e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 4
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 4

UDC 004.056.55

AVALANCHE CHARACTERISTICS OF CRYPTOGRAPHIC FUNCTIONS OF TERNARY LOGIC

Sokolov A. V. – PhD, Senior Lecturer of the Department of Informatics and Control of Information Systems Protection, Odessa National Polytechnic University, Odessa, Ukraine.

Zhdanov O. N. – PhD, Assistant Professor of the IT Security Department, Reshetnev Siberian State University of Science and Technology, Krasnoyarsk, Russia.

ABSTRACT

Context. The development and aplication of cryptographic algorithms based on many-valued logic functions makes it important to research their cryptographic properties and develop effective criteria for the cryptographic quality of their components. The development of efficient methods for the synthesis of high-quality cryptographic primitives based on the functions of many-valued logic is also an important task. The object of this research is the process of improving the efficiency of cryptographic algorithms based on many-valued logic functions.

Objective. The purpose of this paper is to generalize the error propagation criterion and the strict avalanche criterion for the case of functions of three-valued logic.

Method. The emergence of cryptography based on many-valued logic functions led to the understanding that today's dominant cryptographic algorithms based on binary algebraic constructions are only a special case of more general trends. Numerous researches show that the use of cryptographic constructions based on many-valued logic functions leads to the creation of cryptoalgorithms that more fully implement the principles of diffusion and confusion. One of the most important cases of many-valued logic functions are 3-functions, which are also used in quantum cryptography. This article is another step towards developing cryptographic constructions based on many-valued logic functions.

Results. The definition of the propagation criterion was extended to the case of functions of three-valued logic. On the basis of the propagation criterion for the functions of three-valued logic, the definition of a strict avalanche criterion was introduced, which describes the stability of cryptographic constructions against differential cryptanalysis attacks. We experimentally determined the number of 3-functions of length N=9, satisfying the strict avalanche criterion. A method based on three constructive rules is proposed, which allows to synthesize a complete set of 864 S-boxes of length N=9 satisfying strict avalanche criterion. This set of S-boxes is basic for the application of Kim's construction, which allows to recurrently increase the length of the S-box to the required value. The paper shows that using Kim's construction to increase the length preserves the S-box satisfying to a strict avalanche criterion, while allowing to obtain S-boxes with satisfactory non-linearity value as well as small output and input vectors correlation.

Conclusions. The most important criterion of cryptographic quality, which shows the stability of the cryptographic algorithm to attacks of differential cryptanalysis is the propagation criterion that was generalized to the case of 3-functions. The existence of 3-functions of length N=9 satisfying the strict avalanche criterion is shown, and their full set is found. On the basis of the proposed constructive method, a complete set of S-boxes of length N=9 that satisfy the strict avalanche criterion was synthesized. It is shown that the Kim scheme can be applied to recurrently increase the length of S-boxes based on many-valued logic functions. As an actual direction for the continuation of the research, the development of regular and constructive methods for the synthesis of full sets of 3-functions and S-boxes of lengths N=27, 81, 243..., satisfying the strict avalanche criterion can be noted.

KEYWORDS: cryptography, differential properties, ternary logic, Boolean function.

ABBREVIATIONS

SAC is a Strict Avalanche Criterion.

NOMENCLATURE

f, f' are many-valued logic function examples;

x_1, x_2 are arguments of many-valued logic function;

d_1, d_2 are effects on the inputs of many-valued logic function;

N is a length of many-valued logic function or S-box, based on many-valued logic functions;

K^0, K^-, K^+ are numbers of symbols 0, – and + in ternary function;

δ is a transformation of change in ternary function output values;

u is a vector of change in ternary function argument;

$v(u)$ is a number of non-zero values of a vector u;

$D_u f$ is an derivative of ternary logic function;

m is an order of propagation criterion;

X is a vector of ternary function input arguments;

J_1, J_2, J_3 are numbers of S-boxes that can be produced by using Rule 1, Rule 2 and Rule 3 correspondingly;

α is a coding sequence used in Rule 3 to perform sign encodings of ternary functions;

J is a cardinality of the class of S-boxes of length $N = 9$, satisfying strict avalanche criterion;

S, S_{27}, S_{81} are S-box examples;

NL is the nonlinearity distance;

$P = \left\| \rho_{v,\mu} \right\|$ is the matrix of the correlation coefficients between the output y_μ and input x_v vectors of the S-box.

INTRODUCTION

Block symmetric cryptographic algorithms are the very important part of modern information protection systems. A further increase in the computing power of computer systems, as well as the emergence of new methods of cryptanalysis give rise to the need to increase the cryptographic strength of existing and new cryptographic algorithms.

DOI DOI 10.15588/1607-3274-2019-4-17

Further development of existing algorithms and the creation of new ones requires the availability of high-quality cryptographic primitives, in particular, S-boxes.

At the same time, the application of the mathematical apparatus of many-valued logic functions is promising, both from the point of view of quantum cryptography and from the point of view of traditional cryptography.

A special place, especially from the point of view of quantum cryptography, among the functions of many-valued logic is occupied by the functions of three-valued logic.

The creation of new cryptographic primitives based on many-valued logic functions requires the generalization of cryptographic quality criteria, the main of which are: nonlinearity, correlation immunity, propagation criterion and a strict avalanche criterion which is particular case of the propagation criterion.

In this paper, the propagation criterion and strict avalanche criterion are generalized to the case of three-valued logic functions, and effective methods for synthesizing 3-functions and S-blocks of arbitrary length that satisfy the strict avalanche criterion are proposed.

The object of research is the process of improving the efficiency of cryptographic algorithms based on many-valued logic functions.

The subject of research is the synthesis methods of S-boxes based on many-valued logic functions with good avalanche characteristics.

The purpose of the work is to generalize the error propagation criterion and the strict avalanche criterion to the case of functions of three-valued logic that will allow us to develop a recursive method for synthesizing S-boxes satisfying the strict avalanche criterion.

1 PROBLEM STATEMENT

Let the function $f(X)$ of three-valued logic to be given. The scientific problem is to build a method for determining the probability of a change in the output values of a function when its input values change.

