Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 4, pp. 1121–1133
DOI : 10.1080/09720529.2021.2018112

Synthesis method for S-boxes satisfying the criterion of correlation immunity of Boolean and 4-functions

E. V. Bakunina *
O. V. Dykyi
Department of Cybersecurity
National University "Odessa Law Academy"
Odessa, 65011
Richelievskaya st., 28
Ukraine

Abstract

The improvement of cryptanalysis methods, in particular, using the mathematical apparatus of many-valued logic functions, determines the need to create methods for the synthesis of cryptographic primitives, first of all, S-boxes that satisfy the criteria of cryptographic quality both in the sense of component Boolean functions, and in the sense of their possible representations by functions of many-valued logic. The most important criterion characterizing the ability of the S-box, and hence, of the entire cryptographic transformation in which it is used, to resist attacks of correlation cryptoanalysis, is the criterion of the correlation immunity of component functions. At the moment, there are no methods for the synthesis of S-boxes that satisfy the criterion of correlation immunity both in the sense of component Boolean functions and in the sense of component functions of many-valued logic, which complicates the further development of symmetric cryptographic algorithms, considering their possible representation using many-valued logic functions. In this paper, we propose a method for the synthesis of a full class of S-boxes of length N=16 corresponding to both the criterion of the correlation immunity of component Boolean functions and the criterion of the correlation immunity of component 4-functions. With the help of the developed method, it was possible to construct a set of 18 304 S-boxes that satisfies the criterion of correlation immunity both in the sense of component Boolean functions and in the sense of component 4-functions. The synthesized class of S-boxes can be used to increase the diffusion and confusion of modern symmetric cryptographic algorithms, as well as to increase their protection against promising cryptanalysis attacks based on many-valued logic functions.

Subject Classification: *(2010) 94A60.*

Keywords: *Cryptography, S-box, Correlation immunity, Many-valued logic function.*

* *E-mail:* **elenabakunina72@gmail.com (Corresponding Author)**

1. Introduction

One of the most important area in any complex information protection system is occupied by the cryptographic subsystem. At the same time, since the development by C. Shannon of the mathematically strict theory of secret communication [1], the theory of cryptographic strength has received significant development, largely due to the introduction and description of criteria for the cryptographic quality of component Boolean functions, which are the basis of representation of the cryptographic algorithm constructions [2, 3].

Nevertheless, the further development of methods of cryptography and cryptanalysis, as well as the development of new methods of cryptanalytic attacks based on the many-valued logic functions (MVLF) [4], actualizes the transition to the next stage of development of cryptography, based on taking advantage of the use of many-valued logic functions.

The transition to a new stage means the development of cryptographic primitives, first of all, S-boxes, for which the criteria for the cryptographic quality of component Boolean functions as well as criteria for the cryptographic quality of many-valued logic functions (with the help of which it is possible to represent constructions of almost all modern cryptographic algorithms) [5] are fulfilled.

At present, S-boxes which are optimal from the point of view of the criterion of nonlinearity and strict avalanche criterion of component Boolean functions as well as component MVLF have been created. Nevertheless, the task of construction of S-boxes, which satisfies the correlation immunity (CI) criterion both in the sense of component Boolean functions and in the sense of component MVLF, remains unsolved.

The purpose of this paper is to develop a method for synthesis of S-boxes satisfying both the criterion of correlation immunity of component Boolean functions and the criterion of correlation immunity of component 4-functions.

2. Statement of the problem

The S-box is the most important component of modern symmetric cryptographic algorithms, due to both high encryption quality and a high level of performance they provide [3].

To estimate the cryptographic quality of S-boxes, the following approach is used: S-box of length N is represented in the form of $k = \log_2 N$ component Boolean functions, after which a set of cryptographic quality

criteria is applied to each of them. Among the cryptographic quality criteria of Boolean functions, the most important are such criteria as: algebraic degree of nonlinearity, distance of nonlinearity, strict avalanche criterion, and criterion of correlation immunity [6].

In this case, the most important criterion characterizing the ability of the S-box, and hence the entire cryptographic transformation in which it is used, to resist attacks of correlation cryptanalysis is the criterion of the correlation immunity of the S-box component functions.

