ISSN 0735-2727, Radioelectronics and Communications Systems, 2015, Vol. 58, No. 5, pp. 220–227. © Allerton Press, Inc., 2015.
Original Russian Text © A.V. Sokolov, N.A. Barabanov, 2015, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2015, Vol. 58, No. 5, pp. 41–49.

Algorithm for Removing the Spectral Equivalence of Component Boolean Functions of Nyberg-Design S-Boxes

A. V. Sokolov* **and N. A. Barabanov**

Odessa National Polytechnic University, Odessa, Ukraine
**e-mail: radiosquid@gmail.com*

Received in final form December 25, 2014

Abstract—The phenomenon of spectral equivalence of component Boolean functions of Nyberg-design *S*-boxes has been investigated. An effective algorithm for removing the spectral equivalence is proposed based on the introduction of random modifier into each component Boolean function of *S*-box. The analysis of *S*-boxes generated on the basis of the proposed algorithm corroborates its efficiency and shows high cryptographic quality of *S*-boxes.

DOI: 10.3103/S0735272715050040

Substitution box (*S*-box) is the main primitive determining the cryptographic properties of modern block encryption algorithms. The Shannon encryption principles imply that the task of *S*-box is confusion, i.e., provision of complex and nonlinear relationship between the key and plain text [1].

The typical design of the state-of-art *S*-box consists of decryptor, encryptor and the system of interconnections between them. For example, a schematic diagram of *S*-box for the three-bit ($k = 3$) input word is shown in Fig. 1. The structure of *S*-box and its cryptographic properties are completely determined by the coding *Q*-sequence of length $N = 2^k$. For the specified example it assumes the form: $\mathbf{Q} = \{5, 0, 4, 2, 6, 1, 7, 3\}$.

In turn, in order to apply the mathematical tools of Boolean functions for estimating the cryptographic quality of *S*-box, the coding *Q*-sequence can be expanded into a set of *k*-component Boolean functions f_1, f_2, f_3 presented in the form of their truth tables $\mathbf{F}^{(1)}$, $\mathbf{F}^{(2)}$, $\mathbf{F}^{(3)}$. For the specified example the truth tables are presented in Table 1.

The main criteria applicable to modern *S*-boxes include the large nonlinearity distance in the sense of distance to the affine code, low level of correlation between the input and output data vectors, good avalanche effect, and large periods of reset [2]. In this case, the cryptographic quality of *S*-boxes significantly increases with the rise of length *N* of coding *Q*-sequence.

The problem of constructing *S*-boxes satisfying the above criteria is reduced to the design of high-quality structures of coding *Q*-sequences. Nevertheless, even for relatively small lengths, the quantity of possible structures of coding *Q*-sequences soars by the law $J = N!$ that makes prohibitive their search by the method of full enumeration. For example, if the length of input word applied in Rijndael/AES cryptographical transformation is equal to $k = 8$, the quantity of possible variants of coding *Q*-sequences will reach an astronomical value $J = 256!$. Thus, even for relatively small lengths of coding *Q*-sequences the construction of *S*-boxes with high cryptographic quality is possible only by using non-exhaustive search methods.

The Rijndael cryptoalgorithm makes use of the well-known K. Nyberg design [3] that represents the multiplicative inverse transformation of input elements over field $GF(2^8)$

$$y = x^{-1} \operatorname{modd}[g(z), p], \quad y, x \in GF(2^8), \tag{1}$$

at the output of which the affine transformation is applied; this transformation has the form:

$$y' = \mathbf{A}y + \mathbf{a}, \quad \mathbf{a} \in GF(2^k), \tag{2}$$