ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 004.056.55
doi: 10.32620/reks.2023.3.12

Iryna LYSYTSKA[1], Kostiantyn LYSYTSKYI[1],
Oleksii NARIEZHNII[1], Tetiana HRINENKO[2]

[1] ***V. N. Karazin Kharkiv National University, Kharkiv, Ukraine***
[2] ***Kharkiv National University of Radio Electronics, Kharkiv, Ukraine***

THE INFLUENCE OF S-BOXES ON THE ARRIVAL OF THE CIPHER TO THE STATE OF RANDOM SUBSTITUTION

The subject *of this study is the process of developing block symmetric ciphers with improved cryptographic stability indicators for solving the problems of information protection in information and communication systems.* ***The goal of this study is*** *to develop a mathematical model of the optimal s-box design (non-linear substitution block) for modern block symmetric ciphers.* ***Task****: to show that the stability of block symmetric ciphers does not significantly depend on the indicators of the s-boxes included in these ciphers; to justify their use without reducing the stability of random substitutions as s-box constructions of modern block symmetric ciphers; and to prove the futility of searching for s-boxes with special properties.* ***The methods used are:*** *methods of probability theory; mathematical statistics; combinatorics and system analysis; methods of statistical tests; and methods of Boolean algebra. The following* ***results*** *were obtained. In modern ciphers, nonlinear substitution transformations are used as S-boxes (in most ciphers, byte substitutions are used). S-boxes perform the main function of encryption transformation - mixing of text bits. Dynamic indicators of the arrival of the cipher in the state of random substitution depend on their effectiveness. The presented results confirm that the indicators of cipher stability do not significantly depend on the indicators of the S-boxes included in the ciphers. It is not the individual properties of substitutions, but the results of their sequential interactions decisive for achieving stability indicators. It is shown that the fee for encryption is chosen to be three to four times greater than the depth of the avalanche effect - the minimum number of cycles of the cipher's arrival to the state of random substitution) is hardly noticeable.* ***Conclusions****. The scientific novelty of the obtained results is as follows. This work represents a generalization of the transition to the use of random permutations as S-boxes is an increase of only one cycle in the number of cycles of the arrival of the cipher to the state of random permutations, and this is hardly noticeable against the background of the stability margin used in modern ciphers. The result of this generalization is a scientific statement that can be described as follows: random S-boxes can be used in all known modern ciphers without reducing stability. That is, the task of finding S-boxes with special properties loses any meaning, which means that the scientific direction related to the search for S-boxes with special properties becomes redundant.*

Keywords*: complete differential; randomness criteria; S-box; substitution; table of differential differences; table of linear approximations.*

Introduction

As established in previous works [1, 2], all ciphers, regardless of the S-boxes (S-blocks) used (excluding their degenerate constructions) acquire properties of random substitution. This is not affected by the randomness indicators of the S-boxes of the cipher. The randomness indicators of S-boxes affect only the number of cycles of the cipher reaching the state of random substitution, and then only within one cycle.

At the same time, publications on block symmetric ciphers pay considerable attention to the search for S-boxes with special properties. Most often, this is one of the main design decisions when constructing a cipher.

One can find hundreds of dissertations, and publications on substitutions. However, we believe that this direction in the development of cryptography is not promising (it is erroneous).

The search for S-boxes with improved performance does not justify itself. The difference in the indicators of S-boxes is leveled out when passing through the cipher. In the general case, random S-boxes may need an additional encryption cycle to arrive in the random substitution state. However, this, considering the safety margin of ciphers (the number of encryption cycles is three to four times the depth of the avalanche effect), does not lead to a decrease in the stability of the cipher.

In addition, a possibility was found to build the cyclic function of the cipher in such a way that it does not require an additional cycle. This has been proposed in previous studies and is patented. Therefore, the questions of the expediency of careful selection of S-boxes become natural. It is not worth the expense and attention. This fact is what we try to show in our work.

Therefore, a new concept of designing block symmetric ciphers is put forward with a proposal to use them in ciphers without reducing the stability of random S-boxes, which means that the scientific direction associated with the search for S-boxes with special properties becomes non-productive.

1. Problem Statement

The purpose of this study is to show that the stability of ciphers does not depend significantly on the indicators of the S-boxes included in the ciphers.

Moreover, there are attempts to substantiate an important scientific position: in all known modern ciphers, random S-boxes can be used without lowering the stability. This means that the task of finding S-boxes with special properties loses all sense.

2. Review of the Literature

Interest and attention to the study and development of procedures for constructing cryptographically stable substitutive nonlinear transformations (called S-boxes, starting from the works of E. Biham and A. Shamir) arose in the early 90s of the last century. It became a natural result of studying and researching the reliability of the American symmetric encryption standard DES, which by that time had won world authority and recognition (which had actually become the world standard).