The synthesis of sets of correlation immune Boolean functions was performed in [7, 8], while the efficient methods for practical implementation of cryptographically robust Boolean function can be based on [9].

Based on the full set of correlation-immune functions, S-boxes can be synthesized, for example, using the technique [10].

A lot of research has been devoted to the methods of synthesis of S-boxes, the component functions of which satisfy the criterion of correlation immunity, for example [11, 12]. Methods for recurrent increase of the length of correlation-immune S-boxes are also known.

It is also established [6] that S-boxes consisting of component Boolean functions, each of which satisfies the criterion of correlation immunity of component Boolean functions, are characterized by ideal (consisting exclusively of zero values) matrices of correlation coefficients of the output and input vectors.

Nevertheless, the continuing rapid development of cryptanalysis methods, including quantum cryptanalysis, leads to the need for both further improvement of the structure of the cryptographic algorithm as well, as its components.

It is known that the key of modern symmetric cryptographic algorithms is a pseudo-random sequence. It means that with a sufficiently large key length, a quantum attack on a cryptographic algorithm should be performed out by the "brute force" method or using any known vulnerability to break the cryptographic algorithm, as opposed to using an algorithmic attacks, for example, Shor's algorithm [13 ... 15], for breaking algorithms of asymmetric cryptography, which makes detailed research and improvement of symmetric cryptographic algorithms structure especially relevant in the conditions of post-quantum cryptography.

On the other hand, cryptanalysis attacks on modern symmetric cryptographic algorithms, implying the use of MVLF, are already known today [4].

This circumstance determines the urgency of the problem of research of the cryptographic quality of modern symmetric cryptographic algorithms

not only using the mathematical apparatus of Boolean functions, but also when they are represented using many-valued logic functions.

Currently, the theory of cryptographic quality based on the many-valued logic functions is going through a period of active development. In particular, a criterion for the algebraic degree of nonlinearity of many-valued logic functions, a criterion for nonlinearity, an error propagation criterion, as well as a correlation immunity criterion for the many-valued logic functions are introduced [5].

One of the most important practically applicable S-boxes length value is $N = 16$. S-boxes of this length are used in many modern cryptographic algorithms, for example, the Magma cryptographic algorithm [16]. It is known [5] that these S-boxes can be represented both using the mathematical apparatus of Boolean functions, and using the mathematical apparatus of 4-functions.

Nevertheless, the classes of S-boxes of practically valuable length $N = 16$, satisfying to both the criterion of the correlation immunity of component Boolean functions and the criterion of correlation immunity of component 4-functions remain unexplored. At the moment, there no information in open sources either about methods for synthesis of such S-boxes, or about accurate estimates of the number of their possible structures.

3. Materials and methods

Let some S-box of length $N = 16$ to be given

$$S = [4 \quad 2 \quad 12 \quad 1 \quad 10 \quad 9 \quad 7 \quad 15 \quad 11 \quad 13 \quad 3 \quad 14 \quad 5 \quad 6 \quad 8 \quad 0]. \qquad (1)$$

In accordance with the approach of estimation of its cryptographic quality based on the research of component Boolean functions, we represent it in the form of four component Boolean functions

S	4	2	12	1	10	9	7	15	11	13	3	14	5	6	8	0
f_{21}	0	0	0	1	0	1	1	1	1	1	1	0	1	0	0	0
f_{22}	0	1	0	0	1	0	1	1	1	0	1	1	0	1	0	0.
f_{23}	1	0	1	0	0	0	1	1	0	1	0	1	1	1	0	0
f_{24}	0	0	1	0	1	1	0	1	1	1	0	1	0	0	1	0

(2)

In order to determine the correlation immunity of the found component Boolean functions of the S-box (1), we use the following definitions.

Definition 1 [3] : A Boolean function $f(x)$, $x \in V_k$, is called a correlation immune of order m, $1 \le m \le k$ if the output $y = f(x_1^k)$ and any set of its m input variables are statistically independent.

