Artem SOKOLOV[1], Nadiia KAZAKOVA[2], Oleksii FRAZE-FRAZENKO[3]

DOI: https://doi.org/10.53052/9788366249868.21

# METODY BADANIA WŁAŚCIWOŚCI LAWINOWYCH FUNKCJI SKŁADOWYCH LOGIKI WIELOWARTOŚCIOWEJ

**Streszczenie:** Najważniejszym elementem każdego systemu bezpieczeństwa informacji są symetryczne szyfry blokowe. Opracowano oraz dokonano oceny jakości symetrycznych szyfrów blokowych, które reprezentuje się w postaci funkcji Boole'a. Do tego zadania wykorzystano szereg kryteriów jakości kryptograficznej. Najważniejszym z nich jest kryterium propagacji błędu oraz kryterium silnej lawiny. Jednak ostatnie badania pokazują, że reprezentacja konstrukcji algorytmów kryptograficznych z wykorzystaniem aparatu matematycznego funkcji Boole'a nie jest wyczerpująca, konieczne jest również rozważenie możliwości ich reprezentacji za pomocą wielowartościowych funkcji logicznych, do których również można zastosować specjalne kryteria jakości kryptograficznej. W artykule przedstawiono wyniki badań charakterystyk lawinowych S-boxów niektórych znanych algorytmów kryptograficznych.

**Słowa kluczowe:** ochrona informacji, kryptografia, ścisłe kryterium lawinowe, funkcja logiki wielowartościowej

# RESEARCH METHODS FOR AVALANCHE PROPERTIES OF MANY-VALUED LOGIC COMPONENT FUNCTIONS

**Summary:** Block symmetric ciphers are a very important component of any information security system. To develop and estimate the quality of block symmetric ciphers, today their representation in the form of Boolean functions is used, to which cryptographic quality criteria are applied, the most important of which are the error propagation criterion and the strict avalanche criterion. Recent research shows that the representation of structures of cryptographic algorithms using the mathematical apparatus of Boolean functions is not exhaustive; the possibility of their representation using many-valued logic must be considered, for which the special criteria for cryptographic quality may be applied. In the paper we represent the results of research of the avalanche characteristics of S-boxes of some known cryptographic algorithms.

**Keywords:** information protection, cryptography, strict avalanche criterion, many-valued logic function

[1] Engineering Science Ph.D., Odessa National Polytechnic University, associate professor at the department of Cybersecurity and Software, radiosquid@gmail.com

[2] Doctor of Engineering, Odesa State Environmental University, head of department of information technology, kaz2003@ukr.net

[3] Engineering Science Ph.D., Odesa State Environmental University, associate professor at the department of information technology, frazenko@gmail.com

## 1. Introduction

Block symmetric ciphers (BSC) are an important component of any modern information security system, which largely determine its effectiveness. Today there are many different approaches to the synthesis of block symmetric ciphers, which are aimed at solving of one problem - the implementation of the two main methods introduced by Claude Shannon - diffusion and confusion [1] by these cryptographic algorithms.

Diffusion is a method in which redundancy in the input statistics is "distributed" throughout the structure of the output data, while confusion is a method in which the dependence of the key and the output data becomes as complex as possible, in particular, nonlinear.

The classic approach to the synthesis and analysis of cryptoalgorithms and cryptographic primitives on which they are based (primarily, S-boxes, which largely determine the cryptographic quality of cryptographic transformations), is the use of mathematical apparatus of Boolean functions. This approach involves the description of cipher constructs using a set of Boolean functions, to which a set of cryptographic quality criteria is then applied. One of the main criteria, which largely characterizes the level of diffusion, is the error propagation criterion and its special case - a strict avalanche criterion (SAC).

Today, for the numerical estimation of the level of diffusion and confusion, there is a common approach, which involves the representation of the structures of cryptographic algorithms using Boolean functions to which a set of criteria for cryptographic quality is then applied. Thus, the main criterion that characterizes the level of confusion is the distance of nonlinearity [2], while the main criterion that largely characterizes the level of diffusion is the criterion of error propagation and its special case - a strict avalanche criterion [3].

However, the rapid development of cryptanalysis methods, including possible cryptanalysis methods for quantum computers [4], determines the need for a more detailed research of the structure of cryptographic algorithms. In particular, modern methods of cryptanalysis can use the representation of cryptographic algorithms not only using Boolean functions, but also using many-valued logic functions [5]. Thus, when estimating the level of cryptographic quality of block symmetric ciphers, all their possible representations should be considered and researched.

