УДК 621.391.1

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 1, pp. 38-45

CONSTRUCTING OF MINIMAX CLASS OF PERFECT BINARY ARRAYS OF ORDER $N = 6$ FOR MULTI-CHANNEL CRYPTOGRAPHIC INFORMATION TRANSFER SYSTEM

N.I. Kushnirenko, V.Y. Chechelnytskyi, L.A. Kuznetsova

Odessa National Polytechnic University,
av. Shevchenko, 1, Odessa, Ukraine, 65044; e-mail: natalka_kni@ukr.net

This paper presents a method for constructing of the minimax class of perfect binary arrays with order $N = 6$. Maximum peak level of the two-dimensional periodic cross-correlation function between perfect binary arrays of minimax class has been evaluated. Power of the minimax class has been determined. Development of method is based on analysis of structural and correlation properties of thinned matrices. Paper proposes the method for single-channel and multi-channel cryptographic information transfer systems design. These systems are based on codes designed on the basis of minimax class of perfect binary arrays. Limits on the number of channels in multi-channel system determined. The method for overcoming of these limitations proposed.

Keywords: the minimax class, the perfect binary array, error-correcting codes, cryptographic information transfer systems, information security

Introduction

At the present time the heightened attention is paid to the effective application of perfect binary arrays (PBAs). Such structures can be used to solve problems of information security, error-correcting coding, radar and other related areas that directly reflected in contemporary scientific papers. PBAs have attractive correlation properties and allow simple technical implementation of devices for their formation and processing.

As shown in [1] the new classes of error-correcting codes can be built on the basis of the PBAs. Such codes have attractive properties and a number of advantages in comparison to many well-known codes, including BCH codes. Moreover, these codes can be processed using majority decoding. On the other hand, the PBA classes have a very large power which riches billion of arrays depending on the order of PBAs. Owing to this the PBAs can find wide application in the cryptographic information transfer systems design [2-3].

Properties of PBAs of order $N = 2^k$, where k is arbitrary integer, and algorithms for their constructing are well known and widely discussed in domestic and foreign papers. However, PBAs of order $N = 3 \cdot 2^k$ require detailed consideration. There are no known algorithms for constructing of PBAs classes of these orders with desired properties, such as minimax class and classes with constant level of cross-correlation.

The aim of the research

Search of the minimax class on the basis of complete PBA class is fairly complex computational task. The aim of this study is to develop a constructive algorithm for formation of the minimax class of PBA with order $N = 6$ based on the properties of the PBAs and their thinned matrices.

The following problems must be solved to achieve this:

- consider the structural and correlation properties of PBAs' thinned matrices;
- determine the imbalance parameter for PBA of order $N = 6$ and its influence to PBA construction;
- formulate and substantiate rules for formation of minimax class of PBA with order $N = 6$;
- determine magnitude of side lobe of two-dimensional periodic cross-correlation function and power of minimax class for PBAs of order $N = 6$;
- evaluate the effect of inversion and cyclic shift of rows and/or columns of any PBA from minimax class on magnitude of side peaks of two-dimensional periodic cross-correlation function between the given PBA and the rest of the PBAs in this class;
- evaluate the effect of the thinned matrices location in PBAs on formation of minimax class.

Main Body

Minimax class contains all possible combinations of different PBAs for which the two-dimensional periodic cross-correlation function (2D PCCF) between any two PBAs $P^0(N)$ and $P^1(N)$ from this class has minimum modulus of maximum peak. Such class is known as $M(N)$ - class of PBAs [1].

The two-dimensional periodic autocorrelation function (2D PACF) of PBA always has peak of value N^2. Level of interfering signals or level of maximum 2D PCCF peaks (ρ) for PBAs of minimax class required for correct detection of PBA in receiver under the influence of signals constructed on the basis of PBAs is given below

$$\rho < N^2 / 2. \tag{1}$$

As stated in [4], each PBA $P(N)$ by its thinning in spatial coordinates can be presented as four thinned matrices of order $N/2$.