The work of Israeli cryptographers E. Biham and A. Shamir, who proposed an attack of differential cryptanalysis on the DES cipher, occurred at the same time, and two years later, the work of M. Matsui, devoted to linear cryptanalysis, i.e., the second new crypto attack on the DES, appeared [3].

These works became a noticeable stimulus for the further development of studies devoted to the study and analysis of substitution structures [4-6].

Today, these works, of course, have already gone beyond the DES cipher. Many new solutions for constructing encryption algorithms have been developed. To replace the DES cipher itself, the US has adopted a new encryption standard, AES (FIPS-197).

Naturally, advances in cipher construction technologies have led to improvements in cryptanalysis methods aimed at overcoming the stability characteristics incorporated in the cipher by its developers.

It remains to be noted that the issues of constructing more advanced encryption procedures and algorithms for cryptographic protection of information in general have not lost their relevance. The focus of cryptographers and mathematicians continues to be methods and algorithms for constructing new ciphers, including method for the generation of more advanced S-box designs.

To conclude the review of the literature, we will illustrate several examples of S-box construction in modern ciphers.

Thus, in the Rijndael cipher, S-boxes were chosen in a deterministic manner to ensure the minimum value of the differential and linear probabilities, resulting in the 128-bit cipher arriving in the random substitution state in three cycles. The 256-bit cipher requires four cycles to arrive in the random substitution state.

In the 256-bit Kalina cipher [7], byte S-boxes were selected through numerous experiments to obtain a nonlinearity indicator of 104 [8].

Another development is IDEA NXT cipher, which was born on the basis of the FOX cipher, recognized in due time as the leader in block symmetric encryption technologies. We will not focus on the description of this unique construction, but will focus on approaches to constructing S-boxes of the cipher. The developers of the S-boxes of this cipher note that their original intent was to prevent a purely algebraic construction of the S-box.

A secondary goal was the possibility of implementing the S-box in hardware efficiently using ASIC or FPGA technologies. The S-box function implemented by them is a nonlinear bijective mapping of 8-bit input values to 8-bit output values. It is constructed using a three-cycle Leigh-Massey scheme, where three different small (4×4 in size) substitutions are taken as the cycle function and combined using the modulo 2 addition operation. Small substitutions were chosen pseudo-randomly. Finally, the candidates were evaluated and tested against the values of the probability of passing the difference through the DP_{max} substitution and the probability of passing the linear approximation through the LP_{max} substitution to find the best candidate. The authors note that the selected resulting S-box has indicators $DP_{max} = LP_{max} = 2^{-4}$ (S-boxes of the AES have indicators $DP_{max} = LP_{max} = 2^{6}$).

The following requirements for S-boxes formation were substantiated in the process of developing the Mukhomor Block Symmetric Cipher:

− random generation (minimization of the probability to obtain strict mathematical dependencies between input and output bits);

− limiting the maximum value of the probability of passing the difference through the $DP_{max} = 2^{-5}$ substitution;

− limiting the maximum value of the probability of passing a linear approximation through the $LP_{max} = 2^{-4}$ substitution;

− nonlinear order of substitution 7.

Many other examples can be cited when developers pay too much attention to the selection of S-boxes for ciphers. These studies can be identified as a separate scientific direction in cryptology. In general, almost all known ciphers use selected S-boxes.

Today, however, our own concept (methodology) for assessing the resistance of ciphers to differential and linear cryptanalysis attacks has already been formulated, which will be developed in this work. This is partly given in the Introduction.

Extensive research into methods for designing and creating S-boxes has been conducted in this direction.

A review of recent publications reflects this issue [9 - 12]. In all papers, specific and rather complex methods for generating optimal S-box structures are proposed.

In the article [13] the authors themselves talk about the difficulty of the proposed method for generating S-boxes. The article [14] focuses only on the differential properties of S-boxes, which is clearly not enough. Articles [15] and [16] also offer quite complex and time-consuming algorithms for generating S-boxes.

However, we propose a different approach that eliminates the need for complex methods for generating S-boxes. We leave the use of selected substitution transformations and focus on random S-boxes.

In our work, we propose the use of random S-blocks in ciphers (without their degenerate constructions). It is shown that this does not in any way reduce the cryptographic strength of the cipher, which means that the scientific direction associated with the search for S-boxes with special properties becomes unproductive. Therefore, in article [17], this algorithm uses random S-boxes without reducing the cryptographic strength of the cipher. We will continue to develop this direction.

Let us try to generalize the results already achieved in this direction. It is proposed not only to develop new strong ciphers that use random s-boxes. Let us show that random s-boxes can be used in almost all known block symmetric ciphers without security degradation.

3. Materials and Methods

Our task is to show that the indicators of cipher stability are essentially independent of the indicators of S-boxes included in the ciphers.