Definition 2 [3] : A subfunction of a Boolean function $f(x)$, $x \in V_k$, is a function f' obtained by substitution of constants "0" or "1" instead of some variables. If we substitute constants $\sigma_{i_1}, \cdots, \sigma_{i_s}$ in the function f instead of variables $x_{i_1}, \cdots, x_{i_s}$, respectively, then the resulting subfunction is denoted as $f^{\sigma_{i_1}, \cdots, \sigma_{i_s}}_{x_{i_1}, \cdots, x_{i_s}}$. If a constant is not substituted to the variable x_i, then it is called as a free variable.

For example, let a Boolean function $f(x_1, x_2, x_3)$ be given, then its subfunctions will be $f'(x_1, x_2, 0)$, $f'(x_1, x_2, 1)$, $f'(x_1, 0, 0)$, $f'(x_1, 0, 1)$, etc.

Definition 3 [3] : Boolean function $f(x)$, $x \in V_k$, is called correlation immune of order m, if weight is equal to $wt(f') = wt(f)/2^m$, for any of its subfunction f' of $k - m$ variables.

As an example, using **Definition 3**, we research the first component Boolean function (2) of the S-box (1) for compliance with the criterion of first-order correlation immunity. To do this, we find all its subfunctions of $4 - 1 = 3$ variables

$$
\begin{aligned}
f'_{21}(x_1, x_2, x_3, 0) &= [0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0] \\
f'_{21}(x_1, x_2, x_3, 1) &= [0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0] \\
f'_{21}(x_1, x_2, 0, x_4) &= [0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0] \\
f'_{21}(x_1, x_2, 1, x_4) &= [0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0] \\
f'_{21}(x_1, 0, x_3, x_4) &= [0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0]. \\
f'_{21}(x_1, 1, x_3, x_4) &= [0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0] \\
f'_{21}(0, x_2, x_3, x_4) &= [0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1] \\
f'_{21}(1, x_2, x_3, x_4) &= [1\ \ 1\ \ 1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0]
\end{aligned}
\qquad (3)
$$

Thus, since the first component function f_1 (2) is balanced, and all its subfunctions of 3 variables (3) are also balanced, according to the **Definition 3** the first component Boolean function f_1 of the S-box (1) is correlation immune of the first order. It is also easy to establish that all other component Boolean functions (2) are also correlation immune of the first order, which means that the S-box (1) satisfies the criterion of correlation immunity of the first order.

Note also that the S-box (1) in accordance with the approach [5] can be represented in the form of two component 4-functions as follows

S	4	2	12	1	10	9	7	15	11	13	3	14	5	6	8	0
f_{41}	0	2	0	1	2	1	3	3	3	1	3	2	1	2	0	0.
f_{42}	1	0	3	0	2	2	1	3	2	3	0	3	1	1	2	0

(4)

To determine the correspondence of the found component 4-functions (4) to the criterion of correlation immunity, we denote the following. The concept of the criterion of correlation immunity was introduced in [17], while the definition of the correlation independence of the output of the q-function from its given input variable, as well as the definition of the correlation immunity of 3-functions, based on the definition of the imbalance of the MVLF were introduced in [18].

Next, we introduce the definition of the correlation immunity of 4-functions, which we need for further research, based on the generalized definition of the imbalance of the MVLF.

For a given sequence f, we can introduce a vector $K = \{K_0, K_1, ..., K_{q-1}\}$, where K_u is the number of occurrences of a character $u \in \{0, 1, ..., q-1\}$ in the sequence f.

Definition 4 : An imbalance of a sequence f is the absolute value of the sum of element-wise products of vector K elements by the corresponding elements of the exponential alphabet $\{z_0, z_1, ..., z_{q-1}\}$

$$\Delta(f) = | K_0 z_0 + K_1 z_1 + ... + K_{q-1} z_{q-1} | . \quad (5)$$

Based on the **Definition 4** of the imbalance of the MVLF, we introduce the definition of the independence of the output of the 4-function from its input variables, as well as the definition of the correlation immunity of the 4-function.

Definition 5 : A subfunction of a q-function $f(x)$ is a function f' obtained by substituting in f the values from the set $\{0, 1, ...q-1\}$ instead of some variables. If we substitute constants $\sigma_{i_1}, \cdots, \sigma_{i_s}$ in the function f instead of variables $x_{i_1}, \cdots, x_{i_s}$, respectively, then the resulting subfunction is denoted as $f^{\sigma_{i_1}, \cdots, \sigma_{i_s}}_{x_{i_1}, \cdots, x_{i_s}}$.