Another important task solved in this paper is the development of a method for synthesizing the functions $f(X)$ which the uniform probability of a change in output values when one of the input values is changing (such functions are called as satisfying the strict avalanche criterion).

We also solve the problem of constructing S-boxes on the basis of 3-functions satisfying SAC, that can be used in modern cryptographic algorithms based on the principles of many-valued logic.

2 REVIEW OF THE LITERATURE

The development of methods of many-valued logic, occurring at the present time [1], causes the emergence of new algorithms for the cryptographic data protection [2]. Functions of many-valued logic are the excellent basis for the construction of quantum cryptoalgorithms [3…5].

Although many-valued logic algorithms can have an effective hardware implementation [6], by the reason of better realization of the concepts of diffusion and confusion [7], functions of many-valued logic are of considerable interest from the point of view of implementation on binary computers.

Thus, in [8] a block symmetric cryptoalgorithm based on the methods of ternary logic was synthesized. The researches performed show that the use of these methods of ternary logic for the construction of cryptoalgorithms allows us to obtain a high level of diffusion and confusion even when using the simple block replacement (Electronic Codebook [9]) mode at the cost of a small loss of computational efficiency.

The highly nonlinear many-valued functions, that can be, in particular, used in S-boxes construction schemes like modernized Kim's construction [10] was developed in [11] and [12].

Method for constructing S-boxes of ternary logic satisfying the criterion of zero correlation between the output and input vectors is proposed in [13], and method for constructing highly nonlinear S-boxes based on the Nyberg construction is developed in [14].

A method for estimating the non-linearity distance of many-valued logic functions based on the Vilenkin-Chrestenson transform was proposed in [15].

Nevertheless, such an important criterion of the cryptographic quality of S-boxes, as the propagation criterion and the strict avalanche criterion (SAC) remains outside the framework of modern researches devoted to S-boxes based on functions of many-valued logic.

In the binary case, the strict avalanche criterion as a characteristic of resistance to differential cryptoanalysis is one of the basic in the synthesis of S-boxes [16, 17]. The physical interpretation of the error propagation criterion is to measure the degree of change in the output values of a Boolean function when its input values change [18].

3 MATERIALS AND METHODS

The most important problem is the development of a technique for measuring the differential properties of functions of many-valued logic, in particular, 3-functions.

Let's consider an example. Let the truth table of a 3-function of two variables to be given

$$f = \{012012210\}. \quad (1)$$

In order to research the effect of each of the inputs of the 3-function on its output, we connect the summators (Fig. 1) to the inputs, to which we apply the effects $d_1, d_2 \in \{0,1,2\}$. Obviously, a set of values $d_1, d_2 = 0$, means no effect on the inputs of our 3-function.

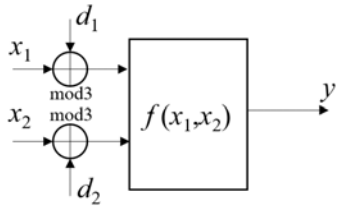

Figure 1 – Example of a scheme for researching the influence of inputs of a 3-function on its output

DOI DOI 10.15588/1607-3274-2019-4-17

Alternately changing the values of the coefficients d_1, d_2, we obtain the rearranged values of the initial 3-function (1), presented in Table 1 (symbol $\oplus$ means addition modulo 3).

Table 1 shows the change in the value of a function when its arguments are changed. Note, that for the binary case this question is trivial, since operating with values from the set $\{0,1\}$ makes it easy to infer the output value: it has changed / has not changed. In the case of ternary logic, obviously, the nature of the change in the output value also plays an important role.

Possible options are:

1. The function value has not changed. Denote this event as 0.

2. The value increased (decreased) by 1 (modulo 3). Denote these events with the symbols "+/–".

We denote this transformation by the symbol δ and introduce the following basic definitions.

Definition 1. Let the $\nu(u)$ to be the number of non-zero values of a vector u. A derivative of a 3-function of k variables in direction of vector u, we call the following 3-function

$$\mathrm{D}_u f = \delta(f(x), f(x+u)). \qquad (2)$$

Definition 2. We say that a 3-function satisfies the propagation criterion in the direction of the vector u if the number of zero values in its derivative $\mathrm{D}_u f$ is equal to the number of positive values and is equal to the number of negative values: $K^0 = K^+ = K^- = N/3$.

In other words, under the influence of the change in input values in direction u the probabilities of events 0, $-$ or $+$ are equal to

$$P_u = \begin{bmatrix} \frac{K^0}{N} & \frac{K^+}{N} & \frac{K^-}{N} \end{bmatrix} = \begin{bmatrix} 0 & + & - \\ 1/3 & 1/3 & 1/3 \end{bmatrix}. \qquad (3)$$

Definition 3. A function is called as satisfying the propagation criterion of order m if it satisfies the propagation criterion in all such directions u that $1 \le \nu(u) \le m$.

Definition 4. A function is said to satisfy a strict avalanche criterion if it satisfies the propagation criterion of order $m = 1$.

Let's continue the example. We find the derivatives of the 3-function (1) and verify its compliance with the strict avalanche criterion (Table 2).

Thus, the researched function does not satisfy the strict avalanche criterion. It is of practical interest to perform the search for 3-functions corresponding to the definition of the strict avalanche criterion that we introduced.

Table 1 – The rearranged values of the initial 3-function (1)

$f(x_1, x_2)$	$f(x_1, x_2 \oplus 1)$	$f(x_1, x_2 \oplus 2)$	$f(x_1 \oplus 1, x_2)$	$f(x_1 \oplus 2, x_2)$
$f(0,0)=0$	$f(0,1)=1$	$f(0,2)=2$	$f(1,0)=0$	$f(2,0)=2$
$f(0,1)=1$	$f(0,2)=2$	$f(0,0)=0$	$f(1,1)=1$	$f(2,1)=1$
$f(0,2)=2$	$f(0,0)=0$	$f(0,1)=1$	$f(1,2)=2$	$f(2,2)=0$
$f(1,0)=0$	$f(1,1)=1$	$f(1,2)=2$	$f(2,0)=2$	$f(0,0)=0$
$f(1,1)=1$	$f(1,2)=2$	$f(1,0)=0$	$f(2,1)=1$	$f(0,1)=1$
$f(1,2)=2$	$f(1,0)=0$	$f(1,1)=1$	$f(2,2)=0$	$f(0,2)=2$
$f(2,0)=2$	$f(2,1)=1$	$f(2,2)=0$	$f(0,0)=0$	$f(1,0)=0$
$f(2,1)=1$	$f(2,2)=0$	$f(2,0)=2$	$f(0,1)=1$	$f(1,1)=1$
$f(2,2)=0$	$f(2,0)=2$	$f(2,1)=1$	$f(0,2)=2$	$f(1,2)=2$

