ISSN 0735-2727, Radioelectronics and Communications Systems, 2013, Vol. 56, No. 11, pp. 513–521. © 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. 11, pp. 16–24.

Nonlinear Transformations Based on Complete Classes of Isomorphic and Automorphic Representations of Field GF(256)

M. I. Mazurkov and A. V. Sokolov

Odessa National Polytechnic University, Odessa, Ukraine

Received in final form September 30, 2013

Abstract—A complete class of maximum-period linear recurrent sequences (MLRS) of volume ψ = 55,296 based on all automorphic and isomorphic representations of the main *GF*(256) field has been built. Constructions of *S*-boxes based on MLRS and having length N = 256 with cryptographic properties as good as the Nyberg construction of Rijndael cipher have been proposed. The total number of substitution *S*-boxes synthesized by the constructive method amounts to $|S| = 7.4518\times10^{16}$ that makes it possible to use them as a long-term key.

DOI: 10.3103/S0735272713110022

Nonlinear substitution *S*-boxes [1] are a basic component of modern algorithms of block encryption and hashing. These *S*-boxes perform the mapping of a group of input bits x_i into another group of output bits y_i in accordance with the rule uniquely specified by the coding *Q*-sequence [2]. The application of enumerative techniques for the synthesis of *Q*-sequences is not possible, since already with the *S*-box length $N = 256$, the number of existing *Q*-sequences reaches an astronomical value $J = 256! \approx 1.17\times10^{505}$.

At the same time, as the length N increases, the correlation, remote, and cryptographic properties of *S*-boxes significantly improve; that is why the development of constructive (other than enumerative) techniques of synthesis of large sets of coding *Q*-sequences with large lengths is a topical problem.

The purpose of this paper is to develop a constructive synthesis method and analyze cryptographic properties of single-byte *S*-boxes having length N = 256 and built on the basis of complete classes of isomorphic and automorphic representations of field *GF*(256) with elements in decimal form.

The basic theorem of Galois fields states that for each prime number p and natural n there is a unique finite algebraic field of order p^n accurate to isomorphism [3]. It should be noted, however, that the methods of synthesis of codes, ensembles of noise-like signals, the cost of hardware equipment for generation and processing of codes and signals materially depend on the choice of the type of field representation. Hence, from the application viewpoint it is expedient to consider different representations of the field of order p^n as different fields [4, 5].

For the sake of simplicity in presenting the material of this study we shall introduce the following designations and definitions.

Quantity $|f_q^k|$ is the number of primitive polynomials $f(x)$ of power k over each isomorphic subfield *GF*(q) determined by expression

$$|f_q^k| = \varphi(q^k - 1)/k,$$

where $\varphi(q^k - 1)$ is the Euler phi function.

Quantity $|\theta_q^k|$ is the number of primitive roots in field (subfield) $GF(q^k)$ determined by expression

$$|\theta_q^k| = \varphi(q^k - 1).$$