Definition 6 : It is said that the output of a 4-function $f(x)$ is independent from the group of its input variables $\{x_i\}$, $i = 1, ..., m$, if, when substituting

any constants $\sigma_{i_1},\cdots,\sigma_{i_s}\in\{0,1,...q-1\}$ instead of these variables, the imbalance of the subfunctions obtained in such way is equal to $\Delta_{f'}=\frac{\Delta_f}{4^m}$.

Definition 7 : A 4-function $f(x)$ is said to be correlation immune of order $m\le k$ if its output is independent with respect to any group of *m* its input variables, i.e. the unbalance of all its subfunctions of $k-m$ variables is equal to $\Delta_{f'}=\frac{\Delta_f}{4^m}$.

Thus, using the conditions of **Definition 7**, we can check the component 4-functions (4) of the S-box (1) for compliance with the first order correlation immunity criterion. For example, let's find the subfunctions of $2-1=1$ variable of 4-function f_1

$$\begin{aligned}
f_{41}'(x_1,0)&=[0\quad 2\quad 3\quad 1]\\
f_{41}'(x_1,1)&=[2\quad 1\quad 1\quad 2]\\
f_{41}'(x_1,2)&=[0\quad 3\quad 3\quad 0]\\
f_{41}'(x_1,3)&=[1\quad 3\quad 2\quad 0].\\
f_{41}'(0,x_2)&=[0\quad 2\quad 0\quad 1]\\
f_{41}'(1,x_2)&=[2\quad 1\quad 3\quad 3]\\
f_{41}'(2,x_2)&=[3\quad 1\quad 3\quad 2]\\
f_{41}'(3,x_2)&=[1\quad 2\quad 0\quad 0]
\end{aligned}\qquad (6)$$

Using **Definition 4**, it is easy to determine that there are subfunctions of the first component 4-function of the S-box (1), the weight of which is not equal to 0, for example, the weight of the subfunction $f_{41}'(x_1,1)=[2\quad 1\quad 1\quad 2]$ is equal to $\Delta(f_{41}'(x_1,1))=\sqrt{8}$. It is easy to see that the same is true for the component function f_{42}. Thus, the S-box (1) satisfies the criterion of correlation immunity of component Boolean functions and does not satisfy the criterion of correlation immunity of component 4-functions. This circumstance can be used by a cryptanalyst to perform correlation analysis attacks on the specified cryptographic construction using 4-functions.

Thus, from a practical point of view, the problem of finding substitution constructions of length $N=16$ that would satisfy correlation immunity both in the sense of component Boolean functions and in the sense of component 4-functions is relevant.

4. Experiments

One of the ways to solve the problem of synthesizing a complete set of S-boxes that satisfy the criterion of correlation immunity both in the sense of component Boolean functions and in the sense of component 4-functions is to use the brute force method.

Nevertheless, the method for synthesizing a complete set of S-boxes based on exhaustive search, even for length $N = 16,$ is associated with significant computational costs due to the need to perform search in a set of $J = 16! = 20922789888000$ elements.

This circumstance leads to the need to develop a constructive method for the synthesis of these cryptographic structures.

In this paper, we propose the following method for the synthesis of S-boxes that satisfy both the criterion of the correlation immunity of component Boolean functions and the criterion of the correlation immunity of component 4-functions, which we write in the form of specific steps:

Step 1 : By considering all possible variants of Boolean functions of length $N = 16,$ the number of which is $J = 2^{16} = 65536,$ using **Definition 3**, select such from them that are correlation immune of the first order.

Step 2 : Based on the found set of first-order correlation immune Boolean functions, in accordance with the S-box construction theorem [10], construct a complete set of S-boxes whose component functions are first-order correlation immune.

Step 3 : Represent each of the obtained S-boxes included in the complete set of S-boxes built in Step 2 in the form of two component 4-functions.

Step 4 : Based on **Definition 7**, research the component 4-functions of the constructed S-boxes for compliance with the criterion of correlation immunity of the first order of the component 4-functions. Discard all S-boxes in which at least one component 4-function is not correlation immune.

