DOI: 10.37943/12DZLQ4553

Ardabek Khompysh
Institute of information and Computational Technologies
ardabek@mail.ru, orcid.org/0000-0002-0702-9346
Al-Farabi Kazakh National University, Kazakhstan

Nursulu Kapalova
Institute of information and Computational Technologies
nkapalova@mail.ru, orcid.org/0000-0001-9743-9981
Al-Farabi Kazakh National University, Kazakhstan

Kunbolat Algazy
Institute of Information and Computational Technologies
kunbolat@mail.ru, orcid.org/0000-0003-3670-2170
Al-Farabi Kazakh National University, Kazakhstan

Kairat Sakan
Institute of information and Computational Technologies
kairat_sks@mail.ru, orcid.org/0000-0002-6812-6000
Al-Farabi Kazakh National University, Kazakhstan

STUDY OF THE CRYPTOGRAPHIC STRENGTH OF THE S-BOX OBTAINED ON THE BASIS OF EXPONENTIATION MODULO

Abstract. This article presents one of the main transformations of symmetric block ciphers used to protect confidential information, a new method for obtaining a non-linear S block, and an analysis of the results obtained. The S-box obtained by this method can be used as a non-linear transformation in block cipher algorithms to protect confidential data transmitted over an open channel. In most well-known works in the field of analysis and synthesis of modern block symmetric ciphers, S-box is used as a mathematical apparatus for cryptographic Boolean functions. In this case, each S-box is represented by a set of composite Boolean functions whose properties characterize the efficiency of the nonlinear substitution node.

Substitution nodes for modern symmetric primitives, including key unfolding functions, are usually implemented as replacement tables. Considering that in most modern block symmetric ciphers for introducing round keys, the encryption algorithm uses a linear operation (bitwise addition modulo 2), S-blocks are the only elements responsible for the cryptographic stability of block encryption algorithms. The required number of rounds of block symmetric ciphers is selected taking into account the results of the cryptographic analysis performed, provided that the properties of S-boxes are specified. As the main criteria and performance indicators, the balance and nonlinearity of composite Boolean functions are used; strict avalanche criterion (SAC), propagation criterion; algebraic degree; the value of the autocorrelation function. In this article, a study was made of the nonlinearity and strict avalanche criterion (SAC) of the S-box used in the block symmetric encryption algorithm. The results of the study were compared with the S-boxes of modern cryptographic algorithms and showed good results.

Keywords: S-box, nonlinearity, strict avalanche criterion, AL03, Hamming distance.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022

Introduction

Modern symmetric block ciphers are among the most effective and widespread cryptographic algorithms that are easily implemented at the software and hardware level and have high encryption speed and cryptographic strength. The structure of modern block ciphers is built on the principles of C. Shannon, i.e. a nonlinear transformation is used for confusion and a linear transformation for diffusion.

To increase the cryptographic strength of an encryption algorithm, good confusion and diffusion are necessary. In modern block cipher algorithms (AES, Kuznyechik, Kalyna, BelT), the applied substitution S-boxes are used as nonlinear transformations.

The S-box (substitution box) is a nonlinear transformation used in most modern block ciphers. The creation of a high-quality S-box is considered the most difficult aspect of block encryption, and therefore, significant efforts of cryptographers are directed to studying the properties of the S-box and obtaining an S-box substitution table with high cryptographic performance [1].

There are many competing ways to obtain S-boxes, such as random selection, selection by sequential testing, manual development, mathematical development, etc.

Recently, most of the works related to S-boxes are based on affine and fractional-linear transformations [2]. In both cases, there are some restrictions on the coefficients of affine and fractional-linear transformations[3]. Also, for chaotic mappings with the property of diffusion. These studies present methods for constructing s-boxes with better performance criteria for all classes of chaotic systems. It was shown that the proposed method makes it possible to obtain a very good s-block for all classes of chaotic systems. The results of the analysis are presented in the article in full [4,5], permutations at the inputs of the S-box and the binary Gray code are used [6]. In these works, the P-Box algorithm was developed using the properties of Gray code for secure real-time transmission of large amounts of data. The efficiency of the algorithm is optimized for operations with n bit integers, which in turn allows direct implementation on almost any hardware platform and avoids rounding errors.

