Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 2, pp. 561–572
DOI : 10.1080/09720529.2021.1964727

A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions

A. V. Sokolov *
V. V. Radush
Odessa National Polytechnic University
Odessa
Ukraine

Abstract

The widespread use of block symmetric ciphers in modern information security systems makes the task of increasing their efficiency urgent, as well as the task of synthesizing high-quality cryptographic primitives used in modern block symmetric ciphers, primarily S-boxes. In particular, the S-boxes must have good avalanche characteristics not only of their component Boolean functions, but also of the component functions of many-valued logic. In this paper, we propose a recursive method for the synthesis of large lengths S-boxes that satisfy the strict avalanche criterion of component 4-functions. As a raw material for the construction of such an S-boxes, small-length S-boxes are used that satisfy the strict avalanche criterion of component 4-functions. In the constructed set of S-boxes that satisfy the strict avalanche criterion of component 4-functions, we found those that simultaneously satisfy the criterion of the maximum avalanche effect of component Boolean functions. The avalanche characteristics of these S-boxes are of high quality both from the point of view of their representation with help of Boolean functions, and from the point of view of their representation using 4-functions. These S-boxes can be recommended for practical use to modernize existing symmetric cryptographic algorithms, as well as to build new perspective ciphers.

Subject Classification: *(2010) 94A60.*

Keywords: *Block symmetric cipher, S-box, Many-valued logic, Strict avalanche criterion, Criterion of maximum avalanche effect.*

* *E-mail:* **radiosquid@gmail.com**

© Taru Publications

Introduction

One of the most important components of modern information security systems are the block symmetric ciphers, the task of which is to ensure reliable cryptographic transformation of large amounts of information in the fastest possible time [1]. Today there are many block symmetric ciphers with a high level of cryptographic quality and, at the same time, a high level of performance. Among these cryptographic algorithms we can mention, for example, the Advanced Encryption Standard (AES) cipher [2] or cellular automata based block cipher using key-dependent S-boxes proposed in [3].

The basic approach by which the primitives of modern cryptographic algorithms, primarily S-boxes, are constructed, assumes their representation using component Boolean functions, to which a set of cryptographic quality criteria is subsequently applied, implying the following requirements: high algebraic degree of nonlinearity, high nonlinearity distance, compliance with the strict avalanche criterion (SAC), and uniform minimization of the elements of the correlation coefficient matrix [4…6].

In accordance with the basic approach, today quite a lot of methods for the synthesis of S-boxes that satisfies the criteria of cryptographic quality have been created, while methods for the synthesis of S-boxes with good avalanche characteristics are of particular interest. In particular, there is method for the synthesis of S-boxes satisfying the strict avalanche criterion according to Kim's construction [7], which was modernized in [8], as well as the method for the synthesis of S-boxes satisfying the criterion of the maximum avalanche effect, which was proposed in [9], while the concept of criterion of maximum avalanche effect was proposed in [10].

Nevertheless, the rapid development of cryptanalysis methods using the mathematical apparatus of many-valued logic functions [11], as well as promising methods of quantum cryptanalysis [12], considering the peculiarities of the structure of the cryptographic algorithm with all its possible representations, determines the need for further improvement of cryptographic algorithms, as well as their components. In order to ensure greater stability of cipher components when they are represented by functions of many-valued logic, a number of criteria for the cryptographic quality of functions of many-valued logic were introduced, in particular, the error propagation criterion for functions of many-valued logic [13].

Thus, when designing modern S-boxes to create new ciphers or improve existing ones, it is important to consider all possible representations

of them by functions of many-valued logic. In the literature, a method is known today [13] that allow synthesis of S-boxes of length $N = 16$ satisfying both the SAC of component Boolean functions and the SAC of component 4-functions. Nevertheless, modern ciphers use S-boxes of large lengths in their composition, in particular length $N = 256$. Due to the fact that today in the literature there are no methods for synthesizing S-boxes of length $N > 16$ that would have good avalanche characteristics both in the sense of component Boolean functions and in the sense of component functions of many-valued logic.

