UDC 004.056.5

Dr. Tech. Sci., prof. **Sokolov A.V.** (NU “Odesa Law Academy”)
Dr. Tech. Sci., prof. **Lienkov S.V.** (VIKNU, Kyev)
Radush V.V. (ONPU, Ukraine)

DOI: http://doi.org/10.17721/2519-481X/2025/86-09

CRYPTOGRAPHIC PROPERTIES OF S-BOXES CONSTRUCTED BASED ON DYNAMIC CHAOS THEORY WHEN REPRESENTED USING MANY-VALUED LOGIC FUNCTIONS

The S-box is the main cryptographic construction, which largely determines the effectiveness of block symmetric ciphers and hash functions. Several basic requirements are imposed on modern S-boxes based on such criteria of cryptographic quality as distance of nonlinearity, error propagation criterion, and absence of a correlation between the output and input vectors. The theory of dynamic chaos is one of the promising tools for the synthesis of S-boxes, which highly correspond to the specified criteria of cryptographic quality. However, the further development of cryptography and cryptanalysis methods led to the development of new attacks based on the representation of the ciphers using many-valued logic functions, which makes it necessary to research the cryptographic quality of S-boxes not only when they are represented by component Boolean functions, but also for all their possible representations with help of the many-valued logic functions. In this paper, we present the results of the research on modern structures of S-boxes based on the theory of dynamic chaos when they are represented by many-valued logic functions. We distinguished the S-box construction characterized by the highest level of cryptographic quality for all its possible representations, which can be recommended for practical use.

Keywords: cryptography, S-box, dynamic chaos theory, many-valued logic function.

Introduction. Increasing the security of modern cryptographic algorithms is associated with the continuous development of methods for synthesizing the cryptographic primitives on which they are based. One of the most important cryptographic primitives is the S-box, the structure of which largely determines the effectiveness and performance of the cryptographic algorithm in which it is operating.

Currently, there are quite a few approaches for constructing S-boxes, among which the classical approach is based on the use of criteria for the cryptographic quality of component Boolean functions. Among such criteria, the main ones are maximization of the nonlinearity distance, compliance with the error propagation criterion, and minimization of the correlation between the output and input vectors.

To date, there are quite a lot of efficient constructions that allow synthesizing S-boxes that correspond to the specified criteria of cryptographic quality, among which we can distinguish such well-known constructions as the Nyberg construction [1], Kim’s scheme [2] and its modification [3], as well as methods for generating S-boxes based on gradient descent [4].

However, in recent years, methods for synthesizing S-boxes based on the theory of dynamic chaos have become increasingly popular, making it possible to achieve a balanced correspondence of the synthesized structures to the basic criteria of cryptographic quality. An important property of these structures is their high algorithmicity: they can be implemented both in the form of a substitution table and using certain computational procedures, which is essential for their implementation on various hardware platforms. There are many known methods for the synthesis of S-boxes based on the theory of dynamic chaos, for example, [5…14]. All considered methods for synthesizing S-boxes based on the theory of dynamic chaos are designed to be characterized by a high degree of compliance with the criteria for the cryptographic quality of component Boolean functions.

However, currently, modern researcher attention is directed to the research of the possibilities of attacks on cryptographic constructions using the mathematical apparatus of many-valued logic

functions [15], which is conditioned by the possibility of representing cryptographic constructions by component functions of many-valued logic with different bases q, such that the length of the cryptographic construction can be represented as $N = q^k$, $k \neq 1$.

For example, S-boxes of practically important length $N = 16$, synthesized using the well-known method [16], have two possible representations: with the help of component Boolean functions, and also with the help of component 4-functions

$$S = \left\{ \begin{array}{c|cccccccccccccccc} S & 4 & 7 & 2 & 14 & 1 & 13 & 8 & 11 & 15 & 12 & 6 & 10 & 5 & 9 & 3 & 0 \\ \hline f_{21} & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ f_{22} & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ f_{23} & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ f_{24} & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ \hline f_{41} & 0 & 3 & 2 & 2 & 1 & 1 & 0 & 3 & 3 & 0 & 2 & 2 & 1 & 1 & 3 & 0 \\ f_{42} & 1 & 1 & 0 & 3 & 0 & 3 & 2 & 2 & 3 & 3 & 1 & 2 & 1 & 2 & 0 & 0 \end{array} \right\}, \quad (1)$$

each of which fully determines the structure of S-box and its cryptographic properties, and, therefore, should be carefully researched.