Table 2 – The derivatives of the 3-function (1)

$f(x_1, x_2)$	$f(x_1, x_2 \oplus 1)$	D_{01}	$f(x_1, x_2 \oplus 2)$	D_{02}	$f(x_1 \oplus 1, x_2)$	D_{10}	$f(x_1 \oplus 2, x_2)$	D_{20}
$f(0,0)=0$	$f(0,1)=1$	$-$	$f(0,2)=2$	$+$	$f(1,0)=0$	0	$f(2,0)=2$	$+$
$f(0,1)=1$	$f(0,2)=2$	$-$	$f(0,0)=0$	$+$	$f(1,1)=1$	0	$f(2,1)=1$	0
$f(0,2)=2$	$f(0,0)=0$	$-$	$f(0,1)=1$	$+$	$f(1,2)=2$	0	$f(2,2)=0$	$-$
$f(1,0)=0$	$f(1,1)=1$	$-$	$f(1,2)=2$	$+$	$f(2,0)=2$	$+$	$f(0,0)=0$	0
$f(1,1)=1$	$f(1,2)=2$	$-$	$f(1,0)=0$	$+$	$f(2,1)=1$	0	$f(0,1)=1$	0
$f(1,2)=2$	$f(1,0)=0$	$-$	$f(1,1)=1$	$+$	$f(2,2)=0$	$-$	$f(0,2)=2$	0
$f(2,0)=2$	$f(2,1)=1$	$+$	$f(2,2)=0$	$-$	$f(0,0)=0$	$-$	$f(1,0)=0$	$-$
$f(2,1)=1$	$f(2,2)=0$	$+$	$f(2,0)=2$	$-$	$f(0,1)=1$	0	$f(1,1)=1$	0
$f(2,2)=0$	$f(2,0)=2$	$+$	$f(2,1)=1$	$-$	$f(0,2)=2$	$+$	$f(1,2)=2$	$+$

DOI DOI 10.15588/1607-3274-2019-4-17

4 EXPERIMENTS

It seems to us that for small values of the length it is possible to carry out a exhaustive search for ternary sequences satisfying the strict avalanche criterion. The search of a complete set of ternary sequences of length $N = 9$ allowed us to establish that there are in total 2052 3-functions of the specified length that satisfy the strict avalanche criterion.

For example, we show (Table 3) that the sequence we have found

$$f' = \{001022121\}, \tag{4}$$

satisfies the strict avalanche criterion.

Since all the D_i in Table 3 are balanced, so $K^0 = K^+ = K^-$, the sequence (4) really satisfies the strict avalanche criterion.

We note that such 3-functions possess special practical value, on the basis of which it is possible to construct such important cryptographic primitives as S-boxes. Experimental research carried out with the requirements of the theorem [20] which regulates the conditions of bijectivity of S-boxes, made it possible to discover that from the total set of the 3-functions of length $N = 9$, satisfying the strict avalanche criterion there are only 72 such 3-functions on the basis of which it is possible to construct the S-box. These 3-functions are given in Table 4.

5 RESULTS

Let us determine the possible number of S-boxes of length $N = 9$ satisfying the strict avalanche criterion. A complete set of such S-boxes of length $N = 9$ can be constructed on the basis of a set of generating S-boxes and rules of their reproduction.

We represent the set of generating S-boxes, on the basis of which the full class of S-boxes of length $N = 9$ satisfying the strict avalanche criterion can be obtained

$$\begin{bmatrix} 0\,1\,3\,2\,8\,6\,5\,7\,4 \\ 0\,1\,3\,6\,2\,8\,7\,4\,5 \\ 0\,1\,4\,2\,7\,8\,3\,6\,5 \\ 0\,1\,4\,6\,5\,3\,8\,2\,7 \\ 0\,1\,6\,2\,5\,3\,8\,4\,7 \\ 0\,1\,6\,3\,2\,5\,4\,7\,8 \\ 0\,1\,7\,2\,4\,5\,6\,3\,8 \\ 0\,1\,7\,3\,8\,6\,5\,2\,4 \\ 0\,2\,3\,1\,7\,6\,4\,8\,5 \\ 0\,2\,3\,6\,1\,7\,8\,5\,4 \\ 0\,2\,5\,1\,8\,7\,3\,6\,4 \\ 0\,2\,5\,6\,4\,3\,7\,1\,8 \end{bmatrix} \begin{bmatrix} 0\,2\,6\,1\,4\,3\,7\,5\,8 \\ 0\,2\,6\,3\,1\,4\,5\,8\,7 \\ 0\,2\,8\,1\,5\,4\,6\,3\,7 \\ 0\,2\,8\,3\,7\,6\,4\,1\,5 \\ 0\,4\,1\,2\,8\,7\,3\,5\,6 \\ 0\,4\,1\,6\,3\,5\,8\,7\,2 \\ 0\,5\,2\,1\,7\,8\,3\,4\,6 \\ 0\,5\,2\,6\,3\,4\,7\,8\,1 \\ 0\,5\,3\,1\,2\,8\,7\,4\,6 \\ 0\,5\,3\,2\,8\,1\,6\,7\,4 \\ 0\,8\,2\,1\,4\,5\,6\,7\,3 \\ 0\,8\,2\,3\,6\,7\,4\,5\,1 \end{bmatrix}. \tag{5}$$

Reproduction of S-boxes (5) may be performed by applying the following rules.

Rule 1. Permutation of the second and third triples of elements of the S-box preserves the compliance of S-box with the strict avalanche criterion.