The method of research of the avalanche properties of Boolean functions was introduced in [3], while in [6] this method was generalized to the case of functions of many-valued logic.

In the literature there are research of avalanche properties of the AES S-box, represented by Boolean functions, 4-functions, and 16-functions is known [7]. However, the cryptographic characteristics of other common modern cryptoalgorithms in the case of their representation by the functions of many-valued logic, remain unknown.

The purpose of this paper is to research and compare the avalanche properties of the component functions of the many-valued logic of cryptographic algorithms AES (USA), Kalyna (Ukraine), Kuznechik (Russia) and BelT (Belarus).

To achieve the purpose of the paper it is necessary to solve the following tasks:

1. development of indicators of maximum and integral deviation from SAC, which will allow to estimate and compare the degree of deviation from the requirements

of SAC of cryptographic structures of different lengths when they are represented in all possible ways using the functions of many-valued logic;

2. research of avalanche properties of component functions of many-valued logic of cryptoalgorithms AES (USA), Kalyna (Ukraine), Kuznechik (Russia) and BelT (Belarus);
3. comparative analysis of the obtained results on the avalanche characteristics of the researched cryptoalgorithms.

## 2. Presenting main material

We introduce the basic definitions necessary for research.

**Definition 1 [8].** The function of the $q$-valued logic of $k$ variables is the mapping $\{0,1,2,...,q-1\}^k \to \{0,1,2,...,q-1\}$.

Functions of many-valued logic are a more general mathematical object in comparison with Boolean functions. For example, Boolean functions are, by definition, mappings $\{0,1\}^k \to \{0,1\}$, that is, a special case of **Definition 1** at value $q=2$.

In [8] the basic definitions are introduced, which allow to estimate the avalanche properties of the functions of many-valued logic.

**Definition 2 [8].** The weight $\varpi(u)$ of a $q$-valued vector is the number of its nonzero components.

**Definition 3 [8].** The derivative of a $q$-function $f(x)$ in the direction of the vector $u$ is a function

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x)\,(\operatorname{mod} q) \ , \qquad (1)$$

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

**Definition 4 [8].** The function of $q$-valued logic $f(x)$ satisfies the error propagation criterion for vector $u \in V_k$ — $PC(u)$, if its derivative in the direction $u$ is a balanced function, that is, values $0,1,...,q-1$ are taken with equal probabilities: $p(D_u f(x) = i(\operatorname{mod} q)) = \dfrac{1}{q}$ for all $0,1,...,q-1$. In other words, $K^0 = K^1 = ... = K^{q-1}$, where $K^i$ is the number of sets of variable values on which the derivative takes the value $i$.

**Definition 5 [8].** The function of $q$-valued logic satisfies the of error propagation criterion of degree $m - PC(m)$, if it satisfies the error propagation criterion for all vectors $u$ of weight $1 \le \varpi(u) \le m$.

**Definition 6 [8].** A function of $q$-valued logic satisfies a strict avalanche criterion (SAC) if it satisfies the error propagation criterion of degree $1 - PC(1)$.

In essence, the strict avalanche criterion is a rigorous requirement that is quite difficult to fulfill, especially while maintaining compliance of the S-box to other criteria of cryptographic quality, primarily the criterion of high nonlinearity. Therefore, the S-boxes of practically used BSC, in particular, the cryptoalgorithms AES, Kalyna, BelT and Kuznechik researched in this paper do not satisfy the requirements of SAC even in the sense of component Boolean functions. However, it is clear that the S-box of practically used cryptoalgorithms should be as close as possible to satisfy the strict avalanche criterion.

To solve the problem of estimating and comparing avalanche properties of real S-boxes, it is advisable to introduce two indicators of cryptographic quality: maximum and integral deviation from SAC. We introduce these indicators on a specific example of the AES cryptoalgorithm S-box.

The S-box of the AES cryptographic algorithm [10] is constructed using the Nyberg construction [11]. S-boxes of the Nyberg construction are determined by the multiplicative inverse elements mapping of the Galois field $GF(2^k)$

$$y = x^{-1} \operatorname{modd}[f(z), p], \quad y, x \in GF(2^k), \tag{2}$$

which in the general case is combined with the affine transformation

$$b = A \cdot y + a, \quad a, b \in GF(2^k), \tag{3}$$

where a standard AES irreducible over the field $GF(2^8)$ polynomial $f(z) = 283_{10} = z^8 + z^4 + z^3 + z + 1$ is used, $A$ is a nonsingular affine transformation matrix, $a$ is a shift vector, $p = 2$ is a characteristic of the extended Galois field, $k = 8$, $0^{-1} \equiv 0$ is accepted, $a, b, x, y$ are elements of the extended Galois field $GF(2^k)$, that are considered as decimal numbers, or binary vectors, or polynomials of degree $k-1$.

The S-box of the AES cryptoalgorithm constructed according to (2) has the following form:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | *A* | *B* | *C* | *D* | *E* | *F* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 00 | 01 | 8D | F6 | CB | 52 | 7B | D1 | E8 | 4F | 29 | C0 | B0 | E1 | E5 | C7 |
| 1 | 74 | B4 | AA | 4B | 99 | 2B | 60 | 5F | 58 | 3F | FD | CC | FF | 40 | EE | B2 |
| 2 | 3A | 6E | 5A | F1 | 55 | 4D | A8 | C9 | C1 | 0A | 98 | 15 | 30 | 44 | A2 | C2 |
| 3 | 2C | 45 | 92 | 6C | F3 | 39 | 66 | 42 | F2 | 35 | 20 | 6F | 77 | BB | 59 | 19 |
| 4 | 1D | FE | 37 | 67 | 2D | 31 | F5 | 69 | A7 | 64 | AB | 13 | 54 | 25 | E9 | 09 |
| 5 | ED | 5C | 05 | CA | 4C | 24 | 87 | BF | 18 | 3E | 22 | F0 | 51 | EC | 61 | 17 |
| 6 | 16 | 5E | AF | D3 | 49 | A6 | 36 | 43 | F4 | 47 | 91 | DF | 33 | 93 | 21 | 3B |
| $S =$ 7 | 79 | B7 | 97 | 85 | 10 | B5 | BA | 3C | B6 | 70 | D0 | 06 | A1 | FA | 81 | 82 |
| 8 | 83 | 7E | 7F | 80 | 96 | 73 | BE | 56 | 9B | 9E | 95 | D9 | F7 | 02 | B9 | A4 |
| 9 | DE | 6A | 32 | 6D | D8 | 8A | 84 | 72 | 2A | 14 | 9F | 88 | F9 | DC | 89 | 9A |
| *A* | FB | 7C | 2E | C3 | 8F | B8 | 65 | 48 | 26 | C8 | 12 | 4A | CE | E7 | D2 | 62 |
| *B* | 0C | E0 | 1F | EF | 11 | 75 | 78 | 71 | A5 | 8E | 76 | 3D | BD | BC | 86 | 57 |
| *C* | 0B | 28 | 2F | A3 | DA | D4 | E4 | 0F | A9 | 27 | 53 | 04 | 1B | FC | AC | E6 |
| *D* | 7A | 07 | AE | 63 | C5 | DB | E2 | EA | 94 | 8B | C4 | D5 | 9D | F8 | 90 | 6B |
| *E* | B1 | 0D | D6 | EB | C6 | 0E | CF | AD | 08 | 4E | D7 | E3 | 5D | 50 | 1E | B3 |
| *F* | 5B | 23 | 38 | 34 | 68 | 46 | 03 | 8C | DD | 9C | 7D | A0 | CD | 1A | 41 | 1C |

(4)

Since the length of the S-box (4) is $N = 256$, it can be represented by eight component Boolean functions, four component 4-functions and two component 16-functions.

Consider the possible representations of the S-box (4) using the functions of many-valued logic, considering, as an example, the first of the corresponding component functions. Thus, the S-box (4) can be represented as 8 component Boolean functions $f_{2i}$, $i = 1, 2, \ldots, 8$, the first of which is given as an example

$$\begin{gathered} f_{20} = \{01101011011001110001110101101000000011101 \\ 1001000000100110001011111110111111101101111010001 \\ 1000010110011100101111111111101000000101010101001 \\ 0010111010000100000010101010011010000000100000111 \\ 1011001100110110001111010000101110001011001110 1 \\ 0011001110011100001010101010\}. \end{gathered} \tag{5}$$