5. Results

Execution of the presented algorithm allows you to obtain the following results.

The research of the complete set of $J = 65536$ Boolean functions made it possible to establish that the total number of first-order correlation

immune Boolean functions is 222, which corresponds to the results obtained in [8]. On the basis of this set of Boolean functions, by applying the method [10], it is possible to construct a set of 6 728 064 bijective S-boxes, each of which satisfies the criterion of correlation immunity of component Boolean functions.

Representing each of the S-boxes in the form of component 4-functions, and testing them for compliance to the criterion of the independence of the output from the input variables, we obtain the results presented in Table 1. In Table 1 the following designations are accepted: α_{11}, α_{12} are the coefficients, the value of which determines whether the component function f_{41} is independent of its variables x_1 and x_2 respectively; α_{21}, α_{22} are the coefficients, the value of which determines whether the component function f_{42} is independent of its variables x_1 and x_2 respectively. The value of these coefficients equal to 0 indicates non-compliance to the specified criterion, while the value equal to 1 indicates compliance.

Analysis of the data presented in Table 1 allows us to establish that among the set of S-boxes whose component Boolean functions satisfies the CI criterion there are exactly 18 304 S-boxes that satisfy both the criterion of correlation immunity of component Boolean functions and the criterion of correlation immunity of component 4-functions. The design of the presented in this paper method allows us to assert that this set is complete.

The set of S-boxes obtained in this paper, simultaneously satisfying both the criterion of the correlation immunity of Boolean functions and the criterion of the correlation immunity of component 4-functions, is a powerful basis for constructing cryptographic algorithms that provide protection against correlation cryptanalysis.

As an example, we present one of the constructed 18 304 S-boxes that satisfies the criterion of correlation immunity both in the sense of component Boolean functions and in the sense of component 4-functions

$$S = [4 \quad 12 \quad 2 \quad 10 \quad 1 \quad 9 \quad 7 \quad 15 \quad 11 \quad 3 \quad 13 \quad 5 \quad 14 \quad 6 \quad 8 \quad 0]. \qquad (7)$$

Note that the cardinality of the obtained set of optimal S-boxes is sufficient to apply the concept of their operational change in order to increase the number of protection levels of the information security systems being developed.

At the same time, the developed method can be used to construct longer S-boxes, for example, of length $N = 256$, oriented to the use in such cryptographic algorithms as Kalyna [19], AES [20], BelT [21], Kuznechik [16] or the similar ones.

Table 1

The number of S-boxes satisfying the given correlation properties

$[\alpha_{11} \quad \alpha_{12} \quad \alpha_{21} \quad \alpha_{22}]$	Number of S-boxes
[0 0 0 0]	1432 704
[0 0 0 1]	769856
[0 0 1 0]	769856
[0 0 1 1]	239360
[0 1 0 0]	769856
[0 1 0 1]	337152
[0 1 1 0]	334912
[0 1 1 1]	93696
[1 0 0 0]	769856
[1 0 0 1]	334912
[1 0 1 0]	337152
[1 0 1 1]	93696
[1 1 0 0]	239360
[1 1 0 1]	93696
[1 1 1 0]	93696
[1 1 1 1]	18304

In this case, to increase the computational efficiency, the synthesis of the initial S-boxes corresponding to the criterion of correlation immunity can be performed in accordance with the well-known algorithms [11, 12]. Obviously, in the case of using this method for the length $N = 256$, their possible representation using 16-component functions should also be considered.

Conclusion

We note the main results obtained in the paper:

1. the method for the synthesis of a full class of S-boxes of length $N = 16$ corresponding to both the criterion of correlation immunity of component Boolean functions and the criterion of correlation immunity of component 4-functions was developed.
2. the developed method made it possible to construct set of 18 304 S-boxes that satisfy the criterion of correlation immunity both in the

sense of component Boolean functions and in the sense of component 4-functions.

3. the synthesized class of S-boxes satisfying the criterion of correlation immunity both in the sense of component Boolean functions and in the sense of component 4-functions can be used to increase the diffusion and confusion of modern symmetric cryptographic algorithms, as well as to increase their protection against promising cryptanalysis attacks based on MVLF.

