Cryptographically Properties of Random S-Boxes

Konstantin Lisitskiy [1[0000-0002-7772-3376]],
Irina Lisitska [1[0000-0001-6758-9516]], Alexandr Kuznetsov [1 [0000-0003-2331-6326]]

Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
constantin.lisickiy@gmail.com, lisitskaiv@ukr.net, kuznetsov@karazin.ua

Abstract. The results of studies of the properties of random permutations carried out with the participation of the authors are generalized. It is shown that random substitutions overwhelmingly have good cryptographic, and in particular, algebraic properties. The prospects of using random S-blocks to build block symmetric ciphers with improved dynamic rates of arrival to random substitution are substantiated. A refined model of random substitution and the corresponding criteria are proposed, with the help of which one can verify the suitability of substitutions generated randomly for use in modern cipher designs. It is a check, since with a very high probability the checked substitutions will be suitable.

Keywords: algebraic properties of S-blocks, Boolean functions, cryptanalysis, random S- boxes, algebraic immunity of S-boxes, algebraic degree of S-boxes, dynamic indicators of a cipher, model of random substitution

1 Introduction

In accordance with the new methodology for assessing the strength of symmetric block ciphers, developed in [1], BSC strength indicators are independent of S-blocks included in the cipher cyclic functions. Substitution transformations (S-blocks) affect only the number of cycles the ciphers arrive at the state of random substitution, and then only within, as a rule, one cycle. A huge number of publications devoted to the construction of S-blocks with high cryptographic performance are aimed at practically winning one cycle in the encryption procedure and increasing other cryptographic performance of ciphers according to the authors' assumptions. In particular, they strive to apply S-blocks with the smallest possible values of differential and linear probabilities (random S-blocks have increased values of differential and linear probabilities and therefore require an additional cycle to arrive at a random substitution).

It turns out that the used constructions of cycle functions provide activation on the first cycles of far from the whole set of S-blocks.

We also note that in accordance with the new methodology for assessing the strength of block symmetric ciphers, all ciphers after several initial encryption cycles, regardless of the S-blocks used, become random substitutions: For example, Rijndael-128 comes to the state of random substitution for four cycle [2].

A natural question arises. And why all this colossal work on the selection and construction of “optimal” S-blocks, if as a result, in all cases, regardless of the S-blocks used, the same result is obtained (the same values of the maximums of differential and linear probabilities are obtained)?

Thus, it turns out that the price of using S-blocks with special properties is actually reduced only to reducing the number of cycles of arrival of ciphers to the state of random substitution (for one cycle). Other special indicators are also leveled when ciphers acquire random substitution properties.

So the idea came up to build an encryption transformation (cipher) with more efficient cyclic functions, allowing increasing the number of activated S-blocks in the first cycles in comparison with traditional methods and thereby switch to using random S-blocks in ciphers without any loss of strength any significant selection. In fact, we are talking about using S-blocks directly from the output of the random permutation generator.

This idea was implemented in the SHUP cipher (our work [3]). The loop function in this cipher is constructed using controlled settings. In this case, the substitution of the cyclic function is connected in a chain, so that the sum of two current segments of the input (folded with the corresponding segment of the cyclic key) and the output of the previous S-block is fed to the input of the current S-block, and the output of the last S-block modulo two with the output of the first or all previous S-blocks.

As a result, the definition of the very concept of a random S-block becomes relevant and evaluations of its cryptographic performance.

2 Formulation of the problem

In our works, we have long turned to the study and discussion of approaches to the design of S-blocks with high cryptographic indicators and ourselves conducted searches and studies in this direction. Note that to date; we can already count a huge number of publications devoted to this problem [4-6] and many others. There is simply not enough space to mark them. An approach based on algebraic methods for describing such constructions can be considered the most developed.

The analysis performed in our work [7-9] and others showed that, despite the beautiful mathematical apparatus that allows us to carry out a rigorous justification of a number of properties of the constructed S-blocks, the proposed approaches either give solutions oriented to certain classes of ciphers (for example, DES-like), often not without weaknesses, or turn out to be quite difficult for practical implementation, not to mention their inherent limitations. For example, the method works only for odd-degree S-blocks or for asymmetric S-blocks. Moreover, it is practically impossible to build S-blocks with simultaneously high all the indicators noted above. For a number of them, the constructed S-blocks are far from optimal.

In our works (here you can point to a work of a generalizing nature [7,9]) at the time, a different approach to the construction (selection) of suitable S-blocks was justified, based on the selection of random permutations using a system of criteria. In our subsequent studies of the properties of random permutations [10-11, etc.], this approach was further developed.

In this work, the task is to summarize the available information on random permutations and justify the prospects of their use in constructing symmetric block ciphers with improved dynamic rates of arrival at random permutations.