The S-box (4) can also be represented as four component 4-functions $f_{4i}, i = 1, 2, ..., 4$, the first of which has the form

$$\begin{gathered} f_{40} = \{0112323103100113002313030310302222211 1 \\ 0112010022012031222103331112331111303301111012 \\ 0033022010132233122303133313133101202002121232 \\ 3023222321132102221020220301012302330102022232 2 \\ 0033110112211023303320031330300223231322030110 \\ 03112322310233102333000230101 01210\}. \end{gathered} \tag{6}$$

And also, the S-box (4) can be represented as two component 16-functions, the first of which is given as an example

$$\begin{gathered} f_{160} = \{01D6B2B18F90015744AB9B0F8FDCF0E2AEA15D8 \\ 91A850422C52C3962250F7B99DE77D15974B34599DC5AC4 \\ 7F8E201C176EF39663471F331B977505AC60061A123EF063 \\ E6BE597294EA2D8A42A4F89C9ABCE3F858682AE722C0FF \\ 15815E6DDC67B8F3A44F9734BCC6A7E35B2A4B45D80B1D \\ 6B6EFD8E73D0E3B384863CDCD0DA1C\}. \end{gathered} \tag{7}$$

Next, on the example of 4-function (6), we introduce the definition of the maximum and integral deviation from SAC for the case of component 4-functions. These indicators for all other cases of representation of cryptographic constructions by functions of many-valued logic are estimated similarly.
Using **Definition 3**, we find, for example, the derivative of the 4-function $f_{40}$ (6) in the direction of the vector $u = \{0, 0, 0, 1\}$, which has the form

$$\begin{gathered} D_{0001} f_{40} = [101231223230102102112132323012 0 \\ 1003103101210020211202101333302021102000 \\ 0130010033113030120203122010310123221022 \\ 0202011202020131331131300330233330031222 \\ 2231231131210113322001300030103101030321 \\ 2130020332011102113132303311330320112012 \\ 121013212010321103131133 1]. \end{gathered} \tag{8}$$

According to the requirements of Definition 6, in order for the S-box (4) to satisfy the error propagation criterion for vector $u = \{0, 0, 0, 1\}$, it is necessary that the number of characters "0", "1", "2" and "3" were equal to each other, i.e. $K^0 = K^1 = K^2 = K^3 = N/4 = 64$. However, this requirement is not met for the derivative (8)

$$\left\{ \begin{matrix} K^0_{D_{0001} f_{40}} & K^1_{D_{0001} Ff_{40}} & K^2_{D_{0001} Ff_{40}} & K^3_{D_{0001} Ff_{40}} \\ 69 & 73 & 55 & 59 \end{matrix} \right\}. \tag{9}$$

Find the derivative (8) deviation value from compliance with the **Definition 6** requirements**.**

$$\left\{ \frac{\Delta K^0_{D_{0001}f_{40}}}{\left|64-K^0_{D_{0001}f_{40}}\right|} \quad \frac{\Delta K^1_{D_{0001}f_{40}}}{\left|64-K^0_{D_{0001}f_{40}}\right|} \quad \frac{\Delta K^2_{D_{0001}f_{40}}}{\left|64-K^0_{D_{0001}f_{40}}\right|} \quad \frac{\Delta K^3_{D_{0001}f_{40}}}{\left|64-K^0_{D_{0001}f_{40}}\right|} \right\} = \\ = \left\{ \frac{\Delta K^0_{D_{0001}f_{40}}}{5} \quad \frac{\Delta K^1_{D_{0001}f_{40}}}{9} \quad \frac{\Delta K^2_{D_{0001}f_{40}}}{9} \quad \frac{\Delta K^3_{D_{0001}f_{40}}}{5} \right\}. \qquad (10)$$

Similarly, we can find the deviation of the derivative of the component 4-function (8) from compliance with the strict avalanche criterion in direction of each considered vector

$$\begin{array}{c|cccc}
 & & a & & \\
 & \Delta K^0_{Df_{40}} & \Delta K^1_{Df_{40}} & \Delta K^2_{Df_{40}} & \Delta K^3_{Df_{40}} \\
\Delta K_{D_{0001}f_{40}} & 5 & 9 & 9 & 5 \\
\Delta K_{D_{0010}f_{40}} & 10 & 6 & 2 & 2 \\
\Delta K_{D_{0100}f_{40}} & 2 & 9 & 4 & 7 \\
\Delta K_{D_{1000}f_{40}} & 3 & 12 & 3 & 6 \\
\Delta K_{D_{0002}f_{40}} & 0 & 2 & 4 & 2 \\
\Delta K_{D_{0020}f_{40}} & 0 & 6 & 12 & 6 \\
\Delta K_{D_{0200}f_{40}} & 14 & 6 & 2 & 6 \\
\Delta K_{D_{2000}f_{40}} & 2 & 2 & 2 & 2 \\
\Delta K_{D_{0003}f_{40}} & 5 & 5 & 9 & 9 \\
\Delta K_{D_{0030}f_{40}} & 10 & 2 & 2 & 6 \\
\Delta K_{D_{0300}f_{40}} & 2 & 7 & 4 & 9 \\
\Delta K_{D_{3000}f_{40}} & 3 & 6 & 3 & 12
\end{array} \; . \qquad (11)$$