For example, from the first basic S-box obtained by us

$$[0\,1\,3\,2\,8\,6\,5\,7\,4], \tag{6}$$

we can obtain a new S-box by applying the Rule 1

$$[0\,1\,3\,5\,7\,4\,2\,8\,6]. \tag{7}$$

Table 3 – The derivatives of the 3-function (5)

$f'(x_1, x_2)$	$f'(x_1, x_2 \oplus 1)$	D_{01}	$f'(x_1, x_2 \oplus 2)$	D_{02}	$f'(x_1 \oplus 1, x_2)$	D_{10}	$f'(x_1 \oplus 2, x_2)$	D_{20}
$f'(0,0)=0$	$f'(0,1)=0$	0	$f'(0,2)=1$	−	$f'(1,0)=0$	0	$f'(2,0)=1$	−
$f'(0,1)=0$	$f'(0,2)=1$	−	$f'(0,0)=0$	0	$f'(1,1)=2$	+	$f'(2,1)=2$	+
$f'(0,2)=1$	$f'(0,0)=0$	+	$f'(0,1)=0$	+	$f'(1,2)=2$	−	$f'(2,2)=1$	0
$f'(1,0)=0$	$f'(1,1)=2$	+	$f'(1,2)=2$	+	$f'(2,0)=1$	−	$f'(0,0)=0$	0
$f'(1,1)=2$	$f'(1,2)=2$	0	$f'(1,0)=0$	−	$f'(2,1)=2$	0	$f'(0,1)=0$	−
$f'(1,2)=2$	$f'(1,0)=0$	−	$f'(1,1)=2$	0	$f'(2,2)=1$	+	$f'(0,2)=1$	+
$f'(2,0)=1$	$f'(2,1)=2$	−	$f'(2,2)=1$	0	$f'(0,0)=0$	+	$f'(1,0)=0$	+
$f'(2,1)=2$	$f'(2,2)=1$	+	$f'(2,0)=1$	+	$f'(0,1)=0$	−	$f'(1,1)=2$	0
$f'(2,2)=1$	$f'(2,0)=1$	0	$f'(2,1)=2$	−	$f'(0,2)=1$	0	$f'(1,2)=2$	−

Table 4 – The 3-functions suitable for S-boxes constructing

001022121	010112022	020122110	100220121	112010022	122020110	202112100	212200110
001121022	010211220	020221011	101002122	112022010	122101002	202211001	220010211
001202211	010220211	022001121	101122002	112100202	122110020	211001202	220100121
001211202	011002212	022010112	101200221	112202100	200101221	211010220	220121100
002011212	011020221	022112010	101221200	121001022	200110212	211202001	220211010
002101122	011212002	022121001	110020122	121022001	200212110	211220010	221011020
002122101	011221020	100112202	110122020	121100220	200221101	212002011	221020011
002212011	020011221	100121220	110200212	121220100	202001211	212011002	221101200
010022112	020110122	100202112	110212200	122002101	202100112	212110200	221200101

DOI DOI 10.15588/1607-3274-2019-4-17

So, the application of Rule 1 allows to obtaining $J_1 = 2$ new S-boxes based on one.

Rule 2. The permutation of the component 3-functions of the S-box preserves the compliance of S-box with the strict avalanche criterion.

As an example, we again consider the first basic S-box, which can be represented as two component 3-functions

$$\begin{bmatrix} 0\ 1\ 3\ 2\ 8\ 6\ 5\ 7\ 4 \\ 0\ 1\ 0\ 2\ 2\ 0\ 2\ 1\ 1 \\ 0\ 0\ 1\ 0\ 2\ 2\ 1\ 2\ 1 \end{bmatrix}. \quad (8)$$

By permuting the component 3-functions, we obtain a new S-box, which also satisfies the strict avalanche criterion

$$\begin{bmatrix} 0\ 3\ 1\ 6\ 8\ 2\ 7\ 5\ 4 \\ 0\ 0\ 1\ 0\ 2\ 2\ 1\ 2\ 1 \\ 0\ 1\ 0\ 2\ 2\ 0\ 2\ 1\ 1 \end{bmatrix}. \quad (9)$$

The application of Rule 2 allows us to obtain on the basis of one S-box $J_2 = k! = (\log_3 N)!$ new S-boxes satisfying the strict avalanche criterion. In the case of length $N = 9$ from one S-box, we obtain two.

Rule 3. All possible $3^k = 3^{\log_3 N} = N$ sign encodings of the component 3-functions of the S-box preserves the compliance of S-box with the strict avalanche criterion.

Let's demonstrate the operation of Rule 3 using as example the first basic S-box and the coding sequence $\alpha = \{\alpha_1 \quad \alpha_2\} = \{12\}$

$$\begin{bmatrix} 0\ 1\ 3\ 2\ 8\ 6\ 5\ 7\ 4 \\ \{0\ 1\ 0\ 2\ 2\ 0\ 2\ 1\ 1\} + \alpha_1 \bmod 3 \\ \{0\ 0\ 1\ 0\ 2\ 2\ 1\ 2\ 1\} + \alpha_2 \bmod 3 \end{bmatrix} \rightarrow \rightarrow \begin{bmatrix} 7\ 8\ 1\ 6\ 3\ 4\ 0\ 5\ 2 \\ 1\ 2\ 1\ 0\ 0\ 1\ 0\ 2\ 2 \\ 2\ 2\ 0\ 2\ 1\ 1\ 0\ 1\ 0 \end{bmatrix}. \quad (10)$$

The application of Rule 3 allows us to obtain on the basis of one S-box $J_3 = 3^k = 3^{\log_3 N} = N$ new S-boxes satisfying the strict avalanche criterion. In the case of length $N = 9$, we obtain 9 new S-boxes.

Thus, using the basic 24 S-boxes of length $N = 9$ (5), as well as Rule 1, Rule 2 and Rule 3, we can synthesize a class of S-boxes of cardinality $J = 24 \cdot 2 \cdot 2 \cdot 9 = 864$, each of which is satisfying the strict avalanche criterion. This cardinality of class of S-boxes satisfying the strict avalanche criterion is equal to the cardinality of their complete set estimated by the exhaustive search.

6 DISCUSSION

The obtained 3-functions of length $N = 9$ (Table 4), satisfying SAC, as well as S-boxes which are built on their basis are important cryptographic constructions from a theoretical point of view.