For example, for an arbitrary array $P^0(6)$

$$P^0(6) = \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix} \tag{2}$$

the thinned matrices are given below

$$A(3) = \begin{bmatrix} - & - & - \\ + & + & + \\ + & + & + \end{bmatrix},\ B(3) = \begin{bmatrix} - & + & + \\ - & + & + \\ - & + & + \end{bmatrix},\ C(3) = \begin{bmatrix} - & + & + \\ + & - & + \\ + & + & - \end{bmatrix},\ \overline{D}(3) = \begin{bmatrix} - & - & + \\ - & + & - \\ + & - & - \end{bmatrix}.$$

It was found that for PBA of order $N = 6$ there is a finite number of thinned matrices of order $N/2 = 3$ [5], whose $4! = 24$ permutations lead to the construction of the PBA. Such structures are shown in Table 1.

Table 1.

Thinned matrices of order *N*/2=3

$A_0(3)$	$A_1(3)$	$A_2(3)$	$\overline{A_0}(3)$	$\overline{A_1}(3)$	$\overline{A_2}(3)$
$\begin{bmatrix}-&-&-\\+&+&+\\+&+&+\end{bmatrix}$	$\begin{bmatrix}+&+&+\\-&-&-\\+&+&+\end{bmatrix}$	$\begin{bmatrix}+&+&+\\+&+&+\\-&-&-\end{bmatrix}$	$\begin{bmatrix}+&+&+\\-&-&-\\-&-&-\end{bmatrix}$	$\begin{bmatrix}-&-&-\\+&+&+\\-&-&-\end{bmatrix}$	$\begin{bmatrix}-&-&-\\-&-&-\\+&+&+\end{bmatrix}$
$B_0(3)$	$B_1(3)$	$B_2(3)$	$\overline{B_0}(3)$	$\overline{B_1}(3)$	$\overline{B_2}(3)$
$\begin{bmatrix}-&+&+\\-&+&+\\-&+&+\end{bmatrix}$	$\begin{bmatrix}+&-&+\\+&-&+\\+&-&+\end{bmatrix}$	$\begin{bmatrix}+&+&-\\+&+&-\\+&+&-\end{bmatrix}$	$\begin{bmatrix}+&-&-\\+&-&-\\+&-&-\end{bmatrix}$	$\begin{bmatrix}-&+&-\\-&+&-\\-&+&-\end{bmatrix}$	$\begin{bmatrix}-&-&+\\-&-&+\\-&-&+\end{bmatrix}$
$C_0(3)$	$C_1(3)$	$C_2(3)$	$\overline{C_0}(3)$	$\overline{C_1}(3)$	$\overline{C_2}(3)$
$\begin{bmatrix}-&+&+\\+&-&+\\+&+&-\end{bmatrix}$	$\begin{bmatrix}+&-&+\\+&+&-\\-&+&+\end{bmatrix}$	$\begin{bmatrix}+&+&-\\-&+&+\\+&-&+\end{bmatrix}$	$\begin{bmatrix}+&-&-\\-&+&-\\-&-&+\end{bmatrix}$	$\begin{bmatrix}-&+&-\\-&-&+\\+&-&-\end{bmatrix}$	$\begin{bmatrix}-&-&+\\+&-&-\\-&+&-\end{bmatrix}$
$D_0(3)$	$D_1(3)$	$D_2(3)$	$\overline{D_0}(3)$	$\overline{D_1}(3)$	$\overline{D_2}(3)$
$\begin{bmatrix}+&+&-\\+&-&+\\-&+&+\end{bmatrix}$	$\begin{bmatrix}-&+&+\\+&+&-\\+&-&+\end{bmatrix}$	$\begin{bmatrix}+&-&+\\-&+&+\\+&+&-\end{bmatrix}$	$\begin{bmatrix}-&-&+\\-&+&-\\+&-&-\end{bmatrix}$	$\begin{bmatrix}+&-&-\\-&-&+\\-&+&-\end{bmatrix}$	$\begin{bmatrix}-&+&-\\+&-&-\\-&-&+\end{bmatrix}$

The 2D PACFs for thinned matrices from Table 1 are given in Table 2.

Table 2.

