ISSN 0735-2727, Radioelectronics and Communications Systems, 2013, Vol. 56, No. 3, pp. 133–140. © Allerton Press, Inc., 2013.
Original Russian Text © M.I. Mazurkov, 2013, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2013, Vol. 56, No. 3, pp. 36–44.

Composite Matrix Cipher Based on Perfect Binary Arrays

M. I. Mazurkov
Odessa National Polytechnic University, Odessa, Ukraine
Received in final form January 18, 2013

Abstract—A composite matrix cipher consisting of four partial ciphers and based on perfect binary arrays has been proposed. This cipher possesses an easily controlled level of data protection from unauthorized access and other practically acceptable computational properties.

DOI: 10.3103/S0735272713030047

The issues of synthesis and application of perfect binary arrays (PBA) were discussed in numerous papers, for example [1–13], in respect to different radio engineering problems, such as synthesis of the antenna aperture, the construction of perfect time-and-frequency codes, construction of new classes of block error-correcting codes, construction of new classes of orthogonal, biorthogonal and minimax signals with the property of multiloop cyclic shift, and the construction of classes of minimax error-correcting codes with majority decoding, etc.

The purpose of this study is to develop single-round and multi-round composite matrix ciphers on the basis of complete classes and equivalent classes of perfect binary arrays.

By perfect binary array is meant a two-dimensional sequence matrix

$$H(N) = ||h_{i,j}||,\ i,j = \overline{0,N-1},\ h_{i,j} \in \{-1,1\}, \tag{1}$$

having an ideal two-dimensional periodic autocorrelation function (TPACF) with the following elements

$$R(\tau_1,\tau_2) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} h_{i,j}h_{i+\tau_1,j+\tau_2} = \begin{cases} N^2, & \tau_1 = \tau_2 = 0, \\ 0, & \text{at other } \tau_1 \text{ and } \tau_2, \end{cases} \tag{2}$$

where $\tau_1,\tau_2 = \overline{0,N-1}$, $N = 2^s$, or $N = 3\times 2^s$, s is an arbitrary natural number. The issues of synthesis of different PBA classes are considered in many sources [1–11], and from the content of the specified papers it follows:

ASSERTION

An algorithm [14] exists that enables us to restore (synthesize) an array proper from the complete $U(N)$-class of PBA [1] on the basis of the array number; and also another algorithm exists that enables us to recover the transposition proper by using the transposition number from $N!$ transpositions.

SINGLE-ROUND CIPHER

The essence of the proposed single-round matrix cipher based on PBA consists in the composition of four partial independent between themselves ciphers:

— cipher 1 determines the structure of working PBA and, consequently, the structure of the ciphering matrix consisting of allowed and disallowed cells, where the open text is consecutively entered row-by-row;

— cipher 2 represents an algorithm of rowwise transposition of the ciphering matrix aimed at mixing the symbols of open text;