# Correlation Immunity of Many-Valued Logic Component Functions of Modern Cryptographic Algorithm S-Boxes

Nadiia Kazakova [1], Artem Sokolov [2] and Alexander Troyanskiy [3]

[1] *Department of Information Technologies, Odessa State Environmental University, Odessa, 65016, Ukraine.*
[2] *Department of Cybersecurity and Software, Odessa National Polytechnic University, Odessa, 65044, Ukraine.*
[3] *Department of Radioelectronic and Telecommunication Systems, Odessa National Polytechnic University, Odessa, 65044, Ukraine.*

**Abstract**

The development of modern cryptanalysis methods, in particular, with the use of many-valued logic functions, leads to the need for a more detailed research of the correlation properties of S-boxes of modern cryptographic algorithms. In this paper, we introduce indicators for the maximum and integral deviation of a many-valued logic functions on the basis of criterion for the independence of its output from the input variables. These indicators are a convenient tool for comparative analysis of the correlation properties of S-boxes of various lengths when they are represented using the many-valued logic functions with different bases $q$. The research and comparative analysis of the S-boxes of the AES and Kalyna cryptographic algorithms was performed, which showed a general tendency of a decreasing of their correlation properties with an increase in the value of representation base $q$, and also made it possible to establish that for all values of the representation base $q$, the correlation properties of the Kalyna cryptographic algorithm S-box are weaker than the correlation properties of the AES cryptographic algorithm S-box.

**Keywords**

Cryptography, many-valued logic function, correlation immunity.

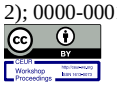


## 1. Introduction and problem statement

Block symmetric ciphers are one of the most important components of modern cybersecurity systems, the task of which is to make it impossible to access transmitted or stored information without knowing the key. Nevertheless, the rapid increase in the computing power of modern information systems, development of the mathematical methods of cryptanalysis, as well as the prospects for the creation of quantum computers lead to the need for continuous improvement of the structure and components of modern block symmetric ciphers.

The issues of improving modern cryptographic algorithms are inextricably linked with the theory of estimation of their cryptographic quality. The modern theory of estimation of the cryptographic quality of block symmetric ciphers involves the representation of their constituent parts (first of all, S-boxes) using component Boolean functions [1, 2]. Further, cryptographic quality criteria are applied to the obtained Boolean functions, each of which reflects the ability of the Boolean function to resist one or another cryptanalysis attack, as well as to provide a sufficient level of diffusion and confusion [3].

However, publications in the field of cryptography [4] show an increasing need to research all possible representations of S-boxes,

*ISIT 2021: II International Scientific and Practical Conference «Intellectual Systems and Information Technologies», September 13–19, 2021, Odesa, Ukraine*
EMAIL: kaz2003@ukr.net (A. 1); radiosquid@gmail.com (A. 2); alex_troy@ukr.net (A. 3)
ORCID: 0000-0003-3968-4094 (A. 1); 0000-0003-0283-7229 (A. 2); 0000-0001-9755-6010 (A. 3)


in particular, using functions of many-valued logic. Research [5] is devoted to the method of estimation of the nonlinearity, as well as avalanche characteristics of S-boxes of modern cryptographic algorithms, represented by functions of many-valued logic.

Nevertheless, the results of the analysis of the correspondence of the constructions of modern cryptographic algorithms to the criterion of correlation immunity of functions of many-valued logic are not presented in the open sources.

The *purpose* of this paper is to perform a comparative analysis of the correlation immunity of the cryptographic algorithms AES (USA) and Kalyna (Ukraine) when they are represented by the many-valued logic functions.

## 2. Correlation immunity of many-valued logic functions

The definition of the correlation immunity of Boolean functions is widely known [6], which can be specified through the definition of a subfunction of a Boolean function.

**Definition 1 [6].** A Boolean function $f(x)$, $x \in V_k$, is called as correlation-immune of order $m$, $1 \le m \le k$ if its output $y = f(x_1^k)$ and any set of $m$ its input variables are statistically independent.