The *purpose* of this paper is to develop a recursive method for the synthesis of S-boxes satisfying the strict avalanche criterion for component 4-functions, as well as the criterion of the maximum avalanche effect of component Boolean functions.

Basic definitions

Consider some given S-box of length $N = 16$, which for the research of avalanche properties can be represented in the form of its component Boolean functions

$$S = \left[\begin{array}{c|cccccccccccccccc} Q & 0 & 1 & 3 & 7 & 14 & 2 & 10 & 9 & 6 & 12 & 11 & 4 & 13 & 8 & 15 & 5 \\ \hline f_{20} & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ f_{21} & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ f_{22} & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ f_{23} & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \end{array}\right]. \quad (1)$$

Let us introduce the basic definitions we need. The research of a Boolean function for compliance with a strict avalanche criterion is based on the following definitions.

Definition 1 : [4]. The directional derivative of a Boolean function f along a vector $u \in V_k$ is a Boolean function

$$D_u f(x) = f(x) \oplus f(x \oplus u), \quad (2)$$

where V_k is the linear vector space of binary vectors of length k, $\oplus$ is the summation modulo 2.

Definition 2 : [4]. A Boolean function f satisfies the error propagation criterion along a vector $u \in V_k$ if its directional derivative along a vector u is a balanced function, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0.5. \quad (3)$$

Definition 3 : [4]. A Boolean function f satisfies the error propagation criterion of the degree k if it satisfies the error propagation criterion along all vectors u of weight $1 \le wt(u) \le k$, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0.5, \ \forall u \in V_k, \quad 1 \le wt(u) \le k. \quad (4)$$

Definition 4 : [4]. A Boolean function f satisfies the strict avalanche criterion if it satisfies the error propagation criterion of degree 1, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0.5, \ \forall u \in V_k, \quad wt(u) = 1. \quad (5)$$

The definition of a strict avalanche criterion is a fairly strict requirement for Boolean functions used for cryptographic purposes. Therefore, instead of defining a strict avalanche criterion, the definition of the criterion of the maximum avalanche effect is often used.

Definition 5 : [9]. A Boolean function satisfies the criterion of the maximum avalanche effect if its derivatives in all directions of weight $u \in V_k \mid wt(u) = 1$ have a weight equal to at least half of its length $wt(D_u f(x)) \ge N/2$, i.e.

$$p\{f(x) = f(x \oplus u)\} \ge 0.5, \ \forall u \in V_k, \quad wt(u) = 1. \quad (6)$$

Using the above definitions, it is not difficult to establish that all component Boolean functions of the S-box (1) satisfy the SAC, thus the entire S-box (1) also satisfies the SAC in the sense of component Boolean functions.

Nevertheless, as it is shown in [14, 15], S-box (1) can also be represented in the form of its component 4-functions

$$S = \left[\begin{array}{c|cccccccccccccccc} Q & 0 & 1 & 3 & 7 & 14 & 2 & 10 & 9 & 6 & 12 & 11 & 4 & 13 & 8 & 15 & 5 \\ \hline f_{40} & 0 & 1 & 3 & 3 & 2 & 2 & 2 & 1 & 2 & 0 & 3 & 0 & 1 & 0 & 3 & 1 \\ f_{41} & 0 & 0 & 0 & 1 & 3 & 0 & 2 & 2 & 1 & 3 & 2 & 1 & 3 & 2 & 3 & 1 \end{array}\right]. \quad (7)$$

The definitions obtained in [12] are used to calculate the avalanche characteristics of the component 4-functions of the S-box (7). Here are the main ones.

Definition 6 : [15]. The weight $\varpi(u)$ of a q-valued vector is the number of its nonzero components.

Definition 7 : [15]. The derivative of a function f along a q-valued vector u is the function

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x) (\mathrm{mod}\, q), \tag{8}$$

where $\underset{q}{\oplus}$ means addition modulo q.