2D PACFs of thinned matrices of order *N*/2=3

Types of thinned matrices	$A_0(3)$, $A_1(3)$, $A_2(3)$, $\overline{A_0}(3)$, $\overline{A_1}(3)$, $\overline{A_2}(3)$	$B_0(3)$, $B_1(3)$, $B_2(3)$, $\overline{B_0}(3)$, $\overline{B_1}(3)$, $\overline{B_2}(3)$	$C_0(3)$, $C_1(3)$, $C_2(3)$, $\overline{C_0}(3)$, $\overline{C_1}(3)$, $\overline{C_2}(3)$	$D_0(3)$, $D_1(3)$, $D_2(3)$, $\overline{D_0}(3)$, $\overline{D_1}(3)$, $\overline{D_2}(3)$
2D PACF of thinned matrices	$R_A=\begin{bmatrix}9&9&9\\-3&-3&-3\\-3&-3&-3\end{bmatrix}$	$R_B=\begin{bmatrix}9&-3&-3\\9&-3&-3\\9&-3&-3\end{bmatrix}$	$R_C=\begin{bmatrix}9&-3&-3\\-3&9&-3\\-3&-3&9\end{bmatrix}$	$R_D=\begin{bmatrix}9&-3&-3\\-3&-3&9\\-3&9&-3\end{bmatrix}$

Statement 1. Value of elements imbalance in thinned matrices of order *N*/2=3

$$\Delta = K^{(+)} - K^{(-)} = \pm N ,$$

where $K^{(+)}$ and $K^{(-)}$ is number of symbols $+1$ and -1 respectively, is given below

$$\Delta_{A(3)} = \Delta_{B(3)} = \Delta_{C(3)} = \Delta_{D(3)} = N/2 = 3 ,$$

$$\Delta_{\overline{A}(3)} = \Delta_{\overline{B}(3)} = \Delta_{\overline{C}(3)} = \Delta_{\overline{D}(3)} = -N/2 = -3 .$$

If the element imbalance of PBA has a positive value such a PBA is called direct. For the negative value of the element imbalance the PBA is called inverse.

Property 1. The PBA can be constructed from three direct matrices and one inverse and vice versa. Only in this case element imbalance of resulting PBA is equal to $\Delta = \pm 6$.

For development of minimax class constructing method the 2D PCCF calculated for $P^1(N)$ и $P^2(N)$ PBAs will be used. It is denoted as follows

$$B(N) = \left\| b_{m,n} \right\|, \qquad (3)$$

where $m = \overline{0, N_1 - 1}$ — numbers of 2D PCCF rows; $n = \overline{0, N_2 - 1}$ — numbers of 2D PCCF columns.

Elements of 2D PCCF (3) between PBAs $P^1(N)$ and $P^2(N)$ are calculated using an equation

$$b_{m,n} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} p_{i,j}^1 p_{i+m,j+n}^2 ,$$

where $p_{i,j}^1$ — elements of $P^1(N)$ PBA; $p_{i,j}^2$ — elements of $P^2(N)$ PBA; while values *i*+*m* and *j*+*n* are calculated modulo *N*.

The following task must be solved for construction of minimax class. Suppose that an arbitrary PBA is given. It will be used as the base PBA for minimax class formation.

Let use for our purpose the PBA (2). It is known [4] that for new PBA constructing from thinned matrices of the base PBA the next methods can be used:

- cyclic shifts of rows and/or columns of thinned matrices;
- inverse of thinned matrices elements;
- permutation of thinned matrices.

Consider all these methods in detail.

2D PCCF between the base PBA of size 6×6 and PBA with cyclically shifted rows and/or columns of thinned matrices was analyzed. It was found that magnitude of 2D PCCF side lobe maximum peak is 24 and it contradicts (1).

Consider an inverse of PBA's thinned matrices elements. Base array (2) consists of thinned matrices

$$A(3)B(3)C(3)\overline{D}(3) . \tag{4}$$

Property 1. Can be accomplished if PBA will be formed without thinned matrices permutation and using the following rules

$$\left.\begin{array}{l} P^0(6) = A(3)B(3)C(3)\overline{D}(3), P^1(6) = A(3)B(3)\overline{C}(3)D(3), \\ P^2(6) = A(3)\overline{B}(3)C(3)D(3), P^3(6) = \overline{A}(3)B(3)C(3)D(3), \\ P^4(6) = \overline{A}(3)\overline{B}(3)\overline{C}(3)D(3), P^5(6) = \overline{A}(3)\overline{B}(3)C(3)\overline{D}(3), \\ P^6(6) = \overline{A}(3)B(3)\overline{C}(3)\overline{D}(3), P^7(6) = A(3)\overline{B}(3)\overline{C}(3)\overline{D}(3). \end{array}\right\} . \tag{5}$$