**Definition 2 [6].** A subfunction of a Boolean function $f(x)$, $x \in V_k$, is a function $f'$ obtained by substitution in $f$ constants "0" or "1" instead of a part of 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 $f_{x_{i_1},\cdots,x_{i_s}}^{\sigma_{i_1},\cdots,\sigma_{i_s}}$. If a constant is not substituted for a variable $x_i$, then $x_i$ 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 [6].** Boolean function $f(x)$, $x \in V_k$, is called correlation-immune of order $m$, $1 \le m \le k$ if weight is equal to $wt(f') = wt(f)/2^m$, for any of its subfunctions $f'$ of $k - m$ variables.

In [7], the theoretical foundations for estimating the correlation immunity of functions of many-valued logic were developed, while in [8], definitions of the independence of the output of a 3-function from its input variables, as well as the definition of the correlation immunity of a 3-function were introduced. The basis of these definitions is the definition of the imbalance of functions of many-valued logic.

Consider an arbitrary sequence over the alphabet $\{0,1,...,q-1\}$

$$f_i \in \{0,1,...,q-1\}, \quad i = 0,1,...,N-1. \qquad (1)$$

Note that the elements of a given sequence (1) can be represented in exponential form by an unambiguous transformation

$$0 \leftrightarrow z_0 = e^{j\frac{2\pi}{q}0}, 1 \leftrightarrow z_1 = e^{j\frac{2\pi}{q}1}, ..., q-1 \leftrightarrow z_{q-1} = e^{j\frac{2\pi}{q}(q-1)}. \qquad (2)$$

For a given sequence (1), it is possible to introduce a vector $K = \{K_0, K_1, ..., K_{q-1}\}$, where the coefficients $K_u$ characterize 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 $\{z_0, z_1, ..., z_{q-1}\}$

$$\Delta(f) = \left| K_0 z_0 + K_1 z_1 + ... + K_{q-1} z_{q-1} \right|. \qquad (3)$$

The definitions of the independence of the output of a 3-function from its input variables, as well as the definition of the correlation immunity of a 3-function, introduced in [8] using **Definition 4** of the imbalance of a many-valued logic function can be generalized to the case of *q*-functions for an arbitrary value of *q*.

**Definition 5 [8].** It is said that the output of a *q*-function $f(x)$ does not depend on 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 this way is $\Delta(f') = \frac{\Delta_f}{q^m}$.

Note, however, that the correlation immunity of component Boolean functions, as well as component many-valued logic functions, is a rather stringent requirement that is not met for most S-boxes used in practice. This circumstance

poses the task of developing a mathematical apparatus for performing a comparative analysis of the degree of correspondence of S-boxes to the correlation immunity criterion of component *q*-functions.

The **Definition 5** gives us the possibility to estimate the degree of deviation of the many-valued logic functions and S-boxes from the criterion of correlation immunity by introducing two basic indicators of cryptographic quality: the maximum and integral deviation from the criterion of independence of the output of many-valued logic functions from their input.

Let's consider these indicators on a specific example, and then apply them to specific cryptographic algorithms.

Let an S-box of length $N=16$ be given, which can be represented in the form of four component Boolean functions, as well as in the form of two component 4-functions.

| $S$ | 12 | 0 | 2 | 14 | 13 | 11 | 3 | 5 | 1 | 7 | 15 | 9 | 10 | 6 | 4 | 8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_{20}$ | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| $f_{21}$ | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| $f_{22}$ | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| $f_{23}$ | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| $f_{40}$ | 0 | 0 | 2 | 2 | 1 | 3 | 3 | 1 | 1 | 3 | 3 | 1 | 2 | 2 | 0 | 0 |
| $f_{41}$ | 3 | 0 | 0 | 3 | 3 | 2 | 0 | 1 | 0 | 1 | 3 | 2 | 2 | 1 | 1 | 2 |

(4)