We note that, for practical use S-boxes of long length N are necessary. Earlier, to increase the length of the S-boxes, both in the binary case [21] and in the ternary case [13], Kim's scheme was successfully used.

Kim's scheme is presented in general form for ternary case on Fig. 2

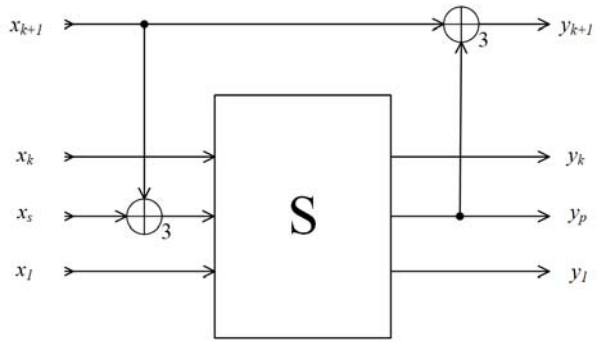

Figure 2 – Kim's scheme for ternary case

Let's consider an example. Suppose the S-box of length $N = 9$ satisfying the strict avalanche criterion is given

$$S = [0 \quad 1 \quad 6 \quad 3 \quad 2 \quad 5 \quad 4 \quad 7 \quad 8], \quad (11)$$

on the basis of which it is necessary to obtain an S-box of length $N = 27$.

We apply to the S-box (11) a Kim's scheme of recurrent increase of length (Fig. 1), which taking into account the length $N = 9$ of the initial S-box and the length $N = 27$ of the required S-box takes the form showed on Fig. 3.

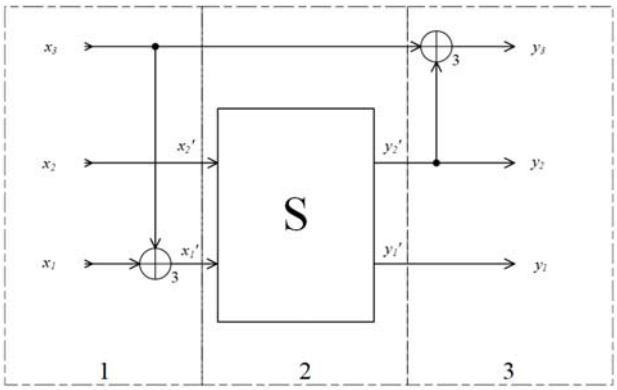

Figure 3 – Kim's scheme for a S-box with two inputs

Suppose, for example, that the vector of the input value of a new S-box of length $N = 27$ has the form

$$X = [x_1 \quad x_2 \quad x_3] = [001]_3. \quad (12)$$

Then, calculating the sum in the first sub-block (Fig. 3), we get the value

$$x_1' = (x_1 + x_3) \bmod 3 = (0+1) \bmod 3 = 1; \quad x_2' = x_2 = 0. \quad (13)$$

In the second sub-block of calculations, in accordance with the small S-box (11) chosen by us, we obtain

$$S(10) = S(1) = 1, \quad y_1' = 1; \quad y_2' = 0. \quad (14)$$

DOI DOI 10.15588/1607-3274-2019-4-17

And, finally, the calculations in the third sub-block

$$\begin{gathered} y_1 = y_1^{'} = 1; \quad y_2 = y_2^{'} = 0; \\ y_3 = (y_2^{'} + x_3) \bmod 3 = (1+0) \bmod 3 = 1 \Rightarrow \\ \Rightarrow Y = [y_1 \quad y_2 \quad y_3] = [101]_3 = 10. \end{gathered} \tag{15}$$

Calculating all the 27 different input values, we get the entire S-box of length $N = 27$

$$\begin{gathered} S_{27} = \big[0\ 1\ 24\ 12\ 2\ 14\ 13\ 25\ 26\ 10\ 6\ 9\ 11 \\ 23\ 21\ 7\ 8\ 22\ 15\ 18\ 19\ 5\ 3\ 20\ 17\ 4\ 16\big]. \end{gathered} \tag{16}$$

In [15] the interconnection between the nonlinearity distance of the S-box component functions and their Vilenkin-Chrestenson transformants was discovered. This interconnection may be described by the formula

$$\mathrm{NL} = \begin{cases} q^k - \max\left\{\left|W_i\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W_i\right|\right\}, & q = 2, \end{cases} \tag{17}$$

where W_i is the vector of S-box i-th component function Vilenkin-Chrestenson (Walsh-Hadamard for the binary case) transformants and $i = 0,1,...,\log_q N - 1$.

From other side, a formula for calculating the matrix $P = \left\|\rho_{\nu,\mu}\right\|$ of the correlation coefficients between the output y_μ and input x_ν vectors of the S-box was introduced in [13]

$$\rho_{\nu,\mu} = \frac{\sum\limits_{t=1}^{N} x_\nu y_\mu - \dfrac{\sum\limits_{t=1}^{N} x_\nu \sum\limits_{t=1}^{N} y_\mu}{N}}{\sqrt{\left[\sum\limits_{t=1}^{N} x_\nu^{\,2} - \dfrac{\left(\sum\limits_{t=1}^{N} x_\nu\right)^2}{N}\right] \cdot \left[\sum\limits_{t=1}^{N} y_\mu^{\,2} - \dfrac{\left(\sum\limits_{t=1}^{N} y_\mu\right)^2}{N}\right]}}, \tag{18}$$

where $\nu,\mu = 0,1,...,\log_q N - 1$.