Therefore, we proceed from the fact that the stability of the cipher is determined by the values of the maxima of the differential and linear probabilities of the total differentials and shifts of tables of linear approximations [1].

Let us recall here in more detail the essence of the proposed methodology for assessing the resistance of block symmetric ciphers to differential and linear cryptanalysis attacks.

All modern block symmetric ciphers undergo several cycles of encryption, regardless of the S-boxes used in the ciphers (of course, we are not talking about their degenerate constructions) according to combinatorial indicators (number of inversions, increments and cycles), as well as according to the laws of distribution of transitions of XOR tables of differences (of complete differentials) and the laws of the distribution of shifts of tables of linear approximations acquire the properties of random permutations.

As a result, the values of the maxima of total differentials and shifts of tables of linear approximations can be determined by calculation using the formulas for the laws of probability distribution of the XOR table transition and shifts of tables of linear approximations of random substitutions of the appropriate degree.

Simultaneously, the verification of the randomness indicators of large ciphers can be performed on the basis of the development and further analysis of the randomness indicators of reduced models, which allows computational experiments to be carried out in acceptable (real) terms.

Small cipher models that repeat their prototypes make it possible to estimate not only the average values of the maximum of tables of differential probabilities (AMDP) and the average values of the maximum of linear probabilities (AMLP) for a limited set of keys but also to solve the problem of determining (checking) the absolute value of the maximum on the full set of keys

The question arises about the influence of S-boxes on the dynamic indicators of the cipher arriving in the random substitution state. Let us try to answer this question.

As follows from the results of [1], the minimum number of cycles for a cipher to arrive in the state of random substitution is directly related to the differential and linear properties of S-boxes.

Let us begin our consideration with the mechanism (the process) of activating the sequence of S-boxes.

First let us pay attention to the fact that one of the popular indicators of S-boxes, which were considered in known publications when choosing them, is the maximum values of the differential and linear probabilities. They define the minimum number of cycles required for the cipher to arrive in the random substitution state.

However, the minimum number of cycles required by the cipher to arrive in a random substitution is influenced not only by the value of the maxima but also by their number.

Table 1 illustrates the dependence of the number of maxima occurring in the byte S-boxes on their values.

It follows from the presented data that for S-boxes with boundary (minimum) linear and differential indicators (S-boxes of the ADE, AES, GrandCru, Labyrinth and some other ciphers), the number of maximum values is large. The maximum is no less than the number of rows of tables of differential differences or shifts of tables of linear approximations. It is sufficient for constructing full differentials and shifts of tables of linear approximations on the first encryption cycles from S-boxes with the maximum possible transitions.

Table 1

Dependence of the number of maxima
on the values of the maxima for the substitution tables
of different ciphers

S-box ciphers	Max. DT	Number of maxima	Max. Lat	Number of maxima
ADE, AES, GrandCru, Labirynt	4	255	16	1275
Iseberg, Khazad	8	80	30	6
Mukhomor	8	90	30	8
Random	10 12	12 1	32 32	3 1
FOX	16	70	32	219

Simultaneously, for other ciphers (S-boxes of Iseberg, Khazad, Mukhomor ciphers and random substitutions) with values of differential and linear transitions of S-boxes that have transition maxima exceeding the maximum achievable minimum values, the number of these maxima is expressed in tens or even units (they are few). An exception is the S-boxes of the FOX cipher.

This means that when constructing differential and linear characteristics with such S-boxes, even transitions with non-maximum possible values will be used in most cases (there are very few maximum values).

Therefore, the real values of the probabilities of the differential and linear characteristics will be determined by a random set of transitions, in which transitions with lower probabilities participate, which will lead to a decrease in the required number of S-boxes to achieve the state of activated random substitution compared to the case of transitions with maximum probabilities.

Here, it would be appropriate to present the results of experiments performed using the Rijndael cipher model reduced to 16-bit input. The construction of this cipher can be found in [18].

Table 2 shows the values of the maximum total differentials for different S-boxes and the number of cycles of the Rijndael algorithm with the MixColumns operation for the entire text (per four half-bytes).

As follows from the presented results, in all cases, regardless of the maximum value of the XOR table of differences of p S-boxes, all ciphers reach the same average value of the maxima of the total differentials, which is characteristic of a random substitution of the corresponding degree.

Table 3 shows the variants of the used S-boxes. Some S-boxes are taken from well-known ciphers (half-byte S-boxes for the AES and Labyrinth ciphers are constructed according to the same rules as byte ones).

The first line of the first S-box of the DES cipher is taken as a half-byte S-box in the DES cipher. Other S-boxes are generated using a random substitution generator.