Calculation of 2D PCCF between all PBAs constructed on the basis of rules (5) gives the following combinations of PBAs for which the maximum magnitude of 2D PCCF side lobe is $\rho = \pm 12$

$$\left.\begin{array}{l} P^0(6) = A(3)B(3)C(3)\overline{D}(3) \\ P^1(6) = A(3)B(3)\overline{C}(3)D(3) \\ P^2(6) = A(3)\overline{B}(3)C(3)D(3) \\ P^3(6) = \overline{A}(3)B(3)C(3)D(3) \end{array}\right\} . \tag{6}$$

However, more combinations from (5) can lead to appropriate maximum peaks.

Property 2. The inverse of one PBA from minimax class does not lead to increasing of 2D PCCF side peaks for given PBA and other PBAs from minimax class.

Other combinations can be obtained by replacing each row in (6) with its inverted form. The expression (6) is a combination of direct thinned matrices for which the 2D PCCF has maximum peaks no greater than $\rho = \pm 12$ and this expression it taken as a base.

Further research allowed revealing of the following property.

Property 3. Cyclic shift by rows and/or columns of one PBA from minimax class does not lead to increasing of 2D PCCF side peaks for given PBA and other PBAs from minimax class.

The matrices (7) are constructed on the basis of rule (6).

Maximum magnitude of 2C PCCF side lobes between PBAs from (6) is not greater than $\rho = \pm 12$ which is acceptable (1) for a minimax class.

$$P^0(6) = \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}, \quad P^1(6) = \begin{bmatrix} - & - & - & + & - & + \\ + & + & - & + & - & - \\ + & - & + & + & + & + \\ - & + & + & - & - & + \\ + & - & + & + & + & + \\ - & - & - & + & + & + \end{bmatrix},$$

$$P^2(6) = \begin{bmatrix} - & + & - & - & - & - \\ - & + & + & + & + & - \\ + & + & + & - & + & - \\ + & + & - & - & + & + \\ + & + & + & - & + & - \\ + & - & + & + & - & + \end{bmatrix}, \quad P^3(6) = \begin{bmatrix} + & - & + & + & + & + \\ - & + & + & + & + & - \\ - & - & - & + & - & + \\ + & + & - & - & + & + \\ - & - & - & + & - & + \\ + & - & + & + & - & + \end{bmatrix}. \tag{7}$$

Evaluate an effect of thinned matrices permutation in the PBA $P^1(6)$ on 2D PCCF between $P^0(6)$ and $P^1(6)$. Permute thinned matrices $B(3)$ and $C(3)$ in PBA $P^1(6)$

$$A(3)C(3)B(3)\overline{D}(3) \tag{8}$$

and calculate 2D PCCF for PBAs $P^0(6)$ and $P^1(6)$

$$P^0(6) = \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}, \quad P^1(6) = \begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & + & + & - & + & + \\ - & - & + & + & + & - \\ + & + & + & + & + & - \\ - & + & + & - & + & - \end{bmatrix}, \quad B(6) = \begin{bmatrix} 20 & 0 & 8 & 0 & 8 & 0 \\ 0 & 4 & 0 & -8 & 0 & 4 \\ -4 & 0 & -4 & 0 & 8 & 0 \\ 0 & 16 & 0 & -8 & 0 & -8 \\ -4 & 0 & 8 & 0 & -4 & 0 \\ 0 & 4 & 0 & 4 & 0 & -8 \end{bmatrix}. \tag{9}$$

Two thinned matrices $A(3)$ and $\overline{D}(3)$ keep initial locations (4) and (8). Magnitude of 2D PCCF maximum peak (9) is quite high. It can be concluded that for the creation of new PBAs for the minimax class the thinned matrices should not be repeated in their places. It is possible, for example, in case of following thinned matrices permutations

$$A(3)B(3)C(3)\overline{D}(3),$$
$$A(3)C(3)\overline{D}(3)B(3),$$
$$A(3)\overline{D}(3)B(3)C(3).$$

2D PCCF for these thinned matrices presented in Table 3.