We begin our research with the first component Boolean function $f_{20}$, for which, in accordance with **Definition 3**, we find all its subfunctions of three variables

$$\begin{aligned}
&wt(f_{20}(x_1,x_2,x_3,0)=[00111100])=4;\\
&wt(f_{20}(x_1,x_2,0,x_4)=[00111100])=4;\\
&wt(f_{20}(x_1,0,x_3,x_4)=[00001111])=4;\\
&wt(f_{20}(0,x_2,x_3,x_4)=[00001111])=4;\\
&wt(f_{20}(x_1,x_2,x_3,1)=[00111100])=4;\\
&wt(f_{20}(x_1,x_2,1,x_4)=[00111100])=4;\\
&wt(f_{20}(x_1,1,x_3,x_4)=[11110000])=4;\\
&wt(f_{20}(1,x_2,x_3,x_4)=[11110000])=4.
\end{aligned} \tag{5}$$

Since the weight of each of the subfunctions (5) is equal to 4, i.e. they are balanced, the first component Boolean function $f_{20}$ (4) corresponds to the criterion of correlation immunity. It is possible to verify that all other component Boolean functions of the S-box (4) also corresponds to the criterion of correlation immunity.

Consider the S-box (4) from the point of view of its possible representation by component 4-functions. Let us find the subfunctions of the component 4-function $f_{40}$ of the S-box (4)

$$\begin{aligned}
&\Delta(f_{40}(x_1,0)=[0112])=2;\\
&\Delta(f_{40}(x_1,1)=[0332])=2;\\
&\Delta(f_{40}(x_1,2)=[2330])=2;\\
&\Delta(f_{40}(x_1,3)=[2110])=2;\\
&\Delta(f_{40}(0,x_2)=[0022])=0;\\
&\Delta(f_{40}(1,x_2)=[1331])=0;\\
&\Delta(f_{40}(2,x_2)=[1331])=0;\\
&\Delta(f_{40}(3,x_2)=[2200])=0.
\end{aligned} \tag{6}$$

In a similar way, we can find subfunctions for the component function $f_{41}$ of the S-box (4)

$$\begin{aligned}
&\Delta(f_{41}(x_1,0)=[3302])=2;\\
&\Delta(f_{41}(x_1,1)=[0211])=2;\\
&\Delta(f_{41}(x_1,2)=[0031])=2;\\
&\Delta(f_{41}(x_1,3)=[3122])=2;\\
&\Delta(f_{41}(0,x_2)=[3003])=\sqrt{8};\\
&\Delta(f_{41}(1,x_2)=[3201])=0;\\
&\Delta(f_{41}(2,x_2)=[0132])=0;\\
&\Delta(f_{41}(3,x_2)=[2112])=\sqrt{8}.
\end{aligned} \tag{7}$$

Analysis of expressions (6) and (7) shows that not all subfunctions of the component 4-function $f_{40}$, as well as subfunctions of the component function $f_{41}$, are balanced, which means that the S-box (4) does not correspond to the criterion of correlation immunity of component 4-functions.

To solve the problem of quantitative estimating of the compliance of the S-box with the criterion of correlation immunity, we introduce the indicators of the maximum and integral deviation from the compliance with the criterion of the independence of the S-box output from its input variables.

**Definition 6.** The maximum deviation of an S-box from the criterion of independence of the output from the input variables when it is represented by component *q*-functions is the maximum among all deviations from the criterion of independence of the output from the input variables of its component *q*-functions.

In our case, the S-box (4) corresponds to the criterion of correlation immunity of component Boolean functions, therefore, its maximum deviation from the criterion of independence of the output from the input variables when it is represented by component Boolean functions is equal to $\Lambda_{\max} f_{2i}=0$.

In the case of representation by component 4-functions, the maximum deviation from the criterion for the independence of the output from the input variables is $\Lambda_{\max} f_{4i} = \sqrt{8} = 2.8284$.

It is obvious that the maximum possible value of the maximum deviation of the *q*-function from the criterion of the independence of the output from the input variables is the maximum value of the imbalance of the *q*-function of $k-1$ variables, that is $\max\{\Lambda_{\max} f_{qi}\} = N/q$. In the case of representing an S-box of length $N=16$ using component 4-functions the maximum value of the maximum deviation from the criterion of independence of the output from the input variables would reach $\max\{\Lambda_{\max} f_{4i}\} = 16/4 = 4$. I.e. the maximum deviation from the criterion of independence of the output from the input variables among the component functions for our S-box (4) is 70.71% of its maximum value.

**Definition 7.** The integral deviation of the S-box from the criterion of independence of the output from the input variables when it is represented by component *q*-functions is the total value of all deviations from the criterion of independence of the output from the input variables of its component *q*-functions

$$\Lambda f_{qi} = \sum_{i=0}^{k} \Delta f_{qi} \,. \qquad (8)$$

In our example, in view of the compliance of the S-box (4) with the criterion of correlation immunity of component Boolean functions, its integral deviation from the criterion of the independence of the output from the input variables is equal to $\Lambda f_{2i} = 0$.

In the case of representation using component 4-functions, and using (8), we obtain that the integral deviation of the S-box (4) from the criterion for the independence of the output from the input variables is $\Lambda f_{q0} = 8$ for the first component 4-function and $\Lambda f_{q1} = 13.6569$ for the second component 4-function.

It is obvious that the maximum value of the integral deviation of the *q*-function from the criterion for the independence of the output from the input variables is

$$\max\{\Lambda f_{qi}\} = q^{k-1} z \,, \qquad (9)$$

where $z$ is the number of subfunctions of the *q*-function.

In our case, the maximum value of the integral deviation of the *q*-function from the criterion of the independence of the output from the input variables is $\max\{\Lambda f_{4i}\} = 4 \cdot 8 = 32$, i.e. the 4-function $f_{40}$ is characterized by the integral deviation from the criterion of the independence of the output from the input variables equal to 25% of the maximum value, while for the component function $f_{41}$ this indicator is 42.68%.

Note also that since the S-box (4) consists of two component 4-functions, the total value of the integral deviation for the two component 4-functions is equal to $\Lambda f_{q0} + \Lambda f_{q1} = 21.6569$, which is 33.84% of the maximum value equal to $\max\{\Lambda S_4\} = 64$.

Note also that for the cryptographic algorithms AES and Kalyna which are researched in this paper, the length of the S-boxes used is $N = 256$, respectively, the maximum value of the maximum deviation of the Boolean function from the criterion for the independence of the output from the input variables is $\max\{\Lambda_{\max} f_{2i}\} = 256/2 = 128$, while the maximum value of the maximum deviation of the 4-functions from the criterion for the independence of the output from the input variables is $\max\{\Lambda_{\max} f_{4i}\} = 256/4 = 64$.

In this case, the maximum value of the maximum deviation of the 16-function from the criterion for the independence of the output from the input variables is $\max\{\Lambda_{\max} f_{16i}\} = 256/16 = 16.$

The maximum value of the integral deviation of the Boolean function from the criterion for the independence of the output from the input variables is $\max\{\Lambda f_{2i}\} = 128 \cdot 16 = 2048$, while this indicator for the entire S-box will be $\max\{\Lambda S_2\} = 8 \cdot 2048 = 16384$.

The maximum value of the integral deviation of the 4-function from the criterion for the independence of the output from the input variables is $\max\{\Lambda f_{4i}\} = 64 \cdot 16 = 1024$, while this indicator for the entire S-box will be $\max\{\Lambda S_4\} = 4 \cdot 1024 = 4096$.

The maximum value of the integral deviation of the 16-function from the criterion for the independence of the output from the input variables is $\max\{\Lambda f_{16i}\} = 16 \cdot 32 = 512$, while this indicator for the entire S-box will be $\max\{\Lambda S_{16}\} = 2 \cdot 512 = 1024$.

## 3. Indicators of deviation from the criterion of correlation immunity of S-boxes of modern ciphers

In this paper, we research the deviation from the criterion of correlation immunity of S-boxes of cryptographic algorithms AES (USA) [9], as well as Kalyna (Ukraine) [10].