Table 2

Value of the maxima of the total differential for different S-boxes and the number of cycles
of the mini-Rijndael algorithm with the MixColumns operation for the entire text

Sbox r	Sbox, Rand *p*4, F2	Sbox. *p*4 Labirynt	Sbox AES, *p*4	Sbox *p*6, F0	Sbox *p*6, F2	Sbox DES, *p*8	Sbox *p*12, F0
1	16384.00	16384.00	16384.0	24576.00	24576.00	32768.00	49152.00
2	83.87	132.00	132.00	490.87	230.40	1152.00	5184.00
3	20.73	**19.47**	**18.80**	25.53	35.27	70.87	146.13
4	**19.60**	18.73	19.00	**19.20**	**18.93**	**19.27**	**19.07**
5	19.13	19.47	19.47	18.93	19.40	19.00	19.00

Table 3

Variants of the S-boxes used with decoding of their description

Variants of used S-boxes	Deciphering of the S-boxes description

SboxAES *p*4 ⇒{A,4,3,B,8,E,2,C,5,7,6,F,0,1,9,D};
SboxDES *p*8 ⇒{E,4,D,1,2,F,B,8,3,A,6,C,5,9,0,7} (the first line of the S-box S1 of the DES cipher);
Sbox *p*6 F2 ⇒ {B,C,5,0,1,3,2,7,8,4,D,F,6,9,E,A};
Sbox *p*6 F0 ⇒ {4,6,F,B,E,7,5,D,9,C,1,0,3,8,A,2};
Sbox *p*12 F0 ⇒ {8,3,1,9,A,B,E,C,5,D,F,2,0,4,7,6};
Sbox, Rand *p*4 F2 {D,E,B,5,4,2,1,F,0,9,6,A,7,C,8,3}, random;
Sbox *p*4 Labirynt ⇒{B,8,6,4,A,0,D,2,C,5,1,E,3,F,9,7}.
	*p*X – X is the maximum value in the S-box differential table;
	FY – Y is the number of fixed points $(S(x)=x)$.
	The absence of FY in the S-box description is equivalent to F0.

S-boxes with a minimum value of maximum, which is equal to 4, have only one cycle advantage over other S-boxes. Note that Table 2 contains a random substitution with a maximum of 4. This allows you to arrive in a random substitution state in four cycles.

Let us follow how the result is formed. For example, consider substitution

8 3 1 9 10 11 14 12 5 13 15 2 0 4 7 6. This permutation has a maximum element of the table of differences equal to 12, and only one such element. The differential table is given in Table 4.

Let us consider the first characteristic:

11→12→6→11→12→6→11→12→6→11→12→6→11→12→6→11→12.

For this characteristic for 9 active S-boxes, we have (for two cycles of the Rijndael cipher):

$$(12/16)^3 \times (1/4)^6 \le 2^{-12},\ 20\big/2^{16} = 2^{-12}.$$

Let us consider the following as the second characteristic:

11→12→5→9→6→11→12→5→9→6→11→12→5→9→6→11→12.

In this case

$$(12/16)^2 \times (1/4)^7 \le 2^{-14} \times 0.56\,.$$

To arrive at the state of random substitution, 9 S-boxes must be activated in two cycles with a resulting probability of at least $20\big/2^{16} = 2^{-11.67}$.

For the first characteristic, 9 S-boxes account for three transitions with a probability of $12\big/2^{-4}$ and 6 S-boxes with a probability of $4\big/2^{-4}$. As a result, we have the characteristic $(12/16)^3 \times (1/4)^6 \le 2^{-12}$.

For the second characteristic, 9 S-boxes account for two transitions with a probability of $12\big/2^{-4}$ and 7 S-boxes with a probability of $4\big/2^{-4}$. As a result, we have the characteristic $(12/16)^2 \times (1/4)^7 \le 2^{-14} \times 0.56$.

Consequently, each such characteristic satisfies the stated condition, but the overall result, judging by the results (see Table 1), allows the cipher to arrive in a random substitution in four cycles.

The S-box of the cipher in the first column of Table 2 has a transition maximum of 4, and there are 18 such fours in the Table, however, the cipher arrives in the random substitution state in four cycles. This effect can be explained by the fact that for this S-box, multiplication by an MDR matrix results in the activation of not 4, but a smaller number of non-zero outputs. As follows from the data of [10], the probability of activating the MDR transformation at the output of three half-bytes is 2^{-8}, and two half-bytes is 2^{-4} (here we have reduced proportionally the data of work [19] for half-bytes). Therefore, in this case, the event that required the number of activated S-boxes for the cipher to arrive in the random substitution state turned out to be more than 7).

Note also that even with a maximum value of more than 4, an event can occur in which even one such transition can be duplicated on all transitions of the differential characteristics. To achieve this, it is sufficient that this maximum transition is on the diagonal of the differential table.