The above approach and the properties of thinned matrices of PBA with order $N = 6$ allow creation of a stepwise algorithm for constructing of minimax arrays on the basis of any arbitrary base PBA.

Algorithm

Step 1. Construct by any known method the base PBA of order $N = 6$ and present it in the form of thinned matrices of order $N/2 = 3$ by thinning in the spatial coordinates.

Step 2. Calculate 2D PCCF for each matrix.

Step 3. Taking into account the Property 1 determine which of thinned matrices is inverted in relation to the other. Denote inverted matrix as $\overline{D}(3)$ and other as $A(3)$, $B(3)$ and $C(3)$ in any order.

Step 4. Construct PBAs using equations

$$\left.\begin{array}{lll} A(3)B(3)C(3)\overline{D}(3), & A(3)B(3)\overline{C}(3)D(3), & A(3)\overline{B}(3)C(3)D(3), \\ \overline{A}(3)B(3)C(3)D(3), & A(3)D(3)B(3)\overline{C}(3), & A(3)D(3)\overline{B}(3)C(3), \\ A(3)\overline{D}(3)B(3)C(3), & \overline{A}(3)D(3)B(3)C(3), & A(3)C(3)D(3)\overline{B}(3), \\ A(3)C(3)\overline{D}(3)B(3), & A(3)\overline{C}(3)D(3)B(3), & \overline{A}(3)C(3)D(3)B(3). \end{array}\right\}.$$

Table 3.

Two-dimensional periodic cross-correlation functions

PBA 1	PBA 2	2D PCCF
$A(3)B(3)C(3)\overline{D}(3)$	$A(3)C(3)\overline{D}(3)B(3)$	
$\begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & + & - & + \\ - & - & - & + & + & + \\ + & + & + & - & + & + \\ - & - & + & + & - & + \\ + & + & + & + & + & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} 8 & 12 & 8 & 0 & 8 & 0 \\ 8 & -4 & -4 & -4 & -4 & 8 \\ -4 & 0 & -4 & 0 & -4 & 12 \\ 8 & 8 & -4 & -4 & -4 & -4 \\ -4 & 0 & -4 & 12 & -4 & 0 \\ 8 & -4 & -4 & 8 & -4 & -4 \end{bmatrix}$
$A(3)B(3)C(3)\overline{D}(3)$	$A(3)\overline{D}(3)B(3)C(3)$	
$\begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & - & - & + \\ - & - & + & + & + & + \\ + & - & + & + & + & - \\ - & + & + & - & + & + \\ + & + & + & - & + & - \\ - & + & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} 8 & -4 & 8 & -4 & 8 & 8 \\ 12 & 8 & 0 & -4 & 0 & -4 \\ -4 & 8 & -4 & -4 & -4 & -4 \\ 0 & 8 & 0 & -4 & 12 & -4 \\ -4 & -4 & -4 & 8 & -4 & -4 \\ 0 & 8 & 12 & -4 & 0 & -4 \end{bmatrix}$
$A(3)C(3)\overline{D}(3)B(3)$	$A(3)\overline{D}(3)B(3)C(3)$	
$\begin{bmatrix} - & - & - & + & - & + \\ - & - & - & + & + & + \\ + & + & + & - & + & + \\ - & - & + & + & - & + \\ + & + & + & + & + & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} - & - & - & - & - & + \\ - & - & + & + & + & + \\ + & - & + & + & + & - \\ - & + & + & - & + & + \\ + & - & + & + & + & + \\ - & + & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} 8 & 8 & 8 & -4 & 8 & -4 \\ -4 & 0 & 8 & 0 & -4 & 12 \\ -4 & 8 & -4 & -4 & -4 & -4 \\ -4 & 0 & -4 & 12 & 8 & 0 \\ -4 & 8 & -4 & -4 & -4 & -4 \\ 8 & 12 & -4 & 0 & -4 & 0 \end{bmatrix}$

Thus, it was found that the power of PBA minimax class is $\Psi_M(6)=12$ perfect binary arrays, while the magnitude of the maximum peak is $\rho=\pm 12$.

Minimax class of PBA is given in Table 4.

Table 4.