The cryptographic algorithm AES is based on a Nyberg construction S-box [11], which is defined using a mapping in the form of multiplicatively inverse elements of the Galois field $GF(2^k)$

$$y = x^{-1} \bmod d[f(z), p], \quad y, x \in GF(2^k), \qquad (10)$$

which is generally combined with the affine transformation

$$b = A \cdot y + a, \quad a, b \in GF(2^k), \qquad (11)$$

where the standard AES irreducible over the field $GF(2^8)$ polynomial is used as a polynomial $f(z)$,

$A$ is a non-singular affine transformation matrix,

$a$ is a the shift vector,

$p = 2$ is the characteristic of the extended Galois field, $k = 8$, and $0^{-1} \equiv 0$,

$a, b, x, y$ are the elements of the extended Galois field $GF(2^k)$, which are considered as decimal numbers, or binary vectors, or polynomials of degree $k - 1$.

In this paper, we consider the AES S-box of the Nyberg construction without using the affine transformation (11), as well as with its application.

The indicators of the maximum and integral deviation from the criterion of independence of the output vectors from the input variables for the AES cryptographic algorithm are presented in Table 1.

**Table 1**

Maximum and integral deviation from the criterion of independence of the output vectors from the input variables of the S-box of the AES cipher

| S-box | Boolean representation | | Representation by the 4-functions | | Representation by the 16-functions | |
|---|---|---|---|---|---|---|
| | $\Lambda_{\max} f_{2i}$, (%) | $\Lambda f_{2i}$, (%) | $\Lambda_{\max} f_{4i}$, (%) | $\Lambda f_{4i}$, (%) | $\Lambda_{\max} f_{16i}$, (%) | $\Lambda f_{16i}$, (%) |
| AES without affine transformation | 16, (12.5%) | 924, (5.64%) | 11.402, (17.82%) | 440.7, (10.76%) | 8.676, (54.23%) | 237.272, (23.17%) |
| AES with affine transformation | 16, (12.5%) | 892, (5.44%) | 14.7648, (23.07%) | 383.1386, (9.35%) | 7.4542, (46.59%) | 214.5931, (20.95%) |

Analysis of the data presented in Table 1 shows a tendency towards an increase in both the maximum and integral deviation from the criterion of independence of the output vectors from the input variables of the AES cipher with an increase in the representation base $q$. At the same time, the use of an affine transformation insignificantly reduces the growth of this value (except for the maximum deviation from the criterion of independence of the output vectors from the input variables of 4-functions), but the deviation even in this case is quite strong.

Ukraine has developed its own block symmetric cryptographic algorithm Kalyna, which was adopted as the standard DSTU 7624: 2014 “Information technologies. Cryptographic data security. Symmetric block transformation algorithm” [12].

Today, there are several options for the implementation of the Kalyna cryptographic algorithm, which differ in the key length: Kalyna-128, Kalyna-256 and Kalyna-512. However, they all use the same cryptographic primitives on which the cryptographic quality of the cryptographic algorithm relies.

The Kalyna block symmetric cipher is characterized by the use of an SP-network and thus has an AES-like structure. The basis of the Kalyna cryptographic transformation is its nonlinear elements, which are four permutations specified in [12].

The indicators of the maximum and integral deviations from the criterion for the independence of the output vectors from the input variables for the permutations $\pi_0, \pi_1, \pi_2, \pi_3$ are presented in Table 2.

Note at the same time that in view of the fact that the overall quality of the cipher is determined by the weakest of its constituent elements [1], in order to demonstrate the overall quality of the Kalyna cryptographic algorithm, the smallest values of the maximum and integral deviations from the criterion for independence of the output from the input vectors are selected in the last row of Table 2.