Table 4

Differential table of S-box Sbox *p*12 F0

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	2	0	2	0	0	0	4	0	0	2	0	2	0	0
2	0	0	2	0	2	0	0	4	0	2	4	0	0	0	0	2
3	0	2	4	2	0	2	4	2	0	0	0	0	0	0	0	0
4	0	0	2	0	2	4	0	0	4	2	0	0	0	0	0	2
5	0	2	0	2	0	2	0	2	0	4	0	0	0	4	0	0
6	0	0	4	0	0	0	4	0	0	0	0	4	0	0	0	4
7	0	0	2	4	2	0	0	0	0	0	4	2	0	2	0	0
8	0	0	0	0	0	0	0	0	0	2	4	2	0	2	4	2
9	0	0	0	2	0	2	4	0	2	0	0	4	0	0	2	0
10	0	2	0	0	4	0	0	2	2	0	0	0	0	4	2	0
11	0	0	0	0	0	0	0	0	0	0	4	0	12	0	0	0
12	0	2	0	0	0	0	4	2	2	0	0	0	0	0	2	4
13	0	0	0	4	0	0	0	4	0	0	0	0	4	0	4	0
14	0	4	0	0	0	4	0	0	0	2	0	2	0	2	0	2
15	0	0	0	2	4	2	0	0	2	4	0	0	0	0	2	0

It would be appropriate here to provide the difference distribution for the XOR table and the transition distribution for the LAT table of random substitution. They are presented in Tables 5 and 6.

Therefore, random S-boxes can increase the number of cycles of cipher arrival in the random substitution state by one cycle. In most cases, this increase will not occur. We are talking about ciphers with a strong linear transformation (Rijndael-like ones and close to them). This means that they retain their strength with a large margin, considering the safety margin of ciphers.

Table 5
The distribution of pairwise differences for XOR Table of random substitution of degree 2^8

2k	Number of cells	Probability
0	39363	0.605345
2	19758	0.303855
4	4959	0.076263
6	830	0.0127609
8	104	0.0016014
10	10	0.0001608
12	1	0.0000134

Table 6
The distribution of transitions for LAT table of random substitution of degree 2^8

|2k|	Number of cells	Probability
0	6466	0.1988876
2	12538	0.192815
4	11424	0.1756848
6	9982	0.1504416
8	7872	0.1210626
10	5952	0.0915406
12	4228	0.0650312
14	2822	0.0433972
16	1768	0.0271986
18	1040	0.01600576
20	574	0.00884176
22	298	0.00458356
24	146	0.0022291
26	66	0.001016608
28	28	0.000434614
30	10	0.000174096
32	4	0.0000653134
34	2	0.0000305176

4. Experiments

To confirm the above, we present the results of experiments with extensive versions of ciphers. It was shown in [2] that reduced cipher models confirm the properties of large ciphers. Therefore, Table 7, taken from [2], demonstrates the per-cycle values of the maxima of the total differentials for the Rijndael cipher with different variants of S-boxes (substitutions).

Table 7
Cycle-by-cycle values of maxima of the total differentials for the Rijndael cipher with different variants of the S-boxes (substitutions)

Number of cycles	Substitutions					
	1	2	3	4	5	6
1	0	0	0	0	0	0
2	24	18	20	18	20	20
3	20	18	18	20	18	20
4	18	18	18	18	20	18
5	18	18	20	18	18	20
6	20	20	18	22	18	20
7	18	20	20	20	18	20
8	20	18	20	20	20	20
9	20	20	20	18	18	20
10	18	18	20	20	20	18
11	18	18	18	18	18	18
12	20	20	20	20	20	20
13	18	18	20	20	18	20

Note that in the experiments, tables were built for 16 bit differences at the input and output of a full-scale cipher. Differences were used for the 4th and 7th input and output bytes.

As a result, after the ShiftRows operation of the first cycle, the bytes changed their positions, and the 12th and 15th bytes with zero output differences and zero transition values were found on the cities of the 4th and 7th output bytes of the linear transformation.

Randomly generated 128-bit blocks are used as master keys. Number 1 in Table 7 shows the results for the Rijndael cipher using S-boxes corresponding to the standard substitution. The following columns show the differential characteristics of the cipher when random substitutions are used.

Table 8, borrowed from [2], shows the results of the linear indicator analysis of the Rijndael cipher with standard and random substitutions. The table shows that the laws of probability distribution, starting from the first cycle, are very close to each other.

The standard key deployment scheme was used in all cases. The general conclusion from the presented results is that random S-boxes provide differential indicators for ciphers that are practically not inferior to those of a cipher with "native" S-boxes selected according to special conditions. Therefore, it turns out that the "hunt" for S-boxes with improved cryptographic performance, which is actively conducted in the cryptographic literature, does not make sense. In both cases, the ciphers arrived in a random substitution state in two cycles. This reduced number of cycles is because we use ciphers of 16 bits. As we have already mentioned, the evidentiary stability for a sixteen-bit cipher is $20/2^{16}=2^{-12}$. In this case, large (byte) S-boxes are used. For example, for a differential table with a byte S-box transition indicator equal to 2^{-6}, two active S-boxes are sufficient for the cipher to arrive in the random substitution state.