The obtained results [17] clearly show that the synthesis of high-quality cryptographic structures, that implement the principles of diffusion and confusion to the maximum extent, is possible only if they meet the criteria of cryptographic quality not only for component Boolean functions but also for component functions of many-valued logic for all possible representations of the S-box.

The current stage of cryptography is characterized by the rapid development of criteria for the cryptographic quality of many-valued logic functions, within which the following main criteria for many-valued logic functions are proposed:

- the criterion for maximizing nonlinearity distance [18, 19];
- the error propagation criterion [16];
- the criterion for minimizing the correlation between the output and input of a cryptographic construction [20].

Next, we consider a mathematical apparatus designed to numerically estimate the degree of compliance of a cryptographic construction with each of the above criteria, and also give an example of determining compliance with the cryptographic quality criteria of an S-box of small length $N = 16$

Formulation of the problem. While S-boxes play a crucial role in cryptographic systems due to their ability to ensure nonlinearity and confusion, their construction and analysis are predominantly based on binary logic. However, the potential of S-boxes generated through dynamic chaos remains underexplored when they are represented using many-valued logic functions. This gap poses a significant problem, as many-valued logic could provide a broader framework for analyzing and optimizing S-boxes, potentially leading to stronger cryptographic properties and more secure systems.

Analysis of previous research. A method for numerically determining the nonlinearity distance of many-valued logic functions is presented in [19] and, thus, a generalized formula for calculating the nonlinearity of Boolean functions and many-valued logic functions for arbitrary q is derived

$$NL = \begin{cases} q^k - \max\left\{\left|\Omega(\omega)\right|\right\}, & q > 2; \\ 2^{k-1} - \dfrac{1}{2}\max\left\{\left|W(\omega)\right|\right\}, & q = 2, \end{cases} \quad (2)$$

where $\Omega(\omega)$ are the coefficients of the Vilenkin-Chrestenson transform of the many-valued logic

function, and $W(\omega)$ are the coefficients of the Walsh-Hadamard transform of the Boolean function.

In this case, the Walsh-Hadamard transform of a Boolean function f is found using the product of its truth table, represented in exponential form using mapping $\{0 \leftrightarrow 1, 1 \leftrightarrow -1\}$, by the Walsh-Hadamard matrix

$$W = FA_N, \tag{3}$$

where

$$A_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix}, \; A_1 = 1. \tag{4}$$

The component Boolean function f_{21} of the S-box (1) has the following Walsh-Hadamard transformants

$$W_{f_{21}} = \{0 \quad 0 \quad -8 \quad 0 \quad 8 \quad 0 \quad 0 \quad 0 \quad 0 \quad 8 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 8\}, \tag{5}$$

and, in accordance with (2), its value of the nonlinearity distance is equal to $N_{f_{21}} = 4$.

The Vilenkin-Chrestenson transform is defined as the product of the component q-function represented over the exponential alphabet $\left\{ e^{j\frac{2\pi}{q}\nu} \right\}, \nu = 0,1,...,q-1$ by the Vilenkin-Chrestenson matrix

$$\Omega = FV_N, \tag{6}$$

in this case, the rows of the matrix V_N are given by the following relation [21]

$$v_t(x) = \mathrm{e}^{\frac{2\pi}{q}\sum_{i=1}^{k} t_i x_i}, \tag{7}$$

where t_i is the i-th digit of the number t written in the positional q-ary system;

k is the number of digits in the q-ary representation of the value N, which determines the length of the signal samples, and $N = q^k$.

For the case of $q = 4$, the matrix V can be constructed according to the following recursive relation

$$V_{4^{k+1}} = \begin{bmatrix} V_{4^k} & V_{4^k} & V_{4^k} & V_{4^k} \\ V_{4^k} & V_{4^k}+1 & V_{4^k}+2 & V_{4^k}+3 \\ V_{4^k} & V_{4^k}+2 & V_{4^k} & V_{4^k}+2 \\ V_{4^k} & V_{4^k}+3 & V_{4^k}+2 & V_{4^k}+1 \end{bmatrix}, \quad V_4 = \begin{bmatrix} z_0 & z_0 & z_0 & z_0 \\ z_0 & z_1 & z_2 & z_3 \\ z_0 & z_2 & z_0 & z_2 \\ z_0 & z_3 & z_2 & z_1 \end{bmatrix}, \tag{8}$$

where $\{z_0, z_1, z_2, z_3\} = \{e^0, e^{j\frac{2\pi}{4}}, e^{j\pi}, e^{j\frac{3\pi}{2}}\}$, and the summation is performed with respect to the indices z.