As a further direction of research, it is worth to note the development of methods for the synthesis of S-boxes of larger lengths, that are correlation immune both in the sense of component Boolean functions and in the sense of their representation using many-valued logic functions.

References

[1] Shannon C. E. Communication Theory of Secrecy Systems, *Bell System Technical Journal,* 1949, Vol. 28-4, P. 656-715. DOI: 10.1002/j.1538-7305.1949.tb00928.x

[2] Zhdanov O. N. Methodology for selecting key information for a block cipher algorithm, Moscow : INFRA-M, 2013, 90 p.

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

[4] Baigneres T., Stern J., Vaudenay S. Linear cryptanalysis of non binary ciphers. International Workshop on Selected Areas in Cryptography, Springer, Berlin, Heidelberg, 2007. P. 184-211. DOI: 10.1007/978-3-540-77360-3_13

[5] Sokolov A. V., Zhdanov O. N. Cryptographic constructions based on many-valued logic functions. Monograph, Moscow: Scientific Thought, 2020, 192 p. DOI: 10.12737/1045434

[6] Salnikov A. A., Logachev O. A. Boolean Functions in Coding Theory & Cryptography, Universities Press (India) Private Limited, 2017, 334 p.

[7] Karelina E. K. On a method of synthesis of correlation-immune Boolean functions. *Discrete Mathematics and Applications*, 2020, Vol. 30, No. 2, P. 79-91. DOI: 10.1515/dma-2020-0008

[8] Yakovlev S. V. Balanced criteria for the quality of long-term key elements in the GOST 28147-89 algorithm, *Information technology and computer engineering*, 2009, P. 5-12.

[9] Enaul Haq Shaik & Nakkeeran Rangaswamy. Implementation of 1×2 decoder and XOR-XNOR logic functions on a PhC structure, *Journal of Information and Optimization Sciences*, 2017, 38:6, P. 953-960. DOI: 10.1080/02522667.2017.1372142

[10] Kim K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC. Proc. of Asiacrypt'91, Springer Verlag, 1991. P. 59-72. DOI: 10.1007/3-540-57332-1_5

[11] Mazurkov M. I. Synthesis method of optimal substitution constructions based on the criterion of zero correlation between the output and input data vectors, Radioelectronics and Communications Systems, 2012, Vol. 55, No. 12. P. 533-543. DOI: 10.3103/s0735272712120023

[12] Mazurkov M. I., Sokolov A. V. Method of S-boxes synthesis based on the criterion of zero correlation between the output and input data vectors and the strict avalanche criterion. *Radioelectronics and Communications Systems*, 2014, Vol. 57, No. 8, P. 376-381. DOI: 10.3103/s0735272714080068

[13] Monz T. et al.Realization of a scalable Shor algorithm, Science, 2016, Vol. 351, No. 6277. P. 1068-1070. DOI: 10.1126/science.aad9480

[14] Gerjuoy E. Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers, *American journal of physics*, 2005, Vol. 73, No. 6, P. 521-540. DOI: 10.1119/1.1891170

[15] Politi A., Matthews J. C. F., O'brien J. L. Shor's quantum factoring algorithm on a photonic chip, Science, 2009, Vol. 325, No. 5945, P. 1221-1221. DOI: 10.1126/science.1173731

[16] GOST 34.12-2018, Information technology, Cryptographic data security, Block ciphers, Moscow, Standardinform, 17 p.

[17] Gopalakrishnan K. Stinson D. R. Three characterizations of non-binary correlation-immune and resilient functions, Designs, Codes and Cryptography, 1995, 5, P. 241-251. DOI: 10.1007/bf01388386

[18] Sokolov A. V., Zhdanov O. N. Correlation immunity of three-valued logic functions, *Journal of Discrete Mathematical Sciences and Cryptography*, 2020, P. 1-17. DOI: 10.1080/09720529.2020.1781882

[19] DSTU 7624:2014, Information technologies, Cryptographic data security, Symmetric block transformation algorithm, Ministry of Economic Development of Ukraine, 2016. 221 p.

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

[21] STB 34.101.31-2011, Information technology and security, Information protection, Cryptographic algorithms for encryption and integrity control, Minsk, Gosstandart, 31 p.

Received June, 2021

Revised November, 2021