Similarly, deviations from the strict avalanche criterion can be found for each of the component 4-functions of the S-box.

It is obvious that it is possible to estimate the degree of deviation of the component functions of the S-box from the requirements of the strict avalanche criterion in two ways, therefore, we introduce two fundamental definitions.

**Definition 7**. The maximum deviation of the S-box from the SAC when it is represented by component $q$-functions is the maximum among all deviations from the SAC of its component $q$-functions.

In our case, the overall quality of the component 4-function is determined by the largest value among the deviations (11), which is equal to $\Delta_{\max} K_{Df_{40}} = 14$, the overall quality of the S-box will be determined by the maximum among the maximum deviations of all its component functions, in our case, $\Delta_{\max} K_{Df_{4i}} = \max\{14,14,16,16\} = 16$, $i = 1,2,...,4$.

From the **Definition 7** it becomes clear that the maximum deviation of the derivative of the component function from the SAC will be $\left|q^{k-1} - q^k\right|$, that represents the difference between the number of characters $K^0, K^1, ..., K^{q-1}$ in a balanced derivative of the $q$-function of length $N = q^k$ and the number of characters $K^0, K^1, ..., K^{q-1}$ in the most unbalanced derivative of the $q$-function of length $N = q^k$. In the case of length $N = 256$ the maximum value of the maximum deviation is 128 for Boolean functions, 192 for 4-functions and 244 for 16-functions. The minimum value of the maximum deviation of the $q$-function from the SAC is 0 for the component functions of many-valued logic satisfying the SAC. In our case, for the S-box (4) the deviation from the SAC is 8.33%.

Note that the smaller value of the deviation of the component function of many-valued logic from the SAC is an indicator of its better compliance with the conditions of the SAC.

Another way to determine the degree of deviation of the component functions of many-valued logic from the requirements of the SAC is to calculate the integral deviation from the SAC.

**Definition 8.** The integral deviation of the S-box from the SAC when it is represented by the component $q$-functions is the total value of the deviations from the SAC of all its component $q$-functions.

$$\Delta K_{D_z f_{qi}} = \sum_{j=0}^{3} \Delta K^{j}_{D_z f_{qi}}, \quad i = 0,1,...,k \,. \tag{12}$$

We can calculate the integral deviation from the SAC for the derivative in the direction 0001 of the component 4-function (8) $\Delta K_{D_{0001} f_{40}} = \sum_{i=0}^{3} \Delta K^{i}_{D_{0001} f_{40}} = 5+9+9+5 = 28$.

Similarly, we can find the sum of the deviations in all directions of the unit weight of the component 4-function (6) of the S-box (4), as required by **Definition 6** of the strict avalanche criterion

$$\Delta K_{Df_{40}} = \sum_{j=1}^{12} \sum_{i=0}^{3} \Delta K^{i}_{D_j f_{40}} = 256 \,. \tag{13}$$

We can also calculate the sum of the deviations from the SAC for each of the 4 component 4-functions of the S-box

$$\Delta K_{DS_4} = \sum_{l=1}^{4} \sum_{j=1}^{12} \sum_{i=0}^{3} \Delta K^{i}_{D_j f_{4l}} = 1040 \,. \tag{14}$$

Obviously, smaller values of the integral deviation of the S-box from the requirements of the SAC is the best indicator. The maximum value of the integral deviation of the S-box from the requirements of the SAC will be determined by the product $\left|q^{k-1} - q^{k}\right| \cdot \log_q N \cdot |z|$, where $|z| = (q-1)\log_q N$ is the number of vectors of unit weight of length *k*.

In our case, for S-boxes of length $N = 256$, the maximum value of the integral deviation from the requirements of the SAC will be $\left|4^3 - 4^4\right| \cdot \log_4 256 \cdot 12 = 9216$.

