ISSN 0735-2727, Radioelectronics and Communications Systems, 2013, Vol. 56, No. 8, pp. 415–423. © Allerton Press, Inc., 2013.
Original Russian Text © A.V. Sokolov, 2013, published in Izv. Vyssh. Uchebn. Zaved., Radioelektron., 2013, Vol. 56, No. 8, pp. 43–52.

Constructive Method for the Synthesis of Nonlinear S-Boxes Satisfying the Strict Avalanche Criterion

A. V. Sokolov

Odessa National Polytechnic University, Odessa, Ukraine

Received in final form July 15, 2013

Abstract—A constructive method is proposed for the synthesis of cryptographic substitution boxes (S-boxes) satisfying both the strict avalanche criterion and the high nonlinearity criterion, where smaller length S-boxes and highly nonlinear bent functions are used as a source material. In addition, effective algorithms for the reproduction of the above S-boxes have been developed.

DOI: 10.3103/S0735272713080049

The main characteristics of modern block ciphers and hash functions determining the level of their security are nonlinearity and avalanche effect. A high level of cipher nonlinearity and a good avalanche effect can be achieved at the expense of applying nonlinear transformations in the form of cryptographic S-boxes, the quality of which determines the security of cryptographic transformation in whole.

S-box represents a substitution table, where a group of input bits x_i is mapped into a group of output bits y_i in accordance with a specific rule determined by the coding Q-sequence.

For example, let us assume that the following coding Q-sequence of length $N = 8$ is specified:

$$Q = \{4\,7\,2\,6\,1\,5\,0\,3\}. \tag{1}$$

Then the functional block diagram of the corresponding S-box has the form presented in Fig. 1.

Each S-box can be presented in the form of $k = \log_2 N$ truth tables of component Boolean functions. For example, for the S-box of sequence (1) the truth tables of component Boolean functions ($k = 3$) have the form presented in Table 1.

It is common to use the distance of nonlinearity N_S in the sense of maximum of the minimal Hamming distance from each of its component Boolean functions F_i to each of the affine functions as a measure of nonlinearity of S-boxes [1]:

$$N_S = \max\left\{\min_{i,j}\{\mathrm{dist}(F_i, \varphi_j)\}\right\}, \quad i = 0,1,\ldots,k-1,\ j = 0,1,\ldots,2^{k+1}-1, \tag{2}$$

where $\varphi = \langle a,x\rangle + b$ are the code words of affine code (the first order Reed–Muller code), $\langle . \rangle$ is the scalar mod2 product, $a, x \in V_k$, V_k is the linear vector space of binary vectors having size k, $b \in \{0,1\}$, while the maximum is sought among all S-boxes.

For example, it is possible to build all code words of the affine code having length $N = 8$:

$$\left\{\begin{array}{l}
\varphi_0 = \{00000000\},\\
\varphi_1 = \{01010101\},\\
\varphi_2 = \{00110011\},\\
\varphi_3 = \{01100110\},\\
\varphi_4 = \{00001111\},\\
\varphi_5 = \{01011010\},\\
\varphi_6 = \{00111100\},\\
\varphi_7 = \{01101001\},
\end{array}\right.
\left\{\begin{array}{l}
\varphi_8 = \{11111111\},\\
\varphi_9 = \{10101010\},\\
\varphi_{10} = \{11001100\},\\
\varphi_{11} = \{10011001\},\\
\varphi_{12} = \{11110000\},\\
\varphi_{13} = \{10100101\},\\
\varphi_{14} = \{11000011\},\\
\varphi_{15} = \{10010110\},
\end{array}\right. \tag{3}$$