Using formula (17) we can determine that the distance of nonlinearity of constructed S-box (16)

$$\mathrm{NL} = 11.412, \tag{19}$$

as well as we can calculate its matrix of correlation coefficients according to formula (18)

$$P = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0.5 & 0.5 \\ 0.5 & 0 & 0 \end{bmatrix}. \tag{20}$$

Continuing usage of the Kim's recurrent construction shown in Fig. 2 on the basis of S-box (16) we can get the S-box of length $N = 81$ that also satisfies the strict avalanche criterion

$$\begin{gathered} S_{81} = [0\ 1\ 78\ 39\ 2\ 41\ 40\ 79\ 80 \\ 10\ 60\ 9\ 11\ 50\ 48\ 61\ 62\ 49 \\ 69\ 18\ 19\ 32\ 30\ 20\ 71\ 31\ 70 \\ 28\ 24\ 27\ 29\ 68\ 66\ 25\ 26\ 67 \\ 6\ 36\ 37\ 77\ 75\ 38\ 8\ 76\ 7 \\ 45\ 46\ 15\ 57\ 47\ 59\ 58\ 16\ 17 \\ 51\ 54\ 55\ 14\ 12\ 56\ 53\ 13\ 52 \\ 63\ 64\ 33\ 21\ 65\ 23\ 22\ 34\ 35 \\ 73\ 42\ 72\ 74\ 5\ 3\ 43\ 44\ 4]. \end{gathered} \tag{21}$$

The calculated S-box S_{81} (21) have the nonlinearity distance

$$\mathrm{NL} = 34.235, \tag{22}$$

and the matrix of correlation coefficients

$$P = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{23}$$

CONCLUSIONS

The scientific novelty of obtained results is that we generalized such important criteria of cryptographic quality as the propagation criterion and the strict avalanche criterion to the case of functions of three-valued logic. The compliance of the 3-function with the strict avalanche criterion makes it possible to ascertain its resistance to attacks of differential cryptanalysis, which is important for practical cryptoalgorithms.

On the basis of the introduced definition of the strict avalanche criterion for 3-functions, in this paper we found a complete set of cardinality $J = 2052$ of 3-functions satisfying the strict avalanche criterion.

It is established that 72 of these functions can be the basis for constructing bijective S-boxes of length $N = 9$ satisfying the strict avalanche criterion. The cardinality of such S-boxes class is equal to 864.

It is proposed to use the ternary analogue of the Kim's scheme for recurrently increasing the length of the constructed S-boxes. It is shown that in the case of using the Kim's scheme, the resulting S-boxes also satisfies the strict avalanche criterion.

The practical significance of the paper is that the obtained class of 864 S-boxes satisfying the strict avalanche criterion can be used in practical cryptographic algorithm, which are based on the many-valued logic functions. At the same time, using Kim's scheme, S-boxes of any required length can be obtained.

DOI DOI 10.15588/1607-3274-2019-4-17

Prospects for further research are the development of regular and constructive methods for the synthesis of full sets of 3-functions and S-boxes of lengths N=27, 81, 243..., satisfying the strict avalanche criterion as well as consideration of another bases q of many-valued logic functions.

REFERENCES

1. Stankovic R. S., Astola J. T., Moraga C. Representation of Multiple-Valued Logic Functions, *Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems*, 2012, 153 p.
2. Sokolov A. V., Zhdanov O. N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. Springer, Cham, International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018, pp. 331–339.
3. Korchenko O., Vasiliu E., Gnatyuk S. Modern quantum technologies of information security, Aviation. Vilnius, Technika, 2010, No. 14 (2), pp. 58–69.
4. Hnatiuk S., Zhmurko T., Kinzeriavyi V., Seilova N. Method for quality evaluation of trit pseudorandom sequence to cryptographic applications, *Information technology and security,* 2015, Vol. 3, No. 2, pp. 108–116.
5. Vol E. D. Quantum theory as a relevant framework for the statement of probabilistic and many-valued logic, *International Journal of Theoretical Physics*, 2013, 52(2), pp. 514–523.
6. Stakhov A. Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic, *The Computer Journal,* 2002, 45(2), pp. 221–236.
7. Shannon, C.E. A Mathematical Theory of Cryptography, *Bell system technical journal,* 1948, Vol. 27, No. 3, pp. 379–423
8. Zhdanov O.N. Sokolov A.V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic, *Far East Journal of Electronics and Communications*, 2015, Vol. 16, No. 3, pp. 573–589.
9. El Fishawy N. F., Zaid O. M. A. Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms, *IJ Network Security*, 2007, 5(3), pp. 241–251.
10. Sokolov, A.V., Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion / A.V. Sokolov. – Radioelectronics and Communications Systems, 2013. – Vol. 56. – No.8. – P. 415–423.
11. Sokolov A. V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties, *Journal of Telecommunication, Electronic and Computer Engineering,* 2016, Vol. 8, No. 9, pp. 39–43.
12. Mazurkov M. I., Sokolov A. V., Barabanov N. A. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis, *Radioelectronics and Communications Systems,* 2016, Vol. 59, No. 11, pp. 510–517.
13. Zhdanov O. N., Sokolov A. V. Algorithm of construction of optimal according to criterion of zero correlation nonbinary S-boxes, *Problems of physics, mathematics and technics*, 2015, No. 3(24), pp. 94–97.
14. Zhdanov O. N., Sokolov A. V. Extending Nyberg construction on Galois fields of odd characteristic / O.N. Zhdanov, // *Radioelectronics and Communications Systems*, 2017, Vol. 60, No. 12, pp. 538–544.
15. Sokolov A. V., Krasota N. I. Very nonlinear permutations: synthesis method for S-boxes with maximal 4-nonlinearity, *Proceeding of ONAT named after A. S. Popov*, 2017, No.1, pp. 145–154.
16. Webster A. F., Tavares S. E. On the design of S-boxes, *Proc. of CRYPTO'85*. Springer-Verlag, 1985, pp. 523–534.
17. Chandrasekharappa T.G.S., Prema K. V., Kumara Shama S - boxes generated using Affine transformation giving maximum avalanche effect, *Int. J. Comput. Sci. Eng.,* 2011, Vol. 3, No. 9, pp. 3185–3193.
18. Chandrasekharappa T. G. S., Prema K. V., Shama Kumara Possible S-boxes generated from Affine transformation those satisfy Maximum Strict Avalanche Criteria, *Proceedings of World Academy of Science, Engineering and Technology*, 2009, Vol. 60, pp. 880–883.
19. Trakhtman A. M., Trakhtman V. A. Fundamentals of the theory of discrete signals on finite intervals. Moscow, Soviet Radio, 1975, 208 p.
20. Kim K. Construction of DES-like S-boxes based on Boolean functions satisfying the SAC, Lect. Notes Comput. Sci., 1993, pp. 59–72.
21. Kim K., Matsumoto T., Imai H. A recursive construction method of S-boxes satisfying the strict avalanche criterion, *Proc. of CRYPTO90*. Springer-Verlag, 1990, pp. 565–574.