Minimax class of PBA with order $N = 6$

$\begin{bmatrix} - & - & - & + & - & + \\ - & - & + & - & + & + \\ + & - & + & + & + & + \\ + & - & - & + & + & - \\ + & - & + & + & + & + \\ + & + & + & - & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & + & - & + \\ + & + & - & + & - & - \\ + & - & + & + & + & + \\ - & + & + & - & - & + \\ + & - & + & + & + & + \\ - & - & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} - & + & - & - & - & - \\ - & + & + & + & + & - \\ + & + & + & - & + & - \\ + & + & - & - & + & + \\ + & + & + & - & + & - \\ + & - & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} + & - & + & + & + & + \\ - & + & + & + & + & - \\ - & - & - & + & - & + \\ + & + & - & - & + & + \\ - & - & - & + & - & + \\ + & - & + & + & - & + \end{bmatrix}$
$\begin{bmatrix} - & + & - & + & - & - \\ - & + & + & - & + & - \\ + & + & + & - & + & + \\ - & - & + & + & - & + \\ + & - & + & + & + & + \\ - & - & + & - & + & + \end{bmatrix}$	$\begin{bmatrix} - & + & - & + & - & - \\ + & - & - & + & - & + \\ + & + & + & - & + & + \\ + & + & - & - & - & + \\ + & - & + & + & + & + \\ + & + & - & + & - & - \end{bmatrix}$	$\begin{bmatrix} - & - & - & - & - & + \\ - & - & + & + & + & + \\ + & - & + & + & + & - \\ - & + & + & - & + & + \\ + & + & + & - & + & - \\ - & + & + & + & + & - \end{bmatrix}$	$\begin{bmatrix} + & + & + & + & + & - \\ - & - & + & + & + & + \\ - & + & - & - & - & + \\ - & + & + & - & + & + \\ - & - & - & + & - & + \\ - & + & + & + & + & - \end{bmatrix}$
$\begin{bmatrix} - & - & - & + & - & + \\ + & + & + & - & - & - \\ + & + & + & - & + & + \\ + & + & - & - & + & - \\ + & + & + & + & + & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} - & - & - & + & - & + \\ - & - & - & + & + & + \\ + & + & + & - & + & + \\ - & - & + & + & - & - \\ + & + & + & + & + & - \\ + & - & - & + & - & + \end{bmatrix}$	$\begin{bmatrix} - & + & - & - & - & - \\ + & - & + & + & - & + \\ + & - & + & + & + & - \\ + & - & - & + & + & + \\ + & - & + & - & + & + \\ - & - & + & + & + & + \end{bmatrix}$	$\begin{bmatrix} + & - & + & + & + & + \\ + & - & + & + & - & + \\ - & + & - & - & - & + \\ + & - & - & + & + & + \\ - & + & - & + & - & - \\ - & - & + & + & + & + \end{bmatrix}$

It is possible to develop a new class of multiparametric error-correcting $M(n)$-codes of length $n = N^2$ on the basis of minimax class of PBA. Their properties and procedures of coding and decoding studied in [1].

It is assumed that the encoder and decoder of authorized users utilize for coding and decoding of each next symbol the same PBA from the equivalence class. Such PBA is constructed on the basis of one PBA (base PBA) from minimax class by means of cyclic shifts of rows and/or columns. Base PBAs are operatively changed for each symbol according to some algorithm, which managed by a secret key. It is this array determines a code word of $M(n)$-code which will be applied for the transmission of next message.

An attacker is not able to determine which PBA from minimax class determined parameters of message transmission in system. Only fact of message transmission can be revealed. Thus, it is possible to create a single-channel cryptographic information transfer system on the basis of single PBA of minimax class. For all other PBAs from minimax class similar systems can be built.

Due to the fact that the signals based on the PBA of the minimax class are the minimax as well, they have a minimal impact on the other signals, which are built on the basis of other PBAs from minimax class. Therefore, the single-channel cryptographic information transfer systems can be used to transmit information in a single communication channel on condition that all the signals are constructed on the basis of the same minimax class. The number of channels of multi-channel cryptographic information transfer system is determined by the power of minimax class of PBAs.

Hypothetically, it is clear that with the growth of the PBA order the power of minimax class and number of channels in multi-channel cryptographic information transfer system grows as well. However, the redundancy of $M(n)$-code which is used for a single character of the original message transmission increases correspondingly. Thus, it is possible to provide any desired number of channels in a multi-channel cryptographic information transfer system by reducing the transmission rate, since the growth of minimax class power causes an increase of $M(n)$-code redundancy.