Table 8

Cycle-by-cycle distributions of maxima of shifts tables of linear approximations for the Rijndael cipher using various substitutions

Number of cycles	Standard substitution	Random substitution
1	11264	10752
2	852	804
3	807	812
4	805	812
5	843	796
6	874	800
7	808	806
8	876	824
9	810	815
10	817	840
11	840	827
12	811	843
13	818	811

Tables 7 and 8 clearly show that the distribution laws of transition probabilities of differential tables for different numbers of encryption cycles, both for substitution according to the specification of the Rijndael cipher, and for a random selected substitution, almost starting from the first cycle, are very close to each other.

Random S-boxes along with the mechanism of linear mixing of their outputs, used in the Rijndael cipher, are able to create an encryption function that makes it possible to effectively realize its convergence to random substitution indicators. The materials of work [2] indicate that other modern ciphers also demonstrate the noted property.

5. Discussion of the results

The presented results confirm that the stability indicators of ciphers do not significantly depend on the indicators of the S-boxes included in the ciphers.

Indeed, S-boxes perform the main function of encryption transformation, namely, mixing bits of text. The dynamic characteristics of the cipher’s arrival in the state of random substitution depend on its effectiveness. Modern ciphers use nonlinear substitution transformations as S-boxes (most ciphers use byte substitutions). It turns out that it is not the individual properties of substitutions, but the results of their sequential interactions that are of crucial importance for achieving stability indicators. We recall here that the product of substitutions (their sequential execution one after another) gives a random substitution [2]. The individual properties of the output substitution are lost.

The properties of accidence inherent in S-boxes are sufficient to ensure that the influence on the dynamic indicators of the cipher arrival in the state of random substitution remains within one cycle.

Therefore, the price for the transition to random substitutions is an increase by one cycle in the number of cycles of the cipher arriving in random substitution, and this is against the background of the stability margin used in modern ciphers (the number of encryption cycles is chosen three to four times more than the depth of the avalanche effect, i.e., the minimum number of cycles of the cipher’s arrival in the random substitution state) is hardly noticeable. Another thing is that it is possible to construct ciphers that, even with random substitutions, do not require an additional encryption cycle, but this is a separate discussion.

Conclusions

This work is a generalization of previously performed studies. The result of such a generalization is a scientific position, which can be described as follows: random S-boxes can be used without reducing security in all known modern block symmetric ciphers. In the process of substantiating this provision, a large complex of theoretical and experimental studies of the randomness indicators of modern block symmetric ciphers were conducted using various S-boxes Numerous experiments were conducted on block symmetric ciphers of various typical designs (Feistel's construction, Ley-Massey, SPN).

It is shown that random S-boxes can increase one cycle in the number of cycles of the cipher coming to the state of random substitution. In this case, we are talking about ciphers with a strong linear transformation. In most cases, this will not happen. If we consider the security margin of modern ciphers, one extra cycle will not affect the security of the cipher at all.

A further direction of research is seen in the comparison of the cryptographic performance of block symmetric ciphers using random S-boxes and S-boxes generated using special methods. The speed and labor advantages are obvious when using random S-boxes.

Another possible direction is the development of the mathematical theory of random substitution by introducing additional indicators of randomness.

Contribution of authors: concept and methodology of research development – **Iryna Lysytska**; development of a software complex for testing models – **Kostiantyn Lysytskyi**; selection and use of software and technical tools for modeling and presentation of results – **Oleksii Nariezhnii**; comparison of the obtained results of theoretical models with the results of the software complex, formation of conclusions – **Tetiana Hrinenko**.

All authors have read and approved the published version of this manuscript.

References

1. Dolgov, V. I., Lisitska, I. V., & Lisitskiy K. Ye. The new concept of block symmetric ciphers design. *Telecommunications and Radio Engineering*, 2017, vol. 76, no. 2, pp. 157–184. DOI: 10.1615/ TelecomRadEng.v76.i2.60.

2. Dolgov, V. I., & Lisitska, I. V., 2013. *Blochnye simmetrichnye shifry. Metodologiia otsenki stoikosti k atakam differentsialnogo i lineinogo kriptoanaliza*. [Block symmetric ciphers. Methodology for assessing the resistance to differential and linear cryptanalysis attacks]. Kharkiv, Fort Publ., 2013. 456 p.

3. Lisitskaya, I. V., Melnychuk, E. D., & Lisitskiy, K. E. Importance of S-Blocks in Modern Block Ciphers. *International Journal of Computer Network and Information Security*, 2012, vol .4, no. 10, pp. 1-12. DOI: 10.5815/ijcnis.2012.10.01.