For example, we find $|\Omega|$ for the component 4-function f_{41}

$$|\Omega| = \{0 \quad 4 \quad 0 \quad 4 \quad 0 \quad 2.8284 \quad 4 \quad 2.8284 \quad 5.6569 \quad 8 \quad 0 \quad 8 \quad 0 \quad 2.8284 \quad 4 \quad 2.8284\},' \tag{9}$$

thus, in accordance with (2), the nonlinearity distance of the component 4-function f_{41} is equal to $N_{f_{41}} = 8$.

Using the formula (2), it is easy to estimate the nonlinearity distances for each component Boolean function f_{2i} of the S-box (1), as well as for each of its component 4-function f_{4j}. Thus, the nonlinearity distances of the component Boolean functions are stable and are equal to $\{4,4,4,4\}$, while the nonlinearity distances of the component 4-functions are equal to $\{8,7.51\}$. The minimum value is used in each case as a general estimate of the nonlinearity of the S-box. Thus, having a maximum and uniformly distributed value of the nonlinearity of the component Boolean functions, the S-box (1) is characterized by a non-uniformly distributed and not reaching the maximum boundary nonlinearity distance of its component 4-functions.

The estimation of the compliance of Boolean functions to the error propagation criterion is based on the following definitions:

Definition 1 [16]. The directional derivative of a Boolean function f along a vector $u \in V_k$ is a Boolean function

$$D_u f(x) = f(x) \oplus f(x \oplus u), \tag{10}$$

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

Definition 2 [16]. A Boolean function f satisfies the error propagation criterion along a vector $u \in V_k$ if its directional derivative along a vector u is a balanced function, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0.5. \tag{11}$$

Definition 3 [16]. A Boolean function f satisfies the error propagation criterion of the degree m if it satisfies the error propagation criterion along all vectors u of weight $1 \le wt(u) \le m$, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0.5, \quad \forall u \in V_k, \quad 1 \le wt(u) \le m. \tag{12}$$

Definition 4 [16]. A Boolean function f satisfies the strict avalanche criterion (SAC) if it satisfies the error propagation criterion of degree 1, i.e.

$$p\{f(x) = f(x \oplus u)\} = 0.5, \quad \forall u \in V_k, \quad wt(u) = 1. \tag{13}$$

Definition 5 [16]. The weight $\varpi(u)$ of a q-valued vector is the number of its nonzero components.

Definition 6 [16]. The derivative of a function f along a q-valued vector u is the function

$$D_u f(x) = f(x \underset{q}{\oplus} u) - f(x) \,(\mathrm{mod}\, q), \tag{14}$$

where $\underset{q}{\oplus}$ means the summation modulo q.

Definition 7 [16]. An q-valued logic function f satisfies the error propagation criterion along a vector $u \in V_k$ if its directional derivative along the vector u is a balanced function, i.e. its values

$0,1,...,q-1$ occur with equal probabilities: $p(D_u f(x) = i(\mathrm{mod}\, q)) = \frac{1}{q}$ for all $i = 0,1,...,q-1$. In other words, $K^0 = K^1 = ... = K^{q-1}$, where K^i is the number of sets of values of variables on which the derivative takes on a value i.

Definition 8 [16]. A q-valued logic function f satisfies the error propagation criterion of order k if it satisfies the error propagation criterion for all vectors u of weight $1 \le \varpi(u) \le k$.

Definition 9 [16]. A q-valued logic function satisfies the SAC if it satisfies the error propagation criterion of the degree 1.

Consider an example of determining the correspondence of the first component Boolean function of the S-box (1) to the SAC using **Definitions 1...4**, for which we find its derivatives in directions $\{0001\},\{0010\},\{0100\},\{1000\}$, which have the following form

$$\begin{array}{l} D_{0001} f_{21} = \{1000111001001101\}; \\ D_{0010} f_{21} = \{0001011100101011\}; \\ D_{0100} f_{21} = \{1101010011101000\}; \\ D_{1000} f_{21} = \{1000111001001101\}. \end{array} \quad (15)$$

Since all derivatives (15) are balanced, we can conclude that the component function f_{21} corresponds to the SAC. It is also easy to verify that the remaining component functions f_2, f_3, f_4 also correspond to the SAC.

Let us check the avalanche properties of the S-box (1) when it is represented by component 4-functions. To do this, following **Definitions 5...9**, we find the derivatives of the component 4-functions in the directions of unit weight

$$\begin{array}{ll} D_{01} f_{41} = \{3302033212010211\}; & D_{01} f_{42} = \{0332330202111201\}; \\ D_{02} f_{41} = \{1221232321123232\}; & D_{02} f_{42} = \{3223303023320303\}; \\ D_{03} f_{41} = \{2321321232122321\}; & D_{03} f_{42} = \{3212232123213212\}; \\ D_{10} f_{41} = \{3100003113000013\}; & D_{10} f_{42} = \{2213132222313122\}; \\ D_{20} f_{41} = \{2110201133203023\}; & D_{20} f_{42} = \{2011211030233320\}; \\ D_{30} f_{41} = \{1212322321212332\}; & D_{30} f_{42} = \{0101122110102112\}. \end{array} \quad (16)$$

Detailed research of the (16) shows that for the function f_{41} only the derivatives $D_{01} f_{41}$ and $D_{20} f_{41}$ are balanced, while for the function f_{42} the derivatives $D_{01} f_{42}$ and $D_{01} f_{42}$ are balanced, thus, none of the component 4-functions of the S-box (1) correspond to the SAC.

For the convenience of measuring the degree of discrepancy of the derivative from the SAC requirements, the indicators of the maximum and integral deviation from the SAC can be used. Consider an example of a derivative $D_{02} f_{41}$, for which we write the number of symbols “0”, “1”, “2” and “3”

$$\begin{Bmatrix} K^0_{D_{02} f_{41}} & K^1_{D_{02} f_{41}} & K^2_{D_{02} f_{41}} & K^3_{D_{02} f_{41}} \\ 0 & 4 & 8 & 4 \end{Bmatrix}. \quad (17)$$

However, based on **Definition 9**, we need the numbers of characters “0”, “1”, “2” and “3” to be equal to each other, i.e. $K^0 = K^1 = K^2 = K^3 = N/4 = 4$. However, in our case, we have the inequality of these values to each other. We can calculate the deviations for each symbol of the derivative from the required amount to correspond to the SAC

$$\left\{\begin{array}{cccc} \Delta K^0_{D_{02}f_{41}} & \Delta K^1_{D_{02}f_{41}} & \Delta K^2_{D_{02}f_{41}} & \Delta K^3_{D_{02}f_{41}} \\ \left|4-K^0_{D_{02}f_{41}}\right| & \left|4-K^1_{D_{02}f_{41}}\right| & \left|4-K^2_{D_{02}f_{41}}\right| & \left|4-K^3_{D_{02}f_{41}}\right| \end{array}\right\} = \\ = \left\{\begin{array}{cccc} \Delta K^0_{D_{02}f_{41}} & \Delta K^0_{D_{02}f_{41}} & \Delta K^0_{D_{02}f_{41}} & \Delta K^0_{D_{02}f_{41}} \\ 4 & 0 & 4 & 0 \end{array}\right\}. \tag{18}$$

The integral deviation from the SAC for the S-box is defined as the sum of all deviations $\Delta K^i_{D_j f_l}$ for all component q-functions in all directions corresponding to **Definition 9**

$$\Delta K_S = \sum_{l=1}^{k}\sum_{j=1}^{h}\sum_{i=0}^{q-1}\Delta K^i_{D_j f_l}, \tag{19}$$

where k is the number of component q-functions, h is the number of derivatives of unit weight for a given length of the component q-function, q is the base of the S-box representation.

The maximum deviation from the SAC for the S-box will be defined as the maximum value among all $\Delta K^i_{D_j f_l}$

$$\Delta_{\max} K_S = \max\left\{\Delta K^i_{D_j f_l}\right\}, \quad l=1,2,...,k, \quad j=1,2,...,h, \quad i=0,1,...,q-1. \tag{20}$$

It is clear that lower values of ΔK_S and $\Delta_{\max} K_S$ characterize a higher quality of the S-box. Ideally, we need equality $\Delta K_S = \Delta_{\max} K_S = 0$ for all possible representations of the S-box by component q-functions.

It is not difficult to determine that for an S-box (1) $\Delta K_S = 0, \Delta_{\max} K_S = 0$ for its representation by component Boolean functions, and $\Delta K_S = 192, \Delta_{\max} K_S = 8$ for its representation by the component 4-functions.

Next, we consider the criterion for minimizing the correlation between the output of a cryptographic construction and its input. To determine the degree of correlation between the output vectors of the S-box and its input vectors, the mathematical apparatus of the matrices of correlation coefficients $R = \left\| r_{i,j} \right\|$, $i, j = 1,2,...,k$ is used, where the correlation coefficients

$$r_{i,j} = 1 - 2^{-(k-1)} \sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j}), \; i, j = 1,2,...,k, \tag{21}$$

where $x_{m,i}$, $y_{m,j}$ denote the input and output vectors of the S-box, respectively.

The absence of correlation between the output and input bits ($r_{i,j} = 0$) is considered as a good quality of the cipher, but researchers are increasingly insisting that a minimization of correlation coefficients absolute values, while their absolute values are approximately equal to each other, is more important.

Formula (21) is suitable for calculating the correlation dependence of output and input vectors for all the most common S-boxes in practice, the length of which can be represented as $N = 2^k$, while the matrix R is the same for representations of S-boxes by different bases q. For the case of researching the correlation dependence of the output and input vectors for S-boxes of length $N \neq 2^k$, the mathematical apparatus [17] is used.

Results. Currently, numerous methods for synthesizing cryptographically high-quality S-boxes based on the theory of dynamic chaos have been created, the most common ones are

presented in [5 - 14]. All specified S-boxes have length $N = 256$, which corresponds to the architecture of modern cryptographic algorithms. Thus, all of these S-boxes can be represented as 8 component Boolean functions, 4 component 4-functions, or 2 component 16-functions, each of which determines the cryptographic quality of the entire construction and should be carefully researched.

Using the mathematical apparatus for researching the cryptographic quality of S-boxes described in this paper, we perform research on the cryptographic quality of S-boxes based on the theory of dynamic chaos [5 - 14], the results of which are presented in Tab. 1.

Table 1

Values of cryptographic quality indicators for S-boxes based on the dynamic chaos theory

№	S-блок	$q = 2$			$q = 4$			$q = 16$			$\max\{\lvert r_{ij} \rvert\}$
		ΔK_S	$\Delta_{\max} K_S$	N_{f_2}	ΔK_S	$\Delta_{\max} K_S$	N_{f_4}	ΔK_S	$\Delta_{\max} K_S$	$N_{f_{16}}$	
1	[5]	520	32	106	1232	18	209.1385	3108	**12**	212.3220	0.1406
2	[6]	656	32	98	1120	18	213.2449	2876	14	206.1523	**0.125**
3	[7]	552	28	102	1312	43	202.3344	3276	17	194.5649	0.1563
4	[8]	544	24	104	1108	24	213.4794	2956	12	214.1403	0.1563
5	[9]	524	28	96	1088	28	214.7689	2980	12	213.7293	0.1641
6	[10]	484	24	100	1024	20	216	2868	14	216.9470	0.1719
7	[11]	484	24	106	1016	**16**	213.0582	2804	14	217.0569	**0.125**
8	[12]	636	28	104	1052	22	210.3054	2968	11	215.2830	0.1641
9	[13]	512	28	104	1096	18	212.1366	2908	18	**219.1407**	0.1719
10	[14]	**432**	**16**	**112**	**880**	**16**	**216.6046**	**2728**	14	216.5184	**0.125**

Analysis of the data presented in Table 1 shows that the cryptographic properties of S-boxes built on the basis of the dynamic chaos theory vary greatly for various well-known structures, both in the case of their representation by component Boolean functions and by component functions of many-valued logic. At the same time, according to most of the calculated indicators, the best construction is [14], which is characterized by both a high level of nonlinearity, low maximal and integral deviations from the SAC, and small peaks in the correlation dependence of the output vectors from the input vectors.

All S-boxes researched in this paper were generated by dynamic chaos algorithms and mostly reached values close to the maximum value in the Boolean component functions and the case of component 4-functions, but unfortunately, not so good results for component 16-functions. According to this, we could affirm that they are good for nonlinear requirements, and this approach could be recommended for synthesizing S-boxes that satisfy the criterion of high nonlinearity.