Definition 8 : [15]. An q-valued logic function f satisfies the error propagation criterion along a vector $u \in V_k$ if its directional derivative along the vector u is a balanced function, i.e. its values $0,1,\ldots,q-1$ occur with equal probabilities: $p(D_u f(x) = i (\mathrm{mod}\, q)) = \frac{1}{q}$ for all $i = 0,1,\ldots,q-1$. In other words, $K^0 = K^1 = \ldots = K^{q-1}$, where K^i is the number of sets of values of variables on which the derivative takes on a value i.

Definition 9 : [15]. A q-valued logic function f satisfies the error propagation criterion of the degree k if it satisfies the error propagation criterion for all vectors u of weight $1 \le \varpi(u) \le k$.

Definition 10 : [15]. A q-valued logic function satisfies the strict avalanche criterion if it satisfies the error propagation criterion of the degree 1.

Using the above definitions for estimation of the avalanche characteristics of component 4-functions, it is easy to establish that the S-box (1) represented as component 4-functions (7) satisfies the strict avalanche criterion of component 4-functions.

Method for the synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions

Nevertheless, despite the method of synthesis of S-boxes satisfying the SAC of component 4-functions, as well as the method for synthesis of S-boxes corresponding simultaneously to the SAC of component Boolean functions and 4-functions [13], the practical application of these S-boxes is difficult due to their insufficient length $N = 16$, while in modern cryptographic algorithms, S-boxes of length $N = 256$ are used. This circumstance determines the need to develop new methods for the synthesis of S-boxes satisfying the SAC of component 4-functions and, at the same time, have good avalanche characteristics of component Boolean functions.

The performed research shows that it is promising to develop a recurrent method for constructing S-boxes with good avalanche characteristics of component Boolean and quaternary functions, which

we represent in the form of steps, accompanying them with a specific example.

Step 1 : As a raw material for the developed method, a set of S-boxes of length $N = 16$ satisfying the SAC of 4-functions, which are constructed in [13], is used. The cardinality of this set is $J = 245760$ of bijective S-boxes.

As an example, we will consider the S-box (1).

Step 2 : A function F_m is specified as the high-order component 4-function in the decomposition of the S-box into 4-functions.

In the case of the S-box (1), this component 4-function has the form

$$F_m = [0001302213213231]. \tag{9}$$

Step 3 : A set of 4 permutations is formed in accordance with the following rule

$$p_j = x \underset{4}{\oplus} (j \circ d), \quad x = 0,1,...,N-1, \quad j = 0,1,2,3, \tag{10}$$

where d is one of the vectors of length $k = \log_4 N$ with 1 at one of its positions, the vector x runs through the quaternary representations of numbers from 0 to $N-1$, the sign $\underset{4}{\oplus}$ means addition modulo 4, $\circ$ is the symbol of elementwise multiplication of the quaternary representation of a number d by a value j.

In the case of our example $k = \log_4 16 = 2$, we take the value $d = [0 \quad 1]$, respectively, the set of permutations has the form

$$\begin{aligned}
p_0 &= [0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15];\\
p_1 &= [1\ 2\ 3\ 0\ 5\ 6\ 7\ 4\ 9\ 10\ 11\ 8\ 13\ 14\ 15\ 12];\\
p_2 &= [2\ 3\ 0\ 1\ 6\ 7\ 4\ 5\ 10\ 11\ 8\ 9\ 14\ 15\ 12\ 13];\\
p_3 &= [3\ 0\ 1\ 2\ 7\ 4\ 5\ 6\ 11\ 8\ 9\ 10\ 15\ 12\ 13\ 14].
\end{aligned} \tag{11}$$

Note, that these permutations are a special case of m-shift permutations [16].

Step 4 : Construct the function G_1 of length $4N$ according to the following rule

$$G_1\left[F_m\right] = \left\{ F_m \underset{4}{\oplus} c_1 \ \mid \ F_m(p_1) \underset{4}{\oplus} c_2 \ \mid \ F_m(p_2) \underset{4}{\oplus} c_3 \ \mid \ F_m(p_3) \underset{4}{\oplus} c_4 \right\}, \tag{12}$$

where $\{c_1, c_2, c_3, c_4\}$ is a set of constants that must contain all values from the set $\{0,1,2,3\}$. Accept by default $c_1 = 0, c_2 = 1, c_3 = 2, c_4 = 3$.