For the Boolean function of the specified length, the maximum value of the integral deviation from the SAC will be 8192, and 14400 in the case of 16-functions. Therefore, the value obtained in (14) is 11.28% from the maximum value.

The minimum value of the integral deviation from the SAC is 0 and is possible for S-boxes that correspond to the SAC, which is the best characteristic of the cipher.

In this case, the maximum and integral deviation from the SAC is calculated in a similar way for the functions of many-valued logic at other values.

Similar to calculating the values of the maximum and integral deviation from the SAC of the S-box of the AES cryptoalgorithm, represented by component Boolean functions, 4-functions and 16-functions, we can find these characteristics for the cryptoalgorithms Kalyna [12], BelT [13] and Kuznechik [14] (Table 1).

Analysis of the data represented in Table 1 shows the absolute values of the maximum and integral deviation from the SAC, as well as these values as a percentage from the maximum possible values of the maximum and integral deviation from the SAC for a S-boxes of given length. Note that since the Kalyna cryptoalgorithm uses four S-boxes, the general parameters are determined by the worst of the values.

*Table 1 - Values of maximum and integral deviation from the SAC for cryptographic algorithms AES, Kalyna, BelT and Kuznechik*

| Crypto-algorithm | Binary case | | Case of 4-functions | | Case of 16-functions | |
|---|---|---|---|---|---|---|
| | $\Delta_{\max} K_{Df_{2i}}$<br>(%) | $\Delta K_{Df_{2i}}$<br>(%) | $\Delta_{\max} K_{Df_{4i}}$<br>(%) | $\Delta K_{Df_{4i}}$<br>(%) | $\Delta_{\max} K_{Df_{16i}}$<br>(%) | $\Delta K_{Df_{16i}}$<br>(%) |
| AES | 12<br>(9.38%) | 516<br>(6.25%) | 16<br>(8.33%) | 1040<br>(11.28%) | 11<br>(4.58%) | 2848<br>(19.78%) |
| Kalyna | 28<br>(21.88%) | 512<br>(6.25%) | 18<br>(9.33%) | 1064<br>(11.55%) | 15<br>(6.25%) | 3284<br>(22.81%) |
| BelT | 20<br>(15.63%) | 480<br>(5.86%) | 18<br>(9.38%) | 712<br>(7.73%) | 10<br>(4.17%) | 2096<br>(14.56%) |
| Kuznechik | 28<br>(21.88%) | 516<br>(6.3%) | 20<br>(10.42%) | 932<br>(10.11%) | 11<br>(4.58%) | 2764<br>(19.19%) |

Analysis of the data represented in Table 1 shows that for AES-like cryptoalgorithms there is a general tendency to decrease the maximum deviation from the SAC (less deviation means higher quality of the cryptoalgorithm) with increasing in the value of basis $q$ of the representation of component functions.

In Fig. 1 we show a graph of the changes in the maximum deviation from the criterion of SAC for S-boxes of the researched BSC. Obviously, a smaller maximum deviation from the SAC is means higher quality of the cryptographic transformation.

In Fig. 2 we show a graph of changes in the integral deviation from the criterion of SAC for S-boxes of researched BSC.

## 3. Conclusion

In this paper, on the basis of the error propagation criterion and the strict avalanche criterion for many-valued logic functions, the indicators of maximum and integral deviation from the strict avalanche criterion of S-boxes are introduced, which allows to estimate and compare the degree of deviation from SAC for the functions of many-valued logic. Maximum and minimum values for an arbitrary length of many-valued logic functions are found for the introduced indicators of maximum and integral deviation from SAC. A research and comparison of avalanche properties of component functions of many-valued logic of cryptoalgorithms AES (USA), Kalyna (Ukraine), Kuznechik (Russia) and BelT (Belarus) were performed, which allowed to obtain the following conclusions:

1. for the substitution constructions of the researched BSC the general tendency of decrease of the maximum deviation from SAC while increasing a basis of representation $q$ value is established. In this case, a greater decrease in the maximum deviation from the SAC indicates means higher quality of the cryptographic transformation.
2. for the substitution constructions of the researched BSC the general tendency of increase of integral deviation from SAC while increasing a basis of representation $q$ is established. Smaller values of the increase of the integral deviation from the SAC indicate a higher quality of cryptographic transformation.

Therefore, on the basis of the performed research the following recommendation can be formulated. When designing cryptoalgorithms, it is important to consider the possibility of their representation by the functions of many-valued logic.

