is_t} = \Phi_{is_t}(f'_{i0}, x_{i0}, z_{i1}, \dots, z_{is_{t-1}}) \\ f_{i0} = \Phi_{i0}(f'_{i0}, x_{i0}, z_{i1}, \dots, z_{is_t}) \end{gathered} \tag{22}$$

$\Phi_{i0}, \Phi_{i1}, \dots, \Phi_{is_t}$—any functions with corresponding (22) variables.

Theorem 6 *If the family f' is proper, then the family f is proper also for any functions Φ_{ij}, $i \in \overline{1,n}$, $j \in \overline{0,s_t}$.*

Proof. Let the family f is not proper. Hence there is the pair of distinct collections $z^{'} = \left(z^{'}_{ij}\right)$, $i \in \overline{1,n}$, $j \in \overline{0,s_t}$, and $z^{''} = \left(z^{''}_{ij}\right)$, $i \in \overline{1,n}$, $j \in \overline{0,s_t}$ such that for all α, β, when $z^{'}_{\alpha\beta} \neq z^{''}_{\alpha\beta}$ we have $f_{\alpha\beta}(z^{'}) \neq f_{\alpha\beta}(z^{''})$. There are two events:

1. $z^{'}_0 \neq z^{''}_0$, where $z^{'}_0 = \left(z^{'}_{10}, \ldots, z^{'}_{n0}\right)$, $z^{''}_0 = \left(z^{''}_{10}, \ldots, z^{''}_{n0}\right)$ By the definition for family $f^{'}_0 = \left(f^{'}_{10}, \ldots, f^{'}_{n0}\right)$ there is $\alpha \in \overline{1,n}$, such that $z^{'}_{\alpha 0} \neq z^{''}_{\alpha 0}$ and $f_{\alpha 0}(z^{'}) = f_{\alpha 0}(z^{''})$. From relations (22) we get that $f_{\alpha 1}(z^{'}) = f_{\alpha 1}(z^{''})$ and accordingly the presumption about family f we get $z^{'}_{\alpha 1} = z^{''}_{\alpha 1}$. Again from relations (22) we get $f_{\alpha 2}(z^{'}) = f_{\alpha 2}(z^{''})$ and therefore we have $z^{'}_{\alpha 2} \neq z^{''}_{\alpha 2}$. The prolongation gives to us the relation $z^{'}_{\alpha s_t} = z^{''}_{\alpha s_t}$ and from (22) we get the relation $f_{\alpha 0}(z^{'}) = f_{\alpha 0}(z^{''})$ and hence $z^{'}_{\alpha 0} \neq z^{''}_{\alpha 0}$, what contradicts the condition of α.

2. $z^{'}_0 = z^{''}_0$. In this case from relations (22) we have $f_{i1}(z^{'}) = f_{i1}(z^{''})$ for all $i \in \overline{1,n}$. By the presumption about family f we have $z^{'}_{i1} = z^{''}_{i1}$ for all $i \in \overline{1,n}$. Now from (22) we have $f_{i2}(z^{'}) = f_{i2}(z^{''})$ for all $i \in \overline{1,n}$. This implies $z^{'}_{i2} = z^{''}_{i2}$ for all $i \in \overline{1,n}$. The prolongation gives to us that $z^{'}_{is_t} = z^{''}_{is_t}$ for all $i \in \overline{1,n}$ and consequently $z^{'} = z^{''}$. This contradicts the choice the pair $z^{'}, z^{''}$. This proves that the family f is proper. ■

Remark 3 *Some generalizations of demonstrated facts for families functions over Abelian groups are presented in paper [3].*

Conclusion.

The construction of parametric family of Latin Squares in analytic form and arbitrary large size is presented. This construction is based on some property of families functions named proper family. For this property some classifying and constructing results are demonstrated. Application of these results to the ciphering system may get the changeable Latin Square in them and to be fit for long data. These applications may guarantee more high level of information security.

References

[1] Nosov V.A. Criterion of regularity of nonautonomous boolen automat with separate input. Intellectual Systems. v-3, n. 3-4,1998,269-280 p.

[2] Alekseev V. B., Nosov V.A. NP-full problems and their polynomial versions. Review. Review of industry and applied math., 1997, v. 4, n. 2, 165-193 p.

[3] Nosov V.A., Pankratiev A.E. Latin squares over abbelian groups. Fundamental and applied math., v. 12, n. 3, 2006, 65-71 p.

[4] Shannon C. Communication theory of secrecy system, Bell System Techn. J.,28,Number 4,(1949),656-715 p.

[5] Denes J., Keedwell A.D. Latin squares and their applications, Budapest,1974, 547 p.

[6] Huffman D.A. Canonical forms for information lossless finite-state logical machines. IRE Trans. Circ. Theory, 1959, v.6, p.41-59.

[7] Kloss B.M., Malishev V.A. Determination of regularity of automat using his canonical equations. Report. The Academy of Science Of The USSR. 1967., v. 172, n. 3, 543-546 p.