Despite the previous fact, according to research performed, we could observe, that all provided S-boxes couldn't reach the values to fully satisfy the SAC. Some of them were very close, but most did not reach full compliance with this criterion. Because of these results, we could make an assumption, that considered algorithms based on dynamic chaos concepts are not designed to generate S-boxes, that fully satisfy SAC, because of their unpredictable nature (the main concept of dynamic chaos) and SAC requires stricter algorithms with more predictable behavior like [2].

So, the very high sensitivity of chaotic algorithms to the input data from one side provides great and even perfect results in the case of nonlinearity and simultaneously good results in the case of SAC.

But, despite all the discussed problems, S-box [14] is characterized by very high compliance with cryptographic quality criteria for all possible representations. So, it could be recommended for practical use in modern block symmetric algorithms such as AES and could potentially improve their effectiveness.

Conclusions. We note the main results of the research:

1. Using any known cryptographic construction to build S-boxes implies thorough research of the properties of the resulting S-box, both when it is represented using the mathematical apparatus of Boolean functions, and using the mathematical apparatus of many-valued logic functions.

2. Methods for synthesizing S-boxes based on the theory of dynamic chaos are promising, while S-boxes synthesized based on them can be characterized by a high level of cryptographic quality. Nevertheless, when developing S-box constructions based on the dynamic chaos theory, it is important to take into account their properties not only when represented by Boolean functions, but also when they are represented using many-valued logic functions.

3. Among the set of researched S-boxes, a construction is selected that is characterized by the best level of cryptographic quality according to most of the considered indicators. This construction can be recommended for practical use in existing and developed cryptographic algorithms.

REFERENCES:

1. Nyberg, K. (1994). Differentially uniform mappings for cryptography. Advances in cryptology. Proc. of EUROCRYPT'93. Berlin, Heidelberg, New York, vol.765, pp.55-65. https://doi.org/10.1007/3-540-48285-76

2. Kim, K., Matsumoto, T., Imai, H. (1990). A recursive construction method of S-boxes satisfying strict avalanche criterion. Proc. of CRYPTO'90. Springer-Verlag, pp. 565-574. https://doi.org/10.3103/s0735272713080049

3. Sokolov, A.V. (2013). Constructive method for the synthesis of nonlinear S-boxes satisfying the strict avalanche criterion. Radioelectronics and Communications Systems, vol. 56, no. 8, pp. 415-423. https://doi.org/10.3103/s0735272713080049

4. Kazimirov, A.V. Oleinikov, R.V. (2013). A method for constructing non-linear replacement nodes based on gradient descent. Radiotekhnika, issue 172, pp. 104-108.

5. Tian, Y., Zhimao, L. (2017). Chaotic S-Box: Intertwining Logistic Map and Bacterial Foraging Optimization, Mathematical Problems in Engineering, pp. 1-11. https://doi.org/10.1155/2017/6969312

6. Tanyildizi, E., Özkaynak, F. (2019). A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps. IEEE Access, vol. 7, pp. 117829-117838. https://doi.org/10.1109/access.2019.293644

7. Farwa, S., Shah, T., Muhammad, N. (2017). An Image Encryption Technique based on Chaotic S-Box and Arnold Transform. International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, pp. 360-364. https://doi.org/10.14569/ijacsa.2017.080647

8. Lu, Q., Zhu, C., Deng, X. (2020). An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box. IEEE Access, vol. 8, pp. 25664-25678. https://doi.org/10.1109/ACCESS.2020.2970806

9. Asim, M., Jeoti, V. (2008). Efficient and Simple Method for Designing Chaotic S-Boxes. ETRI Journal, vol. 30, no. 1, pp. 170-192. https://doi.org/10.4218/etrij.08.0207.0188

10. Wang, J., Zhu, Y., Zhou, C., Qi, Z. (2020). Construction Method and Performance Analysis of Chaotic S-Box Based on a Memorable Simulated Annealing Algorithm. Symmetry. 2020. https://doi.org/10.3390/sym12122115

11. Lambić, D. (2018). S-box design method based on improved one-dimensional discrete chaotic map. Journal of Information and Telecommunication, vol. 2, issue 2, pp. 181-191. https://doi.org/10.1080/24751839.2018.1434723