Conclusions

This paper presents an algorithm for constructing of minimax class of PBAs with order $N = 3 \cdot 2^k$ which can become the basis for creation of recurrent algorithms for constructing of $M(N)$-classes for PBAs of arbitrary orders.

A method of constructing a single-channel cryptographic information transfer system proposed. It is shown how a multi-channel system can be organized. Limits on the number of channels in this information transfer system determined. The way and cost of an increase in number of channels discussed.

References

1. Мазурков, М.И. Класс минимаксных корректирующих кодов на основе совершенных двоичных решеток / М.И. Мазурков // Радиоэлектроника (Изв. вузов). – 2011. – №9. – С. 24-39.
2. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Радиоэлектроника (Изв. вузов). – 2008. – № 11. – С. 53-57.
3. Кушниренко, Н.И. Метод криптографической передачи информации на базе эквивалентного класса совершенных двоичных решеток / Н.И. Кушниренко, В.Я. Чечельницкий // Інформатика та математичні методи в моделюванні. — 2014. — Т.4. — №3. — С. 210-218.

4. Чечельницкий, В.Я. Метод построения полного класса совершенных двоичных решеток порядка $N = 2^k$ / В.Я. Чечельницкий // Радиоэлектроника (Изв. вузов). – 2006. – №9. – С. 44-53.
5. Мазурков, М.И. Свойства полного класса совершенных двоичных решеток на 36 элементов / М.И. Мазурков, В.Я. Чечельницкий // Радиоэлектроника (Изв. вузов). – 2004. – № 6. – С. 56-64.

ПОБУДОВА МІНІМАКСНОГО КЛАСУ ДОСКОНАЛИХ ДВІЙКОВИХ РЕШІТОК ПОРЯДКУ N=6 ДЛЯ БАГАТОКАНАЛЬНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Н.І. Кушніренко, В.Я. Чечельницький, Л.А. Кузнецова

Одеський національний політехнічний університет,
проспект Шевченка, 1, Одеса, 65044, Україна; e-mail: natalka_kni@ukr.net

У роботі представлено метод побудови мінімаксного класу досконалих двійкових решіток порядку N=6, встановлена його потужність, визначено рівень максимальних піків двовимірної періодичної взаємокореляційної функції між досконалими двійковими решітками мінімаксного класу. Даний метод розроблений на основі аналізу структурних і кореляційних властивостей проріджених матриць досконалих двійкових решіток. Запропоновано метод побудови одноканальної і багатоканальної криптографічних систем передачі інформації на основі кодів, які розроблені на базі мінімаксного класу досконалих двійкових решіток. Наведено обмеження на кількість каналів багатоканальної системи і зазначений спосіб подолання цих обмежень.
Ключові слова: мінімаксний клас, досконала двійкова решітка, проріджена матриця, коректувальні коди, криптографічна система передачі інформації, захист інформації

ПОСТРОЕНИЕ МИНИМАКСНОГО КЛАССА СОВЕРШЕННЫХ ДВОИЧНЫХ РЕШЕТОК ПОРЯДКА N=6 ДЛЯ МНОГОКАНАЛЬНОЙ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Н.И. Кушниренко, В.Я. Чечельницкий, Л.А. Кузнецова

Одесский национальный политехнический университет,
проспект Шевченко, 1, Одесса, 65044, Украина; e-mail: natalka_kni@ukr.net

В работе представлен метод построения минимаксного класса совершенных двоичных решеток порядка N=6, установлена его мощность, определен уровень максимальных пиков двумерной периодической взаимнокорреляционной функции между совершенными двоичными решетками минимаксного класса. Данный метод разработан на основе анализа структурных и корреляционных свойств прореженных матриц совершенных двоичных решеток. Предложен метод построения одноканальной и многоканальной криптографической системы передачи информации на основе кодов, которые построены на базе минимаксного класса СДР. Приведены ограничения на количество каналов многоканальной системы и указан способ преодоления этих ограничений.
Ключевые слова: минимаксный класс, совершенная двоичная решетка, прореженная матрица, корректирующие коды, криптографическая система передачи информации, защита информации