UDC xxx.xxx.x

A.V. Sokolov, V.V. Radush

1Odesa Polytechnic National University,

1 Shevchenko ave., Odesa, 65044, Ukraine

**Cryptographic properties of s-boxes constructed on the basis of dynamic chaos theory when represented using many-valued logic functions**

*Abstract.* 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 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 Boolean functions, but also for all possible representations by the many-valued logic functions. In this paper, we represent 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. A construction has been found that has the highest level of cryptographic quality for all its possible representations, which, accordingly, can be recommended for practical use.

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

**1. 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], the Kim 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 , such that the length of the cryptographic construction can be represented as , .

S-boxes of practically important length , for example, 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

, (1)

each of which fully determines the structure and cryptographic properties of these structures, 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.

**2. Research materials and methods**

The current stage of cryptography development 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 quality are proposed:

* the criterion for maximizing nonlinearity distance [18, 19];
* the error propagation criterion [16];
* the criterion for minimizing the correlation between the output;
* the 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 

**3. Analyzing literary sources**

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

 (2)

where  are the coefficients of the Vilenkin-Chrestenson transform of the many-valued logic function, and  are the coefficients of the Walsh-Hadamard transform of the Boolean function.

In this case, the Walsh-Hadamard transform of a Boolean function  is found using the product of its truth table, represented in exponential form by mapping , by the Walsh-Hadamard matrix

, (3)

where

, . (4)

The component Boolean function  of the S-box (1) has the following Walsh-Hadamard transform transforms

 (5)

and, in accordance with (2), the value of the nonlinearity distance .

The Vilenkin-Chrestenson transform is defined as the product of the component *q*-function represented over the exponential alphabet  by the Vilenkin-Chrestenson transform matrix

, (6)

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

, (7)

where  is the -th digit of the number  written in the positional -ary system;

 is the number of digits in the *q*-ary representation of the value , which determines the length of the signal samples, and .

For the case of , the matrix  can be constructed according to the following recursive relation

 (8)

where , and the summation is performed with respect to the indices .

For example, we find  for the component 4-function 

, (9)

thus, in accordance with (2), the nonlinearity distance of the component 4-function  is equal to .

Using formula (2), it is easy to estimate the nonlinearity distances for each component Boolean function  of the S-box (1), as well as for each of its component 4-functions . Thus, the non-linearity distances of the component Boolean functions are stable and are equal to , while the non-linearity distances of the component 4-functions are . The minimum value is used in each case as a general estimate of the non-linearity 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 coincidence of Boolean functions to the error propagation criterion is based on the following definitions:

**Definition 1 [16].** The directional derivative of a Boolean function  along a vector  is a Boolean function

, (10)

where  is a linear vector space of binary vectors of length ,  is summation modulo 2.

**Definition 2 [16].** A Boolean function  satisfies the error propagation criterion along a vector  if its directional derivative along a vector  is a balanced function, i.e.

. (11)

**Definition 3 [16].** A Boolean function  satisfies the error propagation criterion of the degree  if it satisfies the error propagation criterion along all vectors  of weight , i.e.

, . (12)

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

, . (13)

**Definition 5 [16].** The weight  of a *q*-valued vector is the number of its nonzero components.

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

 , (14)

where  means the summation modulo .

**Definition 7 [16].** An *q*-valued logic function  satisfies the error propagation criterion along a vector  if its directional derivative along the vector  is a balanced function, i.e. its values  occur with equal probabilities:  for all . In other words, , where  is the number of sets of values of variables on which the derivative takes on a value .

**Definition 8 [16].** A *q*-valued logic function  satisfies the error propagation criterion of order  if it satisfies the error propagation criterion for all vectors  of weight 

**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 , which have the following form

 (15)

Since all derivatives (15) are balanced, we can conclude that the component function  corresponds to the SAC. It is also easy to verify that the remaining component functions  also corresponds 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, in accordance with **Definitions 5...9**, we find the derivatives of the component 4-functions in the directions of unit weight

 (16)

Detailed research of the (16) shows that for the function  only the derivatives  and  are balanced, while for the function  the derivatives  and  are balanced, thus, none of the component 4-functions of the S-box (1) corresponds 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 , for which we write the number of symbols “0”, “1”, “2” and “3”

. (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. . 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

 (18)

The integral deviation from the SAC for the S-box is defined as the sum of all deviations  for all component *q*-functions in all directions corresponding to **Definition 9**

, (19)

where  is the number of component *q*-functions,  is the number of derivatives of unit weight for a given length of the component *q*-function,  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 

 (20)

It is clear that lower values of  and  characterize a higher quality of the S-box. Ideally, we need equality  for all possible representations of the S-box by component *q*-functions.

It is not difficult to determine that for an S-box (1)  for its representation by component Boolean functions, and  for its representation by the component 4-functions.

*2.3. Criterion for minimizing the connection 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 ,  is used, where the correlation coefficients

, , (21)

where ,  denote the input and output vectors of the S-box, respectively.

The absence of correlation between the output and input bits () 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 , while the matrix  is ​​the same for representations of S-boxes by different bases . For the case of researching the correlation dependence of the output and input vectors for S-boxes of length , the mathematical apparatus [17] is used.

**4. Research results and discussion**

Currently, a lot of 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 , 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 Section 2 of this paper, we perform research of the cryptographic quality of S-boxes based on the theory of dynamic chaos [5…14], the results of which are presented in Table 1.

Table 1 — Values of indicators of cryptographic quality of S-boxes based on the dynamic chaos theory

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | S-блок |  | | |  | | |  | | |  |
|  |  |  |  |  |  |  |  |  |
| 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, accordingly to the most of calculated indicators, the best construction is [14], which is characterized by both a high level of nonlinearity, low differential and integral deviations from the SAC, and small peaks in the correlation dependence of the output vectors from the input vectors.

**5. Results discussion**

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

Despite the previous fact, after investigation we could observe, that all provided S-boxes couldn’t reach values, that are required by SAC. Some of them were very close, but mostly results are more than unappropriated. Because of this results we could make an assumption, that algorithms based on dynamic chaos concepts couldn’t generate S-boxes, that satisfy SAC, because of their unpredictable nature (the main concept of the dynamic chaos) and SAC requires stricter algorithms with more predictable behavior like in [2].

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

But, despite all discussed problems, block 10 from the Table 1 is perfect in nonlinear case in 2-system, very close to perfect value in 4-system and has not bad results in 16-system, so it could be recommended for implementation in modern symmetric block algorithms such as AES, that is supported at hardware level and could potentially improve it work.

**6. Conclusions and recommendations**

We note the main results of the research:

1. The use of any known cryptographic construction to build S-boxes implies a 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.

**7. 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/10.1007/3-540-48285-7\_6
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.