Received 26.06.2019.
Accepted 03.09.2019.

УДК 004.056.55

ЛАВИННІ ХАРАКТЕРИСТИКИ КРИПТОГРАФІЧНИХ ФУНКЦІЙ ТРИЗНАЧНОЇ ЛОГІКИ

Соколов А. В. – канд. техн. наук, старший викладач кафедри інформатики та управління захистом інформаційних систем, Одеський національний політехнічний університет, м. Одеса, Україна.

Жданов О. Н. – канд. физ.-мат. наук, доцент кафедри безпеки інформаційних технологій, Сибірський державний університет науки і технологій імені академіка М. Ф. Решетнева, Красноярськ, Росія.

АНОТАЦІЯ

Актуальність. Розробка і впровадження криптоалгоритмів на основі функцій багатозначної логіки робить актуальною задачу поглибленого вивчення їх криптографічних властивостей, розробки ефективних критеріїв криптографічної якості компонентів, з яких вони складаються. Важливим завданням є також розробка ефективних методів синтезу високоякісних криптографічних примітивів, заснованих на функціях багатозначної логіки. Об'єктом даного дослідження є процеси підвищення ефективності криптоалгоритмів на основі функцій багатозначної логіки.

Мета. Метою статті є узагальнення критерію поширення помилки і суворого лавинного критерію на випадок функцій тризначної логіки.

Метод. Поява криптографії на основі функцій багатозначної логіки привела до розуміння, що домінуючі сьогодні криптографічні алгоритми, засновані на двійкових алгебраїчних конструкціях, є лише окремим випадком більш загальних тенденцій. Численні дослідження показують, що використання криптографічних конструкцій на основі функцій багатозначної

DOI DOI 10.15588/1607-3274-2019-4-17

логіки веде до створення криптоалгоритмів, що більш повно реалізують принципи дифузії і конфузії. При цьому, найважливішим випадком функцій багатозначної логіки є 3-функції, які застосовуються також у квантовій криптографії. Ця стаття є ще одним кроком на шляху освоєння криптографічних конструкцій на основі функцій багатозначної логіки.

Результати. Визначення критерія поширення було узагальнене на випадок функцій тризначної логіки. На основі критерію поширення для функцій тризначної логіки було введено визначення суворого лавинного критерію, який описує стійкість криптографічних конструкцій до атак диференціального криптоаналізу. У статті експериментально визначено кількість 3-функцій довжини N=9, що задовольняють суворому лавинному критерію. Запропоновано метод, заснований на трьох конструктивних правилах, що дозволяє синтезувати повну множину з 864 S-блоків довжини N=9, які задовольняють суворому лавинному критерію. Дана множина S-блоків є базовою для застосування конструкції Кіма, що дозволяє рекурентно збільшити довжину S-блоку до необхідного значення. У статті показано, що використання конструкції Кіма для збільшення довжини зберігає відповідність S-блоку суворому лавинному критерію, при цьому дозволяє отримати S-блоки з задовільними показниками нелінійності та кореляційного зв'язку векторів виходу і входу.

Висновки. Найважливіший критерій криптографічної якості, який показує стійкість криптоалгоритму до атак диференціального криптоаналізу – критерій поширення помилки узагальнено на випадок 3-функцій. Показано існування 3-функцій довжини N=9, що задовольняють суворому лавинному критерію, а також знайдено їх повну множину. На основі запропонованого конструктивного методу синтезовано повну множину S-блоків довжини N=9, які задовольняють суворому лавинному критерію. Показано, що для рекурентного збільшення довжини S-блоків на основі функцій багатозначної логіки може бути застосована схема Кіма. В якості актуального напрямку продовження проведених досліджень можна зазначити побудову регулярних і конструктивних методів синтезу повних множин 3-функцій та S-блоків довжин N=27, 81, 243..., які відповідають суворому лавинному критерію.

КЛЮЧОВІ СЛОВА: криптографія, диференціальні властивості, тризначна логіка, булева функція.

УДК 004.056.55

ЛАВИННЫЕ ХАРАКТЕРИСТИКИ КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ ТРОИЧНОЙ ЛОГИКИ

Соколов А. В. – канд. техн. наук, старший преподаватель кафедры информатики и управления защитой информационных систем, Одесский национальный политехнический университет, г. Одесса, Украина.

Жданов О. Н. – канд. физ.-мат. наук, доцент кафедры безопасности информационных технологий, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева, Красноярск, Россия.

АННОТАЦИЯ

Актуальность. Разработка и внедрение криптоалгоритмов на основе функций многозначной логики делает актуальной задачу углублённого изучения их криптографических свойств, разработки эффективных критериев криптографического качества составляющих их компонентов. Важнейшей задачей является также разработка эффективных методов синтеза высококачественных криптографических примитивов, основанных на функциях многозначной логики. Объектом данного исследования являются процессы повышения эффективности криптоалгоритмов на основе функций многозначной логики.

Цель. Целью статьи является обобщение критерия распространения ошибки и строгого лавинного критерия на случай функций трехзначной логики.

Метод. Появление криптографии на основе функций многозначной логики, привело к пониманию, что доминирующие сегодня криптографические алгоритмы, основанные на двоичных алгебраических конструкциях, является лишь частным случаем более общих тенденций. Многочисленные исследования показывают, что использование криптографических конструкций на основе функций многозначной логики ведет к созданию криптоалгоритмов, более полно реализующих принципы диффузии и конфузии. При этом, важнейшим случаем функций многозначной логики являются 3-функции, которые применяются также в квантовой криптографии. Настоящая статья является еще одним шагом на пути освоения криптографических конструкций на основе функций многозначной логики.