**Table 2**

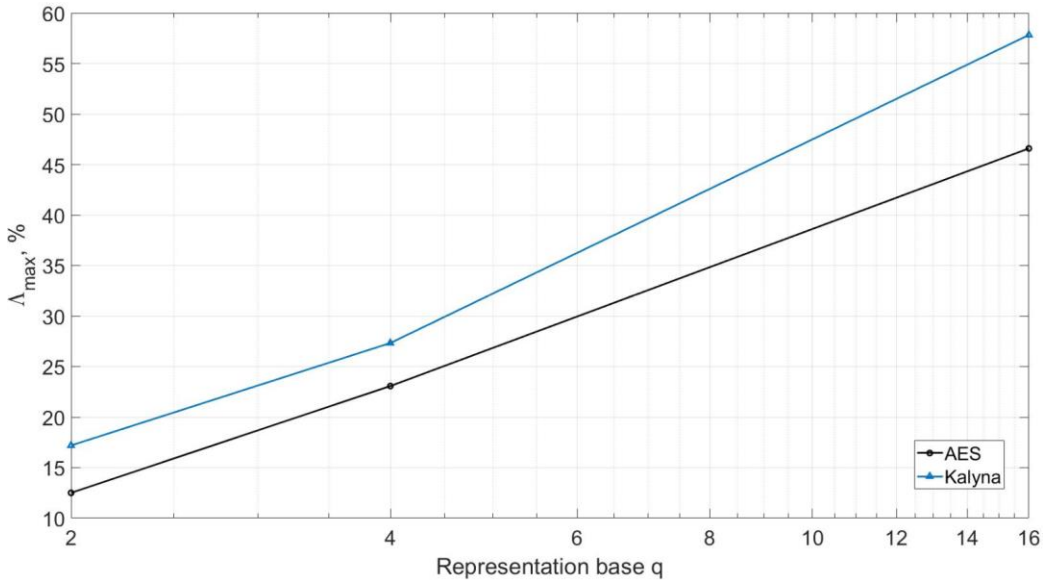
Maximum and integral deviation from the criterion for independence of the output vectors from the input variables of the Kalyna cipher S-box

| S-box | Boolean representation | | Representation by the 4-functions | | Representation by the 16-functions | |
|---|---|---|---|---|---|---|
| | $\Lambda_{\max} f_{2i}$, (%) | $\Lambda f_{2i}$, (%) | $\Lambda_{\max} f_{4i}$, (%) | $\Lambda f_{4i}$, (%) | $\Lambda_{\max} f_{16i}$, (%) | $\Lambda f_{16i}$, (%) |
| $\pi_0$ | 20, (15.63%) | 880, (5.37%) | 15.232, (23.8%) | 387.491, (9.46%) | 9.251, (57.82) | 238.613, (23.3%) |
| $\pi_1$ | 22, (17.19%) | 820, (5.01%) | 15.033, (23.49%) | 358.180, (8.74%) | 8.958, (55.99) | 212.275, (20.73%) |
| $\pi_2$ | 20, (15.63%) | 852, (5.2%) | 14.213, (22.21%) | 402.545, (9.83%) | 8.237, (51.48%) | 221.404, (21.62%) |
| $\pi_3$ | 20, (15.63%) | 964, (5.88%) | 17.493, (27.33%) | 454.290, (11.09%) | 8.246, (51.54%) | 241.167, (23.55%) |
| Overall cipher quality | 22, (17.19%) | 964, (5.88%) | 17.493, (27.33%) | 454.290, (11.09%) | 9.251, (57.82) | 241.167, (23.55%) |

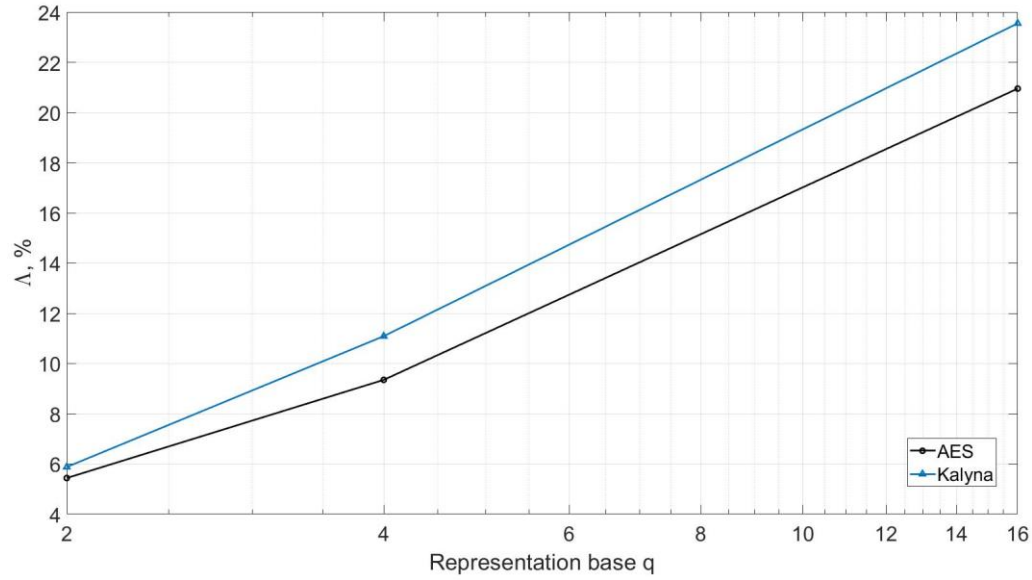
Analysis of the data presented in Table 2 shows a steady increase in both the maximum and integral deviation from the criterion for independence of the output vectors from the input variables of the S-boxes of the Kalyna cipher with an increase in the representation base *q*.