4. Lambić, D., & Živković, M. Comparison of random S-box generation methods. *Publications de L'institut Mathematique Nouvelle série*, 2013, vol. 93, iss. 107, pp. 109-115. DOI: 10.2298/PIM1307109L.

5. Ruisanchez, C. P. A new algorithm to construct S-boxes with high diffusion. *International Journal of Soft Computing, Mathematics and Control (IJSCMC)*, 2015, vol. 4, no. 3, pp. 41-50. DOI: 10.14810/ijscmc. 2015.4303.

6. Kuznetsov, O. O., Gorbenko, Yu. I., Bilozertsev, I. M., Andrushkevych, A. V., & Narizhnyi, O. P. Algebraic immunity of non-linear blocks of symmetric ciphers. *Telecommunications and Radio Engineering*, 2018, vol. 77, no. 4, pp. 309-325. DOI: 10.1615/TelecomRadEng.v77.i4.30.

7. *DSTU 7624:2014. Informatsiyni tekhnolohiyi. Kryptohrafichnyy zakhyst informatsiyi. Alhorytm symetrychnoho blokovoho peretvorennya* [DSTU 7624:2014, 2015. Information Technology. Cryptographic protection of information. Algorithm of symmetric block transformation]. Kyiv. Derzhspozhivstandard of Ukraine Publ., 2015. 238 p.

8. Rodinko, M. Yu, Oliynykov, R. V., & Hrinenko, T. O. Improvement of the method the optimal S-boxes generation. *Applied Radio Electronics*, 2015, vol. 14, no. 4, pp. 315-320. Available at: http://openarchive.nure.ua/handle/document/6469. (accessed 3.12.2022).

9. Lambić, D. S-box design method based on improved one-dimensional discrete chaotic map. *Journal of Information and Telecommunication*, 2018, vol. 2, iss. 2, pp. 181-191. DOI: 10.1080/24751839.2018.1434723.

10. Farhan, A. K., Ali, R. S., Yassein, H. R., Al-Saidi, N. M. G., & Abdul-Majeed, G. H. A new approach to generate multi S-boxes based on RNA computing. *International Journal of Innovative Computing, Information and Control*, 2020, vol. 16, no. 1, pp. 331-348. DOI: 10.24507/ijicic.16.01.331.

11. Sani, H. R., Behnia, S., & Akhshani, A. Creation of S-box based on a hierarchy of Julia sets: image encryption approach. *Multidimensional Systems and Signal Processing*, 2022, vol. 33, no. 1, pp. 39-62. DOI: 10.1007/s11045-021-00786-9.

12. Cassal-Quiroga, B. B., & Campos-Cantón, E. Generation of dynamical S-boxes for block ciphers via extended logistic map. *Mathematical Problems in Engineering*, 2020, vol. 2020, article no. 2702653, pp. 1-12. DOI: 10.1155/2020/2702653.

13. Kuznetsov, A., Wieclaw, L., Poluyanenko, N., Hamera, L., Kandiy, S., & Lohachova, Y. Optimization of a Simulated Annealing Algorithm for S-Boxes Generating. *Sensors*, 2022, vol. 22, iss. 16, article no. 6073. DOI: 10.3390/s22166073.

14. Marochok, S., & Zajac, P. Algorithm for Generating S-Boxes with Prescribed Differential Properties. *Algorithms*, 2023, vol. 16, iss. 3, article no. 157. DOI: 10.3390/a16030157.

15. Isa, H., Junid, S. A. A. S., Z'aba, M. R., Endut, R., Ammar, S. M., & Ali, N. Enhancement of Non-Permutation Binomial Power Functions to Construct Cryptographically Strong S-Boxes. *Mathematics*, 2023, vol. 11, iss. 2, article no. 446. DOI: 10.3390/math11020446.

16. Alsaif, H., Guesmi, R. Kalghoum, A., Alshammari, B. M., & Guesmi, T. A Novel Strong S-Box Design Using Quantum Crossover and Chaotic Boolean Functions for Symmetric Cryptosystems. *Symmetry*, 2023, vol. 15, iss. 4, article no. 833. DOI: 10.3390/sym15040833.

17. Lisickiy, K., Dolgov, V., Lisickaya, I., & Kuznetsova, K. Block Symmetric Cipher with Random S-boxes. *International Journal of Computing*, 2019, vol. 18, iss. 1, pp. 89-100. DOI: 10.47839/ijc.18.1.1278.

18. Evseev, S. P., Ostapov, S. E., & Korolev, R. V. *Ispolzovanie mini-versii dlia otsenki stoikosti blochno-simmetrichnykh shifrov* [Using mini-versions to assess the strength of block-symmetric ciphers]. *Ukrainian Scientific Journal of Information Security*, 2017, vol. 23, no. 2, pp. 100-108. DOI: 10.18372/2225-5036.23.11796.