3 Literature review

It should be noted that there are practically no foreign publications devoted directly to random S-blocks in Google. There are only publications with our participation [7-9] and work with references to the use of random permutations in ciphers. The bulk of the work is the work devoted to the methods of forming S-block structures with improved cryptographic indicators [12-14] and many others. In work [15], a large number of publications in this direction were analyzed in sufficient detail. In the cited works, new techniques for the formation (construction) of S-blocks with improved cryptographic indicators are considered, and there are even works on the selection of random substitutions using a system of criteria close to our proposals. Only all the same, in these works we are talking about the selection of permutations according to strict criteria. And we will be talking about checking (control) substitutions from the output of the random substitution generator, and our criteria will be significantly milder than the proposed ones. Returning to the results of the analysis of the results of the noted works, we will again use the materials of [7], which fix our position at the time of their implementation. They come down to the following:

1. The current approaches to the construction of S-blocks for symmetric block ciphers are primarily aimed at ensuring minimum values of the differential $DP_{\max}$ and linear probabilities $LP_{\max}$. And in this direction significant success has been achieved. S-block constructions with limit and theoretically minimum possible values of $DP_{\max}$ and $LP_{\max}$ close to them were implemented.

2. There is a thoroughly developed apparatus for evaluating cryptographic indicators (properties) of Boolean functions, with the help of which you can describe the transformations carried out by S-blocks. The approaches and rules by which the resulting cryptographic indicators of individual Boolean functions included in

S-block can be converted into indicators of the entire transformation (S-block) as a whole. Although very much attention is paid in the literature to the development and application of Boolean functions of the mathematical apparatus of the mathematical apparatus of S-blocks for evaluating cryptographic indicators, nevertheless, this algebraic approach for S-block constructions actually used in ciphers has not become decisive. Moreover, the S-block constructions used in modern ciphers have far from the best in some indicators, and in some of them even low cryptographic properties of the Boolean functions included in them. Therefore, the main (main) indicators are actually optimized, to the detriment of the secondary ones. These basic indicators include the values of the maxima of the differentials and displacements (δ-uniformity and non-linearity), as well as the values of the algebraic degree and, more recently, the values of algebraic immunity.

If the values of the maxima of the differentials and displacements (δ-uniformity and non-linearity) can be determined without the apparatus of Boolean functions, then the last two indicators, algebraic degree and algebraic immunity, already require the use of the mathematical apparatus of Boolean functions.

3. The results obtained indicate that "good S-blocks (S-blocks with high cryptographic indicators), at least with respect to the main group of the marked criteria), as a rule, can be obtained by exhaustive search methods for S-blocks of degree 256 (byte S-blocks) is very difficult (requires significant computing resources). Therefore, all real developments to build large (byte) S-blocks were initially based on methods that could most likely be considered regular. So in our works of that time it is noted that the use of separate sentences available in publications, in particular, proposals of K. Nyberg [13], looks more progressive for building S-blocks. They found practical application in designs

S-blocks used to create many modern block symmetric ciphers (Rijndael, Camellia, ADE, Labyrinth and some others). In the IDEA NXT cipher, we took the path of building byte S-blocks based on the use of a three-byte composition -blocks, followed by the selection of the best candidate and the like. The elapsed time has made adjustments to the current state of the issue. The time has shown that random S-blocks really deserve more serious attention, as was noted above.

It is worth recalling here that when developing the new standard of Ukraine for the Kalina cipher, the developers have already taken the path of using S-blocks selected from randomly generated permutations with higher non-linearity indicators compared to Rijndael ciphers.

We supplement these conclusions with one more.

4. The experiments performed show that almost all S-blocks used in modern ciphers do not fit into the frames of S-blocks of a random type.

Our interest is focused on using directly randomly generated S-blocks in block symmetric ciphers without any restrictions. The developed approach is based on ideas from [1], devoted to the development of a new methodology for assessing the resistance of block symmetric ciphers to attacks of differential and linear cryptanalysis.

The main result of research in this direction was the substantiation of the position that the resistance indicators of modern block symmetric ciphers to attacks of differential and linear cryptanalysis do not depend on the properties of the used S-blocks (with the exception of their degenerate structures). S-block indices influence even within a single cycle the minimum number of cycles the cipher arrives at the state of random substitution (to the stationary values of the maximums of the differential and linear probabilities of the cipher).

The central point of the developed approach is the construction of new constructions of cyclic functions of block symmetric ciphers, which allow increasing the number of activated S-blocks in the first encryption cycles [3] and others. It is the increase in the number of activated S-blocks in the first cycles that allow substitution structures of a random type to be used in ciphers without decreasing the strength. In this work, it is supposed to describe the main stages of the birth of the methodology for using random S-blocks when constructing ciphers and defining the concept of random substitution.

4. A brief overview of our results.

This section contains materials on the justification (study) of the properties of random permutations and methods (criteria) for their selection, obtained with the participation of the authors of this work. Materials are combined under the general idea of forming a random substitution model.

The following are extracts from our work.