In our example, we get that the function G_1 will take the following form

$$G_1 = [00013022132132311121133003223020232200120331131003331231 \\ 00210212]. \quad (13)$$

Step 5 : We increase the length of the S-box to a value of $4N$ using the following construction

$$G_0 = \{S \mid S(p_1) \mid S(p_2) \mid S(p_3)\}. \quad (14)$$

Step 6 : We construct a new bijective S-box of length $4N$ satisfying the strict avalanche criterion of component 4-functions according to the following rule

$$S_1 = \{G_1 \cdot 4^k + G_0\}, k = \log_4 N. \quad (15)$$

In the case of our example, we get the following S-box of length $N = 64$

$$S_{64} = [0,1,3,23,62,2,42,41,22,60,43,20,61,40,63,21, \\ 17,19,39,16,18,58,57,14,12,59,36,38,56,15,37,13, \\ 35,55,32,33,10,9,30,34,11,52,54,28,31,53,29,8,7,48, \\ 49,51,25,46,50,26,4,6,44,27,5,45,24,47]. \quad (16)$$

It is easy to verify that the component 4-functions of the S-box (16) satisfies the conditions of **Definition 10**, and, accordingly, the S-box (16) satisfies the SAC in the sense of component 4-functions. Contrariwise, the resulting S-box has the following matrix of weights of the derivatives of the component Boolean functions

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$
000001	32	40	32	24	32	40
000010	32	32	32	32	32	32
000100	32	32	32	32	32	32
001000	32	32	32	32	32	32
010000	32	40	32	24	32	24
100000	32	32	32	32	32	32

, (17)

thus, component Boolean functions of the S-box (16) does not satisfy SAC of component Boolean functions.

Repeated application of the developed method to the S-box (16) of length $N = 64$ makes it possible to obtain on its basis a new S-box of length $N = 256$

$$
\begin{gathered}
S_{256} = [0,1,3,87,254,2,170,169,86,252,171,84,253,168,255,85,81,\\
83,167,80,82,250,249,14,12,251,164,166,248,15,165,13,163,247,\\
160,161,10,9,94,162,11,244,246,92,95,245,93,8,7,240,241,243,\\
89,174,242,90,4,6,172,91,5,173,88,175,145,147,231,144,146,58,\\
57,78,76,59,228,230,56,79,229,77,227,55,224,225,74,73,158,\\
226,75,52,54,156,159,53,157,72,71,48,49,51,153,238,50,154,68,\\
70,236,155,69,237,152,239,64,65,67,151,62,66,234,233,150,60,\\
235,148,61,232,63,149,35,119,32,33,138,137,222,34,139,116,\\
118,220,223,117,221,136,135,112,113,115,217,46,114,218,132,\\
134,44,219,133,45,216,47,128,129,131,215,126,130,42,41,214,\\
124,43,212,125,40,127,213,209,211,39,208,210,122,121,142,140,\\
123,36,38,120,143,37,141,199,176,177,179,25,110,178,26,196,\\
198,108,27,197,109,24,111,192,193,195,23,190,194,106,105,22,\\
188,107,20,189,104,191,21,17,19,103,16,18,186,185,206,204,187,\\
100,102,184,207,101,205,99,183,96,97,202,201,30,98,203,180,\\
182,28,31,181,29,200],
\end{gathered}
\tag{18}
$$

which also satisfies the SAC of component 4-functions, and is characterized by the following matrix of weights of the derivatives of component Boolean functions

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
00000001	128	160	128	96	128	160	128	128
00000010	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00010000	128	160	128	96	128	128	128	96
00100000	128	128	128	128	128	128	128	128
01000000	128	160	128	96	128	128	128	128
10000000	128	128	128	128	128	128	128	128

, (19)

thus, component Boolean functions of the S-box (18) does not satisfy the SAC of Boolean functions.