The aim of this work is to obtain a constraint-free scheme for generating a large number of strongly nonlinear S-boxes with the diffusion property. The works of Yasir N, Tariq Sh, Dawood Sh, Sadam H. showed that it is possible to construct a large number of strongly nonlinear substitution permutation boxes (S-p-boxes) [7].

Farwe et al. [8] proposed a simple and practical algorithm for creating S-boxes based on the linear fractional transformation (LFT). LFT is a fractional linear transformation that helps to create S-boxes with high cryptographic strength. Authors generated S-boxes based on LFT and analyzed with SAC, BIG, NL, LP, DP etc. As a result, the resulting S-boxes showed high resistance to cryptographic analysis. Moreover, the authors [9,10] proposed efficient algorithms optimized for generating high-quality S-boxes based on the projection algorithm. The projection algorithm is a general linear group in the Galois field. According to the data presented in the article, it can be seen that the proposed S-boxes show good results compared to other existing S-boxes [11].

But here, among the methods and approaches for making S-boxes, static S-boxes are given special attention. It should be noted that such static S-boxes have disadvantages and weaknesses. The ability of attackers to access the original plaintext during cryptanalysis of the ciphertext obtained using these S-boxes directly depends on the strength of the S-boxes. Because the S-boxes proposed by some authors are dynamic. These S-boxes are used as keys [12].

An important role is now played by the development of simple and efficient methods for creating static S-boxes. This article presents a new algorithm for generating efficient static S-boxes for symmetric block ciphers.

DOI: 10.37943/12DZLQ4553

The developed S-box must meet the following criteria:

- S-block should increase the cryptographic strength of the symmetric block cipher and resistance to cryptanalysis;
- S-block should be easy to create;
- The S-block must meet the requirements of SAC, BIC, NL, LP, DP, etc.

Within the framework of the project "Development of a means of cryptographic information protection for secure negotiations over HF radio" of the Ministry of Education and Science of Kazakhstan, the AL03 encryption algorithm was developed [13]. Currently, the analysis of the cryptographic strength of the AL03 algorithm is being carried out. In this regard, a comprehensive study of the S-box, which is one of the transformations of this algorithm, is considered one of the most important tasks. The method for obtaining the S-box used in the AL03 encryption algorithm is described in [14].

1. Method for obtaining the S-box

Let's consider a way to obtain an S-box consisting of three steps. At the first, an irreducible polynomial is chosen that step generates a multiplicative group in the Galois field $GF(2^8)$ and an irreducible polynomial is called a base [14]. The selected polynomial is exponentiated modulo $\mathrm{P}(x)$:

$$Sbox_i(x) = F(x)^i mod P(x)\ i = \overline{0{,}255}, \tag{1}$$

Where $\mathrm{M}(x)$ is an irreducible polynomial called a base, $\mathrm{P}(x)$ is a module.

At the second step, we consider the coefficients of the polynomial $Sbox_i(x)$ as a vector of length 8, i.e. $Sbox_i{}' = (s'_7, s'_6, s'_5, s'_4, s'_3, s'_2, s'_1, s'_0)\ \ s'_j \in \{0,1\}\ j = \overline{7{,}0}$, if $Sbox_i{}'(x) = s'_7x^7 + s'_6x^6 + s'_5x^5 + s'_4x^4 + s'_3x^3 + s'_2x^2 + s'_1x + s'_0$. Then $Sbox_i$ is added modulo $2(XOR)$ with a fixed vector $B(x)$:

$$Sbox_i{}' = Sbox_i \oplus B \tag{2}$$

In the third step, we multiply by the matrix M $(Sbox''_i = M \times Sbox_i{}')$:

$$\begin{bmatrix} s''_0 \\ s''_1 \\ s''_2 \\ s''_3 \\ s''_4 \\ s''_5 \\ s''_6 \\ s''_7 \end{bmatrix} = \begin{bmatrix} 1\,1\,0\,1\,1\,1\,1\,1 \\ 1\,1\,1\,0\,1\,1\,1\,1 \\ 1\,1\,1\,1\,0\,1\,1\,1 \\ 1\,1\,1\,1\,1\,0\,1\,1 \\ 1\,1\,1\,1\,1\,1\,0\,1 \\ 1\,1\,1\,1\,1\,1\,1\,0 \\ 0\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,1\,1\,1\,1\,1\,1 \end{bmatrix} \mathrm{x} \begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \\ s'_4 \\ s'_5 \\ s'_6 \\ s'_7 \end{bmatrix} \tag{3}$$

Table 1 shows the values obtained after converting the binary result obtained by formula (3) to the hexadecimal number system.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022

Table 1. S-box used in the AL03 encryption algorithm

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

2. Algebraic analysis and simulation result

To assess the quality of the developed S-box, we used the standard algebraic analysis. This analysis includes the bit independence test, nonlinearity, strict avalanche test, and the probability of linear and differential approximation. The proposed S-box was also compared with some classical S-boxes and currently constructed S-boxes [7]. The proposed S-box corresponds to all the optimal values of the standard algebraic analysis. The details of this analysis are shown below.

2.1. Nonlinearity

According to [14], the degree of nonlinearity of Boolean functions $NL(f)$ is defined as the minimum Hamming distance between the i-th Boolean function and linear functions.

Degree of non-linearity $NL(f)$ is determined using the W.Hadamard transform.

The Walsh Hadamard transform of the function $f \in P_2(n)$ where $P_2(n)$ is the set of all Boolean functions of n variables, is the function $W(n)$: $V_n \to Z$ where for each $a \in V_n$:

$$W(n) = \sum_{x \epsilon V_n} (-1)^{f(x) \oplus (a,x)} \quad (5)$$

Values $W(n)$ are called transformation coefficients Walsh Hadamard.

The degree of nonlinearity of Boolean functions $NL(f)$, where $f \in P_2(n)$ is an S-box, is defined as: [15]:

$$NL(f) = \frac{1}{2} \cdot (2^n - \max(|W(\omega))|). \quad (6)$$

Table 2 shows the comparative characteristics of the S-boxes of block symmetric ciphers AES, SM4, Ref [4], Ref [15], and the proposed S-box.

The graphical representation is shown in Figure 2. The nonlinearity of the proposed S-box is 100 (see Table 2). This value is higher than Ref [4] and Ref [15].

DOI: 10.37943/12DZLQ4553

Table 2. Results of the analysis of the nonlinearity of the constituent functions of various S-boxes

S -boxes	AES	SM 4	Proposed S box	Ref [4]	Ref [15]
f_0	112	112	104	106	108
f_1	112	112	110	106	104
f_2	112	112	106	106	106
f_3	112	112	108	104	106
f_4	112	112	108	108	102
f_5	112	112	104	102	98
f_6	112	112	104	106	104
f_7	112	112	100	104	104
Average	**112**	**112**	**105.5**	**105.25**	**104**

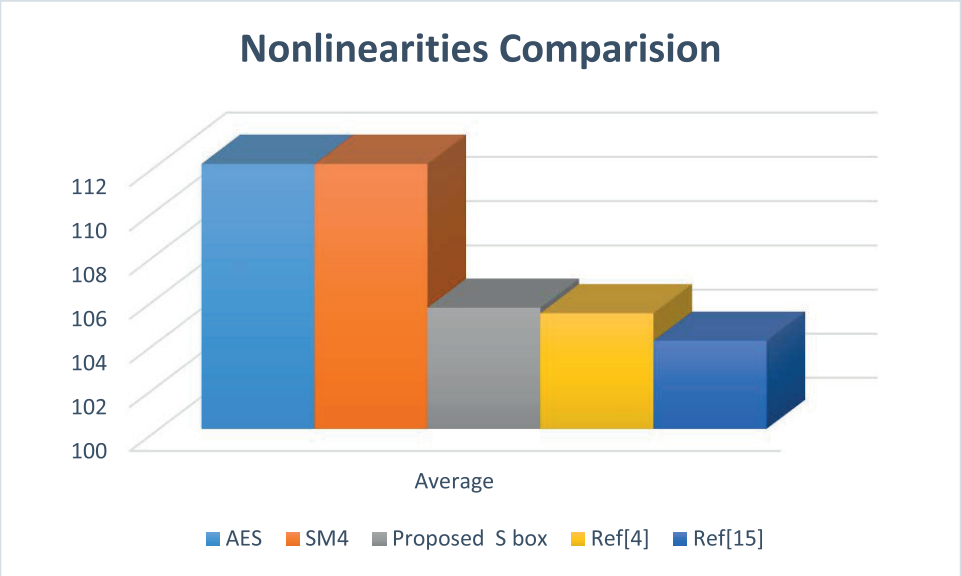

Figure 1. Graphical Representation of Nonlinearities

2.2. Strict Avalanche Criterion

A Boolean function $f(x)$ satisfies the strict avalanche criterion (SAC) if the system of equations holds for all s [16]:

$$\begin{cases} hw(s) = 1 \\ \sum_{x=0}^{2^n-1}\left(f(x)\oplus f(x\oplus s)\right) = 2^{n-1}. \end{cases} \quad (7)$$

The Strict Avalanche Criterion (SAC) determines how much the output bits change when the input bits change once. An S-box satisfies the SAC criterion if a single bit change in the input bit causes about half of the output bits to change [7]. A comparison of the overall SAC analysis of the proposed S-box with AES[17], S-p-box, and Ref [15] is shown in Tables 3–6, while the mean results are shown in Table 7, and a graphical representation of the comparative analysis is shown in Figure 2. From Table 7 it can be seen that the proposed S-box has a maximum value of 0.526, a minimum value of 0.437, a mean value of 0.487, and a standard deviation of 0.015.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022

Table 3. SAC Analysis of Proposed S-box.

	bit 0	bit1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7
f_0	116	136	140	128	116	124	128	132
f_1	128	128	128	128	128	128	128	128
f_2	136	136	128	132	144	120	140	120
f_3	142	140	136	132	116	124	128	136
f_4	124	128	136	124	140	136	132	116
f_5	140	128	116	124	128	132	116	136
f_6	128	116	120	128	128	116	120	128
f_7	132	132	144	120	116	128	128	136

Table 4. SAC Analysis of S-box (AES)

	bit 0	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7
f_0	132	120	132	136	116	116	136	128
f_1	132	124	132	136	128	132	136	140
f_2	116	144	128	120	116	132	120	136
f_3	114	128	120	116	132	120	132	132
f_4	116	124	144	128	128	120	120	144
f_5	124	116	128	136	128	140	136	120
f_6	116	128	136	128	140	136	136	132
f_7	128	136	128	140	136	136	124	120

Table 5. SAC analysis of S-box (S-p-box)

	bit 0	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7
f_0	128	128	116	116	132	128	124	124
f_1	116	116	132	124	124	128	136	128
f_2	120	116	120	144	136	132	124	120
f_3	124	124	140	144	140	124	136	132
f_4	136	128	116	112	124	116	128	116
f_5	112	116	124	116	128	128	128	116
f_6	116	124	128	116	128	116	116	128
f_7	116	128	128	128	116	124	132	116

Table 6. SAC Analysis of S-box (Ref [15])

	bit 0	bit 1	bit 2	bit 3	bit 4	bit 5	bit 6	bit 7
f_0	116	116	140	132	132	116	132	136
f_1	132	136	132	148	136	116	132	132
f_2	120	136	120	128	116	140	128	124
f_3	124	120	132	144	140	140	116	120
f_4	128	148	136	132	124	124	132	132
f_5	128	136	124	128	136	144	124	136
f_6	140	140	132	124	116	132	140	124
f_7	120	124	124	124	116	124	144	132

DOI: 10.37943/12DZLQ4553

Table 7. Average outcomes of SAC

S-boxes	Proposed S-box	AES	S-P-Box	SM4	Ref [15]
Minimum Value	0.453	0.453	0.437	0.437	0.453
Maximum value	0.562	0.526	0.526	0.562	0.578
Average	0.501	0.504	0.487	0.499	0.506
Square Deviation	0.029	0.032	0.015	0.0039	0.034

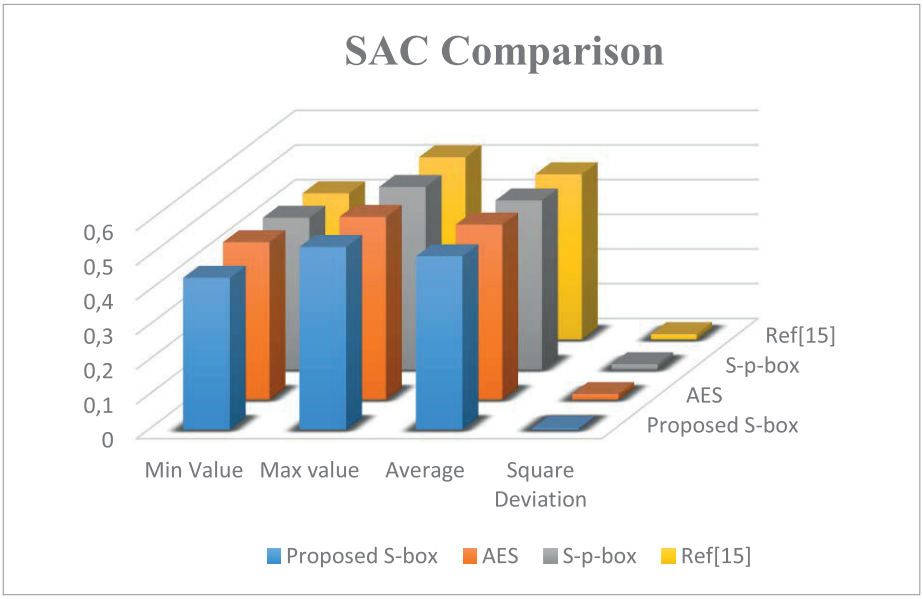

Figure 2. Graphical Representation of SAC.

Conclusion

S boxes play an important role in ensuring the robustness of symmetric transformations. In order to protect the algorithms against various cryptanalysis methods, S-blocks must have a number of cryptographic properties and satisfy a number of criteria. In this paper, it has been shown that the nonlinear and strong avalanche effect (SAC) of the S-box used in the AL03 encryption algorithm has very good performance. The results of comparing the studied S-box with the S-boxes of known cryptographic algorithms were also presented. As a result of the comparison, the corresponding result was obtained with the popular S-boxes. The S-boxes that I compared in the article are dynamic, so they only use it once. And since our proposed S-box is stable, it can be used for any block encryption algorithm. The proposed S-box has all the necessary cryptographic properties, and it has been proven that it can be used in any cryptosystem. In further works, the cryptographic strength of S-box will be studied by other methods, and the results will be obtained. The fully studied S-box is used as the main nonlinear transformation method responsible for the crypto-strength of the block encryption algorithm developed according to the research conducted under the grant project.

Acknowledgment

The research work was carried out at the Institute of Information and Computing Technologies of the RK MES CS within the framework of the AP14870419 “Development of cryptographic protection tools for safe negotiations via HF radio”.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022

References

1. Oleinikov, R.V., & Kazimirov, A.V. (2010). Selection of S-boxes for symmetric cryptographic algorithms based on the analysis of algebraic properties. *Bulletin of Kharkiv NU, 95*, 79-85.
2. Amjad, H.Z., Arshad, M.J., & Ahmad, M. (2019). A novel construction of efficient Substitution-Boxes using cubic fractional transformation. *Entropy, 21*(3), 2-13. https://doi.org/10.3390/e21030245
3. Ismail, E. S., & Chew, L. C. N. (2020). S box construction based on linear fractional transformation and permutation function. *Symmetry*, *12*(826), 1-16. https://doi.org/10.3390/sym12050826
4. Ozkaynak, F. (2017). Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications, 31*, 3317-3326. https://doi.org/10.1007/s00521-017-3287-y
5. Ahmad, M., Zahid, A.H., & Al Solami, E. (2020). A novel modular approach based Substitution Box design for image encryption. *In IEEE Access*, *8*, 150326-150340. https://doi.org/10.1109/ACCESS.2020.3016401
6. Massimiliano, Z., & Alexander, N.(2014). Gray code permutation algorithm for high-dimensional data encryption. *Information Sciences*, *270*, 288-297. https://doi.org/10.1016/j.ins.2014. 02.131
7. Yasir. N., Tariq, Sh., Dawood, Sh., & Sadam, H. (2019). A novel algorithm of constructing highly nonlinear S-p-boxes. *Cryptography*, *3*(1), 2–13. https://doi.org/10.3390/cryptography3010006
8. Hussain, I., Shah, T., Gondal, M.A., Khan, M., & Khan, W.A. (2011). Construction of new S-box using a linear fractional transformation. *World Applied Sciences Journal*, *14*, 1779–1785. https://www.idosi.org/wasj/wasj14(12)11/2.pdf
9. Saeed, M.S., Altaleb, A., Hussain, I., & Aslam M. (2017). An algorithm for the construction of substitution – box for block ciphers based on projective general linear group. *AIP Advances*, *7*(3), 1-12. https://doi.org/10.1063/1.4978264
10. Sarfraz, M., Hussain, I., & Ali F. (2016). Construction of S-Box based on mobius transformation and increasing its confusion creating ability through invertible function. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(2), 187–199. https://www.researchgate.net/publication/ 45900764
11. Gangadari, B.R., & Ahamed, S.R. (2016). Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications. *Healthcare Technology Letters*, *3*(3), 177–183. https://doi.org/10.1049/htl.2016.0033
12. Manjula, G., Mohan, H.S. (2016 July 21-23) Constructing key dependent dynamic S-Box for AES block cipher system. *2nd International Conference on Applied and Theoretical Computing and Communication Technology (ICATCCT)* (pp. 613-617). Bangalore, India. https://doi.org/10.1109/ICATCCT.2016.7912073
13. Algazy, K.T., Kapalova, N.A., Sakan, K.S., & Khompysh A. (2022). Modification of the AL01 encryption algorithm. *Bulletin of AUES*, *1*(56), 162-170. https://doi.org/10.51775/2790-0886_2022_56_1_162
14. Khompysh, A., Kapalova, N.A., Sakan, K.S., & Algazy K. (2022). Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information. *Cogent Engineering*, *9*(1), 1-12. https://doi.org/10.1080/233 11916.2022.2080623
15. Alkhaldi, A.H., Hussain, I., & Gondal, M.A. (2015). A novel design for the construction of safe S-boxes based on TDERC sequence. *Alexandria Engineering Journal*, *54*(1), 65–69. https://doi.org/10.1016/j.aej.2015.01.003
16. Algazy, K.T., Duysenbayev, D.S., & Sakan, K. (2021). Study of nonlinear nodes used in symmetric ciphers. *International scientific and practical conference (APISK-2021)* (pp. 34-38). Almaty, Kazakhstan.
17. Kazimirov, A.V. (2013). Methods and tools for generating nonlinear substitution nodes for symmetric cryptoalgorithms. [*PhD. thesis in Engineering Science, Kharkiv*], p.190.