Результаты. Определение критерия распространения было обобщено на случай функций трехзначной логики. На основе критерия распространения для функций трехзначной логики было введено определение строгого лавинного критерия, который описывает устойчивость криптографических конструкций к атакам дифференциального криптоанализа. В статье экспериментально определено количество 3-функций длины N=9, соответствующих строгому лавинному критерию. Предложен метод, основанный на трех конструктивных правилах, позволяющий синтезировать полное множество из 864 S-блоков длины N=9, удовлетворяющих строгому лавинному критерию. Данное множество S-блоков является базовым для применения конструкции Кима, позволяющей рекуррентно увеличить длину S-блока до необходимого значения. В статье показано, что использование конструкции Кима для увеличения длины сохраняет соответствие S-блока строгому лавинному критерию, при этом позволяет получить S-блоки с удовлетворительными показателями нелинейности и корреляционной связи векторов выхода и входа.

Выводы. Важнейший критерий криптографического качества, показывающий устойчивость криптоалгоритма к атакам дифференциального криптоанализа – критерий распространения ошибки обобщен на случай 3-функций. Показано существование 3-функций длины N=9, соответствующих строгому лавинному критерию, а также найдено их полное множество. На основе предложенного конструктивного метода синтезировано полное множество S-блоков длины N=9, удовлетворяющих строгому лавинному критерию. Показано, что для рекуррентного увеличения длины S-блоков на основе функций многозначной логики может быть применена схема Кима. В качестве актуального направления продолжения проведенных исследований может быть отмечено построение регулярных и конструктивных методов синтеза полных множеств 3-функций и S-блоков длин N=27, 81, 243…, удовлетворяющих строгому лавинному критерию.

КЛЮЧЕВЫЕ СЛОВА: криптография, дифференциальные свойства, троичная логика, булева функция.

DOI DOI 10.15588/1607-3274-2019-4-17

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Stankovic R. S. Representation of Multiple-Valued Logic Functions / R. S. Stankovic, J. T. Astola, C. Moraga. – Morgan & Claypool Publishers, Synthesis lectures on digital circuits and systems, 2012. – 153 p.
2. Sokolov A. V. Prospects for the Application of Many-Valued Logic Functions in Cryptography / A. V. Sokolov, O. N. Zhdanov. – Springer, Cham, International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018. – P. 331–339.
3. Korchenko, O. Modern quantum technologies of information security / O. Korchenko, E. Vasiliu, S. Gnatyuk. – Aviation. Vilnius : Technika, 2010. –No. 14 (2). – P. 58–69.
4. Метод оцінювання якості тритових псевдовипадкових послідовностей для криптографічних застосувань / [С. Гнатюк, Т. Жмурко, В. Кінзерявий, Н. Сейлова]. – Інформаційні технології та безпека. – 2015. – Т. 3, № 2. – С. 108–116.
5. Vol E. D. Quantum theory as a relevant framework for the statement of probabilistic and many-valued logic / E. D. Vol. – International Journal of Theoretical Physics, 2013. – 52(2). – P. 514–523.
6. Stakhov A. Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic / A. Stakhov // The Computer Journal. – 2002. – 45(2). – P. 221–236.
7. Shannon C. E. A Mathematical Theory of Cryptography / C. E. Shannon // Bell system technical journal. – 1948. – Vol. 27, No. 3. – P. 379–423
8. Zhdanov O. N. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic / O. N. Zhdanov, A. V. Sokolov // Far East Journal of Electronics and Communications. – 2015. – Vol. 16, No. 3. – P. 573–589.
9. El Fishawy N. F. Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms / N. F. El Fishawy, O. M. A. Zaid. – IJ Network Security, 2007. – 5(3). – P. 241–251.
10. Sokolov A. V. Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion / A. V. Sokolov // Radioelectronics and Communications Systems. – 2013. – Vol. 56, No. 8. – P. 415–423.
11. Sokolov A. V. Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties / A. V. Sokolov // Journal of Telecommunication, Electronic and Computer Engineering. – 2016. – Vol. 8, No. 9. – P. 39–43.
12. Mazurkov M. I. Synthesis method for bent sequences in the Vilenkin-Chrestenson basis / M. I. Mazurkov, A. V. Sokolov, N. A. Barabanov // Radioelectronics and Communications Systems. – 2016. – Vol. 59, No. 11. – P. 510–517.
13. Жданов О. Н. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен / О. Н. Жданов, А. В. Соколов // Проблемы физики, математики и техники. – 2015. – № 3 (24). – С. 94–97.
14. Zhdanov O. N. Extending Nyberg construction on Galois fields of odd characteristic / O. N. Zhdanov, A. V. Sokolov // Radioelectronics and Communications Systems. – 2017. – Vol. 60, No. 12. – P. 538–544.
15. Соколов А. В. Сильно нелинейные подстановки: метод синтеза S-блоков, обладающих максимальной 4-нелинейностью / А. В. Соколов, Н. И. Красота. – Наукові праці ОНАЗ ім. О.С. Попова. – 2017. – № 1. – С. 145–154.
16. Webster A. F. On the design of S-boxes / A. F. Webster, S. E. Tavares // Proc. of CRYPTO'85. – Springer-Verlag, 1985. – P. 523–534.
17. Chandrasekharappa T. G. S. S-boxes generated using Affine transformation giving maximum avalanche effect / T. G. S. Chandrasekharappa, K. V. Prema, Shama Kumara. // Int. J. Comput. Sci. Eng. – 2011. – Vol. 3, No. 9. – P. 3185–3193.
18. Chandrasekharappa T. G. S. Possible S-boxes generated from Affine transformation those satisfy Maximum Strict Avalanche Criteria / T. G. S. Chandrasekharappa, K. V. Prema, Kumara Shama. – Proceedings of World Academy of Science, Engineering and Technology, 2009. – Vol. 60. – P. 880–883.
19. Трахтман А. М. Основы теории дискретных сигналов на конечных интервалах / А. М. Трахтман, В. А. Трахтман. – М. : Советское радио, 1975. – 208 с.
20. Kim, K. Construction of DES-like S-boxes based on Boolean functions satisfying the SAC / K. Kim. – Lect. Notes Comput. Sci., 1993. – P. 59–72.
21. Kim K. A recursive construction method of S-boxes satisfying the strict avalanche criterion / K. Kim, T. Matsumoto, H. Imai // Proc. of CRYPTO90. – Springer-Verlag, 1990. – P. 565–574.

DOI DOI 10.15588/1607-3274-2019-4-17