19. Ruzhentsev, V. I. *Proverka metoda dokazatelstva stoikosti blochnykh shifrov k atake nevypolnimykh differentsialov* [Verification of a method for proving the resistance of block ciphers to the attack of impracticable differentials]. *Applied Radio Electronics*, 2016, vol. 15, no. 3, pp. 184-190. Available at: http://nbuv.gov.ua/UJRN/Prre_2016_15_3_10 (accessed 26.12.2022).

Received 26.12.2022, Accepted 20.09.2023

ПРО ВПЛИВ S-БЛОКІВ НА ПРИХІД ШИФРІВ ДО СТАНУ ВИПАДКОВОЇ ПІДСТАНОВКИ

Ірина Лисицька, Костянтин Лисицький, Олексій Нарєжній, Тетяна Гріненко

Предметом дослідження є розробка блокових симетричних шифрів з поліпшеними показниками криптографічної стійкості для вирішення завдань захисту інформації в інформаційно-комунікаційних системах. **Метою** є розробка математичної моделі оптимальної s-блокової конструкції (блока нелінійної заміни) для сучасних блокових симетричних шифрів. **Завдання:** показати, що стійкість блокових симетричних шифрів суттєво не залежить від показників s-блоків, що входять в ці шифри; обґрунтувати використання без зниження стійкості випадкових підстановок у якості s-блокових конструкцій сучасних блокових симетричних шифрів; довести безперспективність пошуку s-блоків з особливими властивостями. Використовуваними **методами** є: методи теорії ймовірностей; математичної статистики; комбінаторики і системного аналізу; методи статистичних випробувань; методи булевої алгебри. Отримані такі **результати.** У сучасних шифрах в якості S-блоків використовуються нелінійні підстановочні перетворення (в більшості шифрів байтові підстановки). S-блоки виконують головну функцію шифруючого перетворення – перемішування бітів тексту. Від їхньої ефективності залежать динамічні показники приходу шифру до стану випадкової підстановки. Представлені результати підтверджують, що показники стійкості шифрів суттєво не залежать від показників S-блоків, що входять в шифри. Вирішальне значення для досягненні показників стійкості мають не індивідуальні властивості підстановок, а результати їхньої послідовної взаємодії. **Висновки.** Наукова новизна отриманих результатів полягає в наступному. Робота представляє собою узагальнення результатів наукових досліджень переходу до використання у якості S-блоків випадкових підстановок. При переході відбувається збільшення всього на один цикл числа циклів приходу шифру до стану випадкової підстановки, а це на тлі запасу стійкості, що використовується в сучасних шифрах, є мало помітним. Результатом цього узагальнення є наукове положення, що можна сформулювати таким чином: во всіх відомих сучасних шифрах без зниження стійкості можна використовувати випадкові S-блоки. Тобто задача пошуку S-блоків з особливими властивостями втрачає будь який сенс, а це означає, що науковий напрям, пов'язаний з пошуком S-блоків з особливими властивостями, виявляється зайвим.

Ключові слова: S-блок; критерій випадковості; підстановка; повний диференціал; таблиця диференціальних різниць; таблиця лінійних апроксимацій.

Лисицька Ірина Вікторівна – д-р тех. наук, проф., проф. каф. безпеки інформаційних систем і технологій, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

Лисицький Костянтин Євгенійович – канд. техн. наук, старш. викл. каф. штучного інтелекту та програмного забезпечення, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.

Нарєжній Олексій Павлович – канд. техн. наук, доц. каф. безпеки інформаційних систем і технологій, Харківський національний університет імені В. Н. Каразіна, Харків, Україна.

Гріненко Тетяна Олексіївна – канд. техн. наук, доц., доц. каф. безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна.

Iryna Lysytska – Doctor of Technical Sciences, Professor, Professor of Information Systems and Technologies Security Department, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: ivlisitska@karazin.ua, ORCID: 0000-0001-6758-9516, Scopus Author ID: 57201720899.

Kostiantyn Lysytskyi – PhD, Senior Lecturer of Artificial Intelligence and Software Department, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: constantin@karazin.ua, ORCID: 0000-0002-7772-3376, Scopus Author ID: 57201719901.

Oleksii Nariezhnii – PhD, Associate Professor of Information Systems and Technologies Security Department, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: o.nariezhnii@karazin.ua, ORCID: 0000-0003-4321-0510, Scopus Author ID: 57201777102.

Tetiana Hrinenko – PhD, Associate Professor, Associate Professor of Information Technologies Security Department, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine,
e-mail: tetiana.grinenko@nure.ua, Scopus Author ID: 57190444905.