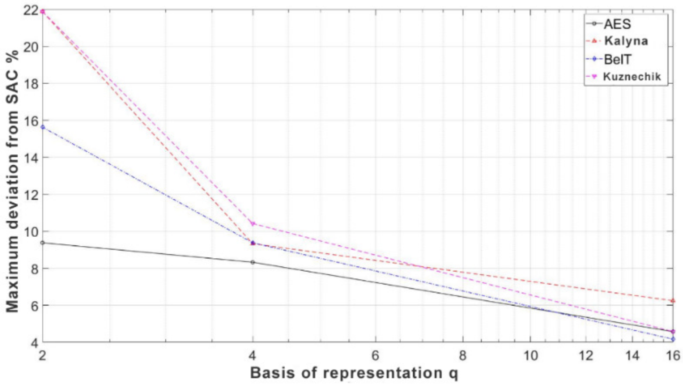

*Figure 1. The maximum deviation from the SAC for S-boxes of the researched BSC*

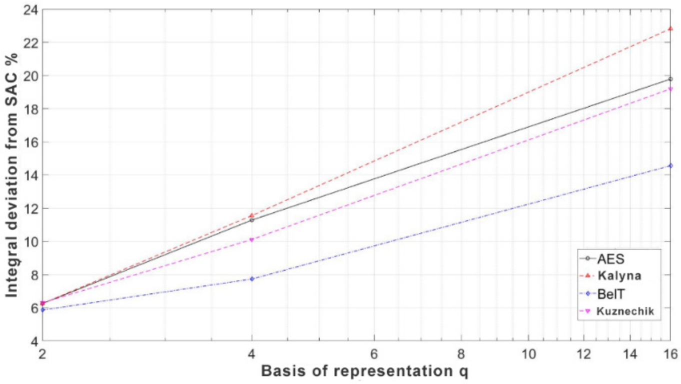

*Figure 2. Integral deviation from SAC for S-boxes of the researched BSC*

## REFERENCES

1. SHANNON C.E.: A Mathematical Theory of Cryptography / C.E. Shannon. — Bell System Technical Memo, 1945. MM 45-110-02.
2. MAIER W.: Nonlinearity criteria for cryptographic functions / W. Maier, O. Staffelbach // In Advances in Cryptology — EUROCRYPT'89, Lecture Notes in Computer Science, Springer-Verlag, 1990. Vol. 434. P. 549-562.
3. FEISTEL H.: Cryptography and Computer Privacy. Scientific American, 1973. Vol. 228, No. 5. P. 15-23.
4. GRASSL M. ET AL.: Applying Grover's algorithm to AES: quantum resource estimates. Post-Quantum Cryptography. Springer, Cham, 2016. P. 29-43.
5. BAIGNERES T.: Linear cryptanalysis of non binary ciphers / T. Baigneres, J. Stern, S. Vaudenay. International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2007. P. 184-211.
6. 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. P.183-190.
7. SOKOLOV A.V., RADUSH V.V.: Avalanche characteristics of Nyberg construction S-boxes represented by the many-valued logic functions. Informatics & Mathematical Methods in Simulation, 2019. No. 9 (3). P. 111-119.
8. SOKOLOV A.V., ZHDANOV O.N.: Cryptographic constructions based on many-valued logic functions. Monograph. M: Scientific Thought, 2020.192 p.
9. LOGACHEV O.A., SALNIKOV A.A., IASHCHENKO V.V.: Boolean functions in coding theory and cryptography. American Mathematical Soc., 2012. 241 p.
10. FIPS 197. [Electronic resource] Advanced encryption standard. 2001. http://csrc.nist.gov/publications/
11. NYBERG K.: Differentially uniform mappings for cryptography. I Advances in cryptology. Proc. of EUROCRYPT'93. Berlin, Heidelberg, New York. 1994. Vol.765, Lecture Notes in Compuer Springer-Verlag. P.55-65.
12. DSTU 7624:2014 Information technologies. Cryptographic data security. Symmetric block transformation algorithm. Ministry of Economic Development of Ukraine, 2016. 221 c.
13. STB 34.101.31-2011. Information technology and security. Information protection. Cryptographic algorithms for encryption and integrity control. Minsk. Gosstandart. 31 p.
14. GOST 34.12-2018. Information technology. Cryptographic protection of information. Block chippers. Moscow. Standartinform. 17 p.