The experiments show that based on the full set of S-boxes of length $N = 16,$ that satisfy the strict avalanche criterion of component 4-functions, by applying the developed method, S-boxes of practically valuable length $N = 256$ can be obtained, which simultaneously satisfies the SAC of component 4-functions and the criterion of the maximum avalanche effect of Boolean functions. The amount of such S-boxes strongly depends on the value of the selected parameters $c_1, c_2, c_3, c_4,$ as well as on the selected direction vector d. For example, let the following parameters be given: the length of the S-box $N = 256,$ the parameter values $c_1 = 0, c_2 = 1, c_3 = 2, c_4 = 3$ at the first and second iteration of the method application, as well as the values $d = [0 \quad 1]$ at the first iteration of the method application and $d = [0 \quad 0 \quad 1]$ at the second iteration of the method application. Then we obtain that from the set of $J = 245760$ S-boxes of length $N = 256$ obtained on the basis of the set of S-boxes of length $N = 16$ [13] and satisfying SAC of the component 4-functions, exactly $J_1 = 3968$ S-boxes simultaneously satisfies to the criterion of the maximum avalanche effect of component Boolean functions. As an example, we give one of these S-boxes of length $N = 256$ built on the basis of the S-box $S = [0,1,2,12,7,11,3,8,15,9,6,13,5,4,10,14]$

$$S_{256} = [1,2,252,0,171,3,168,87,169,86,253,255,84,170,254,85,82,12,80,81,83,$$
$$248,167,251,166,13,15,249,250,14,165,164,92,160,161,162,8,247,11,163,93,$$
$$95,9,246,94,245,244,10,240,241,242,172,7,91,243,88,175,89,6,173,5,4,90,$$
$$174,66,60,64,65,67,232,151,235,150,61,63,233,234,62,149,148,76,144,145,$$
$$146,56,231,59,147,77,79,57,230,78,229,228,58,224,225,226,156,55,75,227,$$
$$72,159,73,54,157,53,52,74,158,49,50,236,48,155,51,152,71,153,70,237,239,$$
$$68,154,238,69,124,128,129,130,40,215,43,131,125,127,41,214,126,213,212,$$
$$42,208,209,210,140,39,123,211,120,143,121,38,141,37,36,122,142,33,34,220,$$
$$32,139,35,136,119,137,118,221,223,116,138,222,117,114,44,112,113,115,$$
$$216,135,219,134,45,47,217,218,46,133,132,192,193,194,188,23,107,195,104,$$
$$191,105,22,189,21,20,106,190,17,18,204,16,187,19,184,103,185,102,205,207,$$
$$100,186,206,101,98,28,96,97,99,200,183,203,182,29,31,201,202,30,181,180,$$
$$108,176,177,178,24,199,27,179,109,111,25,198,110,197,196,26].$$

(20)

The component 4-functions of following S-box satisfies the SAC as well as component Boolean functions satisfies the criterion of the maximum avalanche effect, which can be shown with help of its matrix of weights of the derivatives of component Boolean functions

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
00000001	128	160	128	160	128	128	128	160
00000010	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00010000	128	160	128	160	128	128	128	128
00100000	128	128	128	128	128	128	128	128
01000000	128	160	128	160	128	128	128	128
10000000	128	128	128	128	128	128	128	128

(21)

This set of $J_1 = 3968$ S-boxes which have good avalanche characteristics both in the sense of component Boolean functions and in the sense of component 4-functions, and thus can be recommended for practical application.

Conclusion

We note the main results obtained in the paper:

1. A recurrent method for the synthesis of S-boxes satisfying the strict avalanche criterion of component 4-functions has been developed, which allows obtaining S-boxes of any given length $N = 4^k$, in particular, of practically valuable length $N = 256$.
2. Based on the known set of S-boxes of length $N = 16$ and cardinality $J = 245760$, a set of S-boxes of length $N = 64$ and a set of S-boxes of length $N = 256$ are obtained, the component 4-functions of which satisfy the strict avalanche criterion.
3. In the constructed set of S-boxes of length $N = 256$ which satisfies the SAC of component 4-fucntions, the $J_1 = 3968$ S-boxes which simultaneously satisfies the criterion of the maximum avalanche effect of component Boolean functions are found. In view of the fact that these S-boxes have good avalanche characteristics both in the sense of component Boolean functions and in the sense of component 4-functions, they can be recommended for practical use for modernizing existing cryptographic algorithms, as well as for developing new ones.

References

[1] Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. Wiley, 2015, 784 p. DOI: 10.1002/9781119183471

[2] FIPS 197. [Electronic resource] Advanced encryption standard, 2001. http://csrc.nist.gov/publications/

[3] Khadija Achkoun, Charifa Hanin & Fouzia Omary (2020) SPF-CA: A new cellular automata based block cipher using key-dependent S-boxes, *Journal of Discrete Mathematical Sciences and Cryptography,* 23:8, 1529-1544, DOI: 10.1080/09720529.2019.1649031

[4] Zhdanov O.N. Methods for choosing key information for a block encryption algorithm [Original text in Russian], Moscow : INFRA-M, 2013, 90 p.

[5] Sokolov A.V. New methods for synthesis of nonlinear transformations of modern ciphers [Original text in Russian], Germany, Lap Lambert Academic Publishing, 2015,100 p.

[6] Logachev O.A., Salnikov A.A., Yashchenko V.V. Boolean functions in coding theory and cryptography. *American Mathematical Soc.*, 2012, 334 p. DOI: 10.1090/mmono/241

[7] Kim K., Matsumoto T., Imai H. A recursive construction method of S-boxes satisfying strict avalanche criterion, Proc. of CRYPTO'90, Springer-Verlag, 1990, pp.565-574. DOI: 10.1007/3-540-38424-3_39

[8] Sokolov A.V. Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion. *Radioelectronics and Communications Systems,* 2013, Vol. 56, No. 8, pp. 415-423. DOI: 10.3103/s0735272713080049

[9] Mazurkov M.I., Sokolov A.V. Non-linear S-box of Nyberg construction with maximal avalanche effect, *Radioelectronics and Communications Systems,* 2014, Vol. 57, No. 6, P. 274-281. DOI: 10.3103/s0735272714060053

[10] Chandrasekharappa T.G.S., Prema K.V., Kumara Shama. S-boxes generated using Affine Transformation giving Maximum Avalanche Effect. *Internation Journal of Computer Science and Engineering.* 2011. Vol.3(#9). P.3185—3193.

[11] Baigneres T., Stern J., Vaudenay S. Linear cryptanalysis of non binary ciphers, International Workshop on Selected Areas in Cryptography, Springer, Berlin, Heidelberg, 2007, pp. 184-211. DOI: 10.1007/springerreference_336

[12] Grassl M. et al. Applying Grover's algorithm to AES: quantum resource estimates, Post-Quantum Cryptography, Springer, Cham, 2016, pp. 29-43. DOI: 10.1007/978-3-319-29360-8_3

[13] Sokolov A.V., Zhdanov O.N. Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength, *Siberian Journal of Science and Technology,* 2019, Vol. 20, No. 2, pp.183-190. DOI: 10.31772/2587-6066-2019-20-2-183-190

[14] Sokolov A.V., Zhdanov O.N. Prospects for the Application of Many-Valued Logic Functions in Cryptography. International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018. pp. 331-339. DOI: 10.1007/978-3-319-91008-6_33

[15] Sokolov A.V., Zhdanov O.N. Cryptographic constructions based on many-valued logic functions [Original text in Russian], Moscow: Scientific thought, 2020. 192 p. DOI: 10.12737/1045434

[16] Trakhtman A.M., Trakhtman V.A. Fundamentals of the theory of discrete signals at finite intervals [Original text in Russian]. Moscow: Sov.radio, 1975. 208 p.

Received February, 2021

Revised June, 2021