12. Lu, Q., Zhu, C., Wang, G. (2019) A Novel S-Box Design Algorithm Based on a New Compound Chaotic System. Entropy, no. 21(10), pp. 1004, 2019. https://doi.org/10.3390/e21101004

13. Lai, Q., Akgul, A., Li, C., Xu, G., Çavuşoğlu, U. (2018). A New Chaotic System with Multiple Attractors: Dynamic Analysis, Circuit Realization and S-Box Design. Entropy, no. 20(1), pp. 12. https://doi.org/10.3390/e20010012

14. Hussain, I., Anees, A., Al-Maadeed, T., Mustafa, M. (2019). Construction of S-Box Based on Chaotic Map and Algebraic Structures. *Symmetry*, no. 11(3), pp. 351. https://doi.org/10.3390/sym11030351

15. Baigneres, T., Stern, J., Vaudenay, S. (2007). Linear cryptanalysis of non-binary ciphers. Proceedings of the International Workshop on Selected Areas in Cryptography, Berlin, Heidelberg: Springer, pp. 184-211.

16. Sokolov, A.V., Zhdanov, O.N. (2019). Strict avalanche criterion of four-valued functions as the quality characteristic of cryptographic algorithms strength. Siberian Journal of Science and Technology, vol. 20, no. 2, pp.183-190. https://doi.org/10.31772/2587-6066-2019-20-2-183-190

17. Sokolov, A.V., Zhdanov, O.N. (2020). Cryptographic constructions based on many-valued logic functions, Monograph. M: Scientific Thought, 192 p. https://doi.org/10.12737/1045434

18. Sokolov, A.V., Djiofack, T.V.N. (2019). Nonlinear Properties of Rijndael S-boxes Represented by the Many-Valued Logic Functions. Proceedings of the International Workshop on Cyber Hygiene, Kyiv, pp. 96-106.

19. Sokolov, A.V., Zhdanov, O.N. (2016). Regular synthesis method of a complete class of ternary bent-sequences and their nonlinear properties. Journal of Telecommunication, Electronic and Computer Engineering, vol. 8, no. 9, pp. 39-43.

20. Bakunina, E.V., Dykyi, O.V. (2022). Synthesis method for S-boxes satisfying the criterion of correlation immunity of Boolean and 4-functions. Journal of Discrete Mathematical Sciences and Cryptography. https://doi.org/10.1080/09720529.2021.2018112

21. Trakhtman, A.M., Trakhtman, V.A. (1975). Fundamentals of the theory of discrete signals on finite intervals, M: Sov.radio. 208 p.

д.т.н., проф. Соколов А.В., д.т.н.,проф. Лєнков С.В., Радуш В.В.

КРИПТОГРАФІЧНІ ВЛАСТИВОСТІ S-БЛОКІВ, ЩО ПОБУДОВАНІ НА ОСНОВІ ТЕОРІЇ ДИНАМІЧНОГО ХАОСУ ПРИ ПРЕДСТАВЛЕННІ ЗА ДОПОМОГОЮ ФУНКЦІЙ БАГАТОЗНАЧНОЇ ЛОГІКИ

S-блок є основною криптографічною конструкцією, яка багато в чому визначає ефективність блочних симетричних шифрів і хеш-функцій. До сучасних S-блоків висувається декілька основних вимог, заснованих на таких критеріях криптографічної якості, як відстань нелінійності, критерій розповсюдження помилки та критерій відсутності кореляції між вихідним і вхідним векторами. Теорія динамічного хаосу є одним із перспективних інструментів для синтезу S-блоків, які у великій мірі відповідають заданим критеріям криптографічної якості. Проте подальший розвиток криптографії та методів криптоаналізу привів до розробки нових атак, заснованих на представленні шифрів за допомогою функцій багатозначної логіки, що робить необхідним дослідження криптографічної якості S-блоків не тільки при їх представленні компонентними булевими функціями, а також для всіх можливих їх представлень за допомогою функцій багатозначної логіки. У цій роботі надано результати дослідження сучасних конструкцій S-блоків на основі теорії динамічного хаосу при їх представленні функціями багатозначної логіки. Було виділено конструкцію S-блока, що характеризується найвищим рівнем криптографічної якості для всіх можливих її представлень, яку можна рекомендувати для практичного використання.

Ключові слова: криптографія, S-блок, теорія динамічного хаосу, функція багатозначної логіки.