ISSN 0735-2727, Radioelectronics and Communications Systems, 2014, Vol. 57, No. 6, pp. 274–281. © 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. 6, pp. 47–55.

Non-Linear S-box of Nyberg Construction with Maximal Avalanche Effect

M. I. Mazurkov and A. V. Sokolov*
Odessa National Polytechnic University, Odessa, Ukraine
**e-mail: radiosquid@gmail.com*
Received in final form February 11, 2014

Abstract—The full class of irreducible polynomials $f(z)$ of eight degree over all isomorphic representations of Galois field $GF(256)$ is constructed. The set of optimal pairs $\{f(z), A\}$, where A is nonsingular affine transformation matrix is founded which allowed to increase significantly amount of Nyberg construction S-boxes, giving maximum avalanche effect.

DOI: 10.3103/S0735272714060053

Key stage of development of arbitrary up-to-date encryption algorithm is development of cryptographically qualitive nonlinear transformation (S-box), whose properties define the cipher reliability to attacks of linear, correlation and differential crypto analysis.

Last time a great attention is paid to questions of synthesis of non-linear S-boxes of construction, proposed by K. Nyberg [1], satisfying the criterion of maximal avalanche effect [2], with regard to Rijndael/AES cipher [3].

Nonlinear S-boxes of Nyberg construction, satisfying maximal avalanche criterion, are synthesized by selection of appropriate pair: a form of irreducible polynomial $f(z)$ of degree $\deg f(z) = 8$ and form of matrix of affine transformation $y = Ax + b$. At that, in [2] they used polynomials of eighth degree, which are irreducible in a field $GF(2^8)$ and amount of them $|f_2^8| = 30$.

The purpose of the paper is construction of nonlinear S-boxes of Nyberg construction, satisfying the criterion of maximal avalanche effect on a basis of full class of irreducible polynomials in whole amount of isomorphic representations of $GF(256)$, applied to Rijndael/AES cipher.

For completeness of paper material description we represent the essence of S-boxes construction, satisfying maximal avalanche effect criterion [2].

Let $X = [x_i]$, $i = \overline{0, 255}$ is a sequence of rising numbers from 0 to 255. Nyberg construction transforms each element x_i into element y_i, which is multiplicatively orthogonal, applying following rule

$$y_i \equiv x_i^{-1} \operatorname{modd}(f(z), 2), \quad i = \overline{0, 255}, \tag{1}$$

where $f(z)$ is irreducible polynomial $f(z) = z^8 + z^6 + z^3 + z^2 + 1$, $\operatorname{modd}(f(z), 2)$ is double modulo.

As a result we obtain the sequence $Y = [y_i]$, $i = \overline{0, 255}$ with another order of numbers y_i, which is different from sequence x_i order, where it is assumed $0^{-1} = 0$.

Then elements y_i of sequence Y are treated with affine transformation

$$q_i = Ay_i + b, \quad i = \overline{0, 255}, \tag{2}$$

where matrix A of affine transformation and shift vector b in Rijndael cipher [1] is following: