ISSN 0735-2727, Radioelectronics and Communications Systems, 2014, Vol. 57, No. 8, pp. 376–381. © Allerton Press, Inc., 2014.
Original Russian Text © M.I. Mazurkov, A.V. Sokolov, 2014, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2014, Vol. 57, No. 8, pp. 54–60.

Method of S-Boxes Synthesis Based on the Criterion of Zero Correlation between the Output and Input Data Vectors and the Strict Avalanche Criterion

M. I. Mazurkov and A. V. Sokolov*
Odessa National Polytechnic University, Odessa, Ukraine
**e-mail:* radiosquid@gmail.com

Received in final form May 2, 2014

Abstract—A constructive method of synthesis of correlation-immune *S*-boxes of length $N = 256$ satisfying the strict avalanche criterion has been proposed. Its properties and estimates of the number of optimal *S*-boxes that can be obtained by using the proposed method were determined. In addition a regular method of multiplication of the obtained optimal *S*-boxes was proposed.

DOI: 10.3103/S0735272714080068

Cryptographic *S*-box is the main component of practically all modern symmetric ciphers that determines its avalanche effect, correlation between output vectors y_j and input vectors x_j, and also the nonlinearity. The issues of synthesis of cryptographically high-quality *S*-boxes have found its reflection in many papers [1–6], where a particular criterion was selected as a basis for their synthesis. However, for constructing new high-speed encryption algorithms it is of interest to employ such *S*-boxes that simultaneously comply with several criteria of cryptographic quality and thus make it possible at the same time to effectively resist several kinds of cryptoanalysis attacks.

Among the most significant from the practical viewpoint quality criteria of *S*-boxes are the criterion of independence of *S*-box output vectors y_j on *S*-box input vectors x_j that is known as correlation immunity [1], and also the strict avalanche criterion [2]. *S*-box of length $N = 2^k$ is called correlation-immune, if each component Boolean function F_j, $j = \overline{1,k}$ of this *S*-box possesses the correlation immunity of the first order or higher $m \geq 1$that is valid then and only then, when its Walsh–Hadamard spectral coefficients are as follows:

$$W(\omega) = F_j A(n) = \sum_{i=0}^{n-1} F_j(i)(-1)^{\langle i,\omega\rangle} = 0,$$

$$\forall\omega, \quad \mathrm{wt}(\omega) = m, \tag{1}$$

where $A(n)$ is the Walsh–Hadamard matrix of order $n = N^2$, $N = 2^m$; wt(.) is the Hamming weight; $\langle i,\omega\rangle$ is the bmod2 scalar product of coefficients of binary notation of decimal numbers that can be written in the form $(i)_{10} = (i_{s-1}, i_{s-2}, \ldots, i_0)_2$ and correspondingly $(\omega)_{10} = (\omega_{s-1}, \omega_{s-2}, \ldots, \omega_0)_2$, then

$$\langle i,\omega\rangle = \sum_{r=0}^{s-1} i_r \omega_r, \quad s = \log_2 k. \tag{2}$$

If condition (1) is satisfied for all component Boolean functions F_j, $j = \overline{1,k}$ of *S*-box, it possesses the ideal (zero) matrix of correlation coefficients $R = \| r_{\nu,\mu} \|$ of output vectors y_j and input vectors x_j [3], where correlation coefficients are equal to