ISSN 0735-2727, Radioelectronics and Communications Systems, 2013, Vol. 56, No. 9, pp. 448–455. © Allerton Press, Inc., 2013.
Original Russian Text © M.I. Mazurkov, A.V. Sokolov, 2013, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2013, Vol. 56, No. 9, pp. 34–43.

Nonlinear Substitution S-boxes Based on Composite Power Residue Codes

M. I. Mazurkov and A. V. Sokolov

Odessa National Polytechnic University, Odessa, Ukraine

Received in final form August 15, 2013

Abstract—A design technique based on the composite power residue codes has been proposed for building new constructions of nonlinear substitution *S*-boxes of length $N = 256$ and volume $|S| = 8.6248\times10^{13}$. The synthesized constructions possess good cryptographic properties, appreciably amplify and extend the class of Nyberg constructions of the Rijndael cipher and also ensure the possibility of their application as a long-term key.

DOI: 10.3103/S0735272713090045

Power residue codes are widely used for building normal, composite and large systems of discrete frequency signals with large bandwidth-duration product and the specified structural, distant and correlation properties [1]. However, the issues of building the nonlinear *S*-boxes based on composite power residue codes have not been adequately studied [2].

The purpose of this paper is to develop a technique for building nonlinear substitution *S*-boxes based on composite power residue codes with good cryptographic properties in relation to the Rijndael/AES cipher.

Irrespective of the selected architecture of block symmetrical cipher, be it the Feistel Network or SP-network, the main component determining the resistance of cryptographic transformation to the main kinds of cryptanalysis attacks is the reliability of nonlinear *S*-box of cipher performing the mapping of a group of input bits x_i into a group of output bits y_i in accordance with the rule of coding *Q*-sequence that completely determines the structure and cryptographic properties of *S*-box.

Let us assume, for example, that the following coding *Q*-sequence is specified:

$$Q_1 = \{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15\}, \quad (1)$$

that corresponds to the absence of substitution, i.e., to direct mapping of input bits of *S*-box into the output ones: $y_i = x_i$. It is obvious that such *S*-box lacks the property of cryptosecurity. Nevertheless, coding *Q*-sequence (1) does not contain repeating elements: the substitution operation performed by using this *S*-box is completely reversible. Such *S*-box is called bijective [2] and can form the basis for building the substitution constructions of high cryptographic-quality.

Owing to the strong interrelation of the cryptosecurity of block symmetrical ciphers and bijective *S*-boxes utilized in them, the problem of building large sets of coding *Q*-sequences that might form the basis for building the cryptographic-quality *S*-boxes is topical. The studies of many researchers have dealt with solving of the specified problem, however the existing methods for building *Q*-sequences either lead to cryptographically vulnerable *S*-boxes or allow only a small number of such blocks to be constructed.

For example, in building the *S*-box of the Rijndael/AES cipher [3] its designers, Daemen and Rijmen, selected for a basis the K. Nyberg construction [2] that represents the mapping in the form of multiplicatively inverse elements of $GF(2^k)$ field in double modulus:

$$y = x^{-1} \bmod d[f(x), p], \ \ y, x \in GF(2^k), \quad (2)$$

combined with affine transformation

$$b = Ay + a, \ \ a, b \in GF(2^k), \quad (3)$$