For the convenience of comparing the correlation properties of the AES cipher S-box (with affine transformation) and the Kalyna cipher S-box the Fig. 1 shows the graphs of changes in the maximum (a) and integral (b) deviation from the criterion of independence of the output vectors from the input variables for these cryptographic algorithms.

Analysis of the data presented in Fig. 1 shows that both the maximum and integral deviation of the S-boxes of the AES and Kalyna cryptographic algorithms from the criterion for the independence of the output vectors from the input variables show an increase with an increase in the representation base *q*. At the same time, the Kalyna cryptographic algorithm has a significantly higher level of the maximum and integral deviation from the criterion for the independence of the output vectors from the input variables.




a)




b)

**Figure 1**: Graphs of changes in the maximum and integral deviation from the criterion for independence of the output vectors from the input variables of the ciphers AES and Kalyna

## 4. Conclusions

1. The development of cryptanalysis methods necessitates a more detailed research of the structure of modern cryptographic algorithms, not only when they are represented by Boolean functions, but also when they are represented by functions of many-valued logic. In this paper, on the basis of the criterion for the independence of the output of many-valued logic functions from their input variables, the indicators of the maximum and integral deviation from the criterion for the independence of the output of many-valued logic functions from their input variables are introduced. For these indicators, the maximum possible values for the given $N$ and $q$ are obtained. These indicators are applicable to individual functions of many-valued logic, as well as to S-boxes of various lengths with all their possible representations, and allow a comparative analysis of the correlation properties of S-boxes of modern cryptographic algorithms when they are represented by functions of many-valued logic.

2. The analysis of S-boxes of modern cryptographic algorithms AES and Kalyna was

performed, which showed that S-boxes of both ciphers demonstrate a decrease in correlation properties with an increase in the representation base *q*. At the same time, for all values of the representation base *q*, the correlation properties of the Kalyna cryptographic algorithm are weaker than the correlation properties of the S-box of the AES cryptographic algorithm.

3. Research shows the possibilities for further improvement of the nonlinear transformation of the Ukrainian cryptographic algorithm Kalyna due to its representation by functions of many-valued logic, in conjunction with the fact that the DSTU 7624: 2014 standard allows the use of other, more advanced nonlinear elements, increases the relevance of the development of new cryptographic constructions, which are optimal from the point of view of criteria for the cryptographic quality of functions of many-valued logic.

## 5. References


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

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

[3] C.E. Shannon, A Mathematical Theory of Cryptography, Bell System Technical Memo, 1945, MM 45-110-02.

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

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

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

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

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

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

[10] I. D. Gorbenko, R.V. Olyynikov, O.V. Kazimirov et al., Symmetric block cipher Kalyna is a new national standard of Ukraine, Radio engineering, 2015, (181), pp. 5-22.

[11] K. Nyberg, Differentially uniform mappings for cryptography, I Advances in cryptology, Proc. of EUROCRYPT'93. Berlin, Heidelberg, New York, Lecture Notes in Compuer Science, Springer-Verlag, vol. 765, pp. 55-65, 1994. doi:10.1007/3-540-48285-7_6

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