We first recall the results of studying the laws of the distribution of inversions, increases and cycles of random permutations of degree $n \geq 4$ and reduced to 16-bit inputs of models of modern ciphers (our works [16]). It was found that they are distributed in accordance with the theory of random permutations according to the normal laws of probability distribution with corresponding numerical characteristics determined by the degrees of permutations [17].

On the basis of these results, the concept of random permutation was introduced, which was associated with checking the correspondence of combinatorial exponents of substitutions (the number of inversions, increases, and cycles) with the numerical characteristics of the asymptotic distribution laws of these exponents for random permutations [7,9,18].

Next, the distribution laws of differential and linear exponents of permutation transformations [19,20] were established with a refinement [21]. We recall here the theorems proved in [20-21] that determine the distribution laws of transitions XOR of random permutation tables and the distribution laws of displacements of linear approximation tables of random permutations. From the work [19]:

Statement 1. *For any non-zero fixed* ΔX *,* $\Delta Y \in Z_2^m$*, assuming that the substitution π is chosen equally from the set* S_2^m и $1 \leq k \leq 2^m - 1$*,*

$$\Pr\left(\Lambda_\pi(\Delta X, \Delta Y) = 2k\right) = \begin{pmatrix} 2^{m-1} \\ k \end{pmatrix}^2 \cdot \frac{k! \cdot 2^k \cdot \Phi(2^{m-1} - k)}{2^m\,!}, \tag{1}$$

where the function $\Phi(d)$ *is determined by the expression*

$$\Phi(d) = \sum_{i=0}^{d} (-1)^i \cdot \begin{pmatrix} d \\ i \end{pmatrix}^2 \cdot 2^i \cdot i! \cdot (2d - 2i)!\,. \tag{2}$$

Here, ΔX and ΔY – are the input and output differences of the encryption conversion.

In [22] it is shown that formulas (1) and (2) correspond to an approximation in the form of a Poisson law of probability distribution of XOR transitions of tables of random substitutions:

$$\Pr\left(\Lambda_{\pi}(\Delta X,\Delta Y)=2k\right)=e^{-1/2}\cdot\frac{1}{2^{k}\cdot k!}.$$

From our work [20]:

Theorem 1: *Let* $\lambda(\alpha,\beta)$ *be a random number that corresponds to the value of the cells of the linear approximation table of the substitution when the substitution* π *is chosen equally from the set* S_2^n *and the mask* α,β *nonzero. Then* $\lambda(\alpha,\beta)$ for whole values of k , $0\le k\le 2^{n-1}$ *it takes only even values and the probability* $\lambda(\alpha,\beta)=2k$ *determined by the expression*

$$\Pr\left(\lambda(\alpha,\beta)=2\,k\right)=\frac{\left(2^{\,n-1}!\right)^{2}}{2^{n}\,!}\cdot\binom{2^{n-1}}{k}^{2}. \tag{3}$$

In the robot [23], it is shown that formulas (3) are approximated by the normal law, which can be considered Theorem 3 of the robots. Here you will go for number 2.

Theorem 2: *For a random n-bit substitution* with $n \geq 5$ the imbalance Imb (v, u) o*f the approximation is a random value with a distribution that can be approximated as*

$$\Pr(\mathrm{Imb}(v,\,u)=\mathrm{z})\approx\ 2Z\left(\frac{z}{2^{(n-2)/2}}\right) \tag{4}$$

for z even and zero for z odd

If we substitute $z = 2x$ in (4), then it can be rewritten as

$$\Pr(\mathrm{Imb}(v,\,u)=2x)\approx Z\left(\frac{x}{2^{(n-4)/2}}\right),$$

that is, the imbalance Imb(v, u) = z at z = 2k corresponds to the value of the cell in the LAT table $\lambda(\pi)=2k$

On the basis of these results, a model of random substitution was substantiated and studied in the form of a set of criteria for the proximity of combinatorial indices, as well as the laws of the distribution of transitions of differential and displacement tables of linear approximations of substitutions to the standard ones, which were considered by the corresponding laws of random substitutions [24].

Much attention has been paid to the use of algebraic methods for describing substitution transformations using the Boolean mathematical apparatus. In particular, the algebraic indices of the S-blocks of most known ciphers were determined.

As a result, was concluded that, although in the modern literature, much attention is paid to the development and application for the estimation of cryptographic indices of S-blocks of algebraic methods based on the mathematical apparatus of Boolean functions, nevertheless, this algebraic the approach for many known S-block designs has not been decisive. Moreover, the S-block constructions used in modern ciphers do not have much better, but rather a number of indicators and rather low cryptographic properties of Boolean functions included in them. The real designs of S-blocks are built, rather, on the basis of indicators that can be determined (calculated) without the involvement of the Boolean function apparatus (although there is a direct relationship of some of these indicators with the properties of Boolean functions of S-blocks).

It turned out that the use of substitutions selected using the developed randomness criteria did not lead to any noticeable advantages.

Finally, we note the work on the construction of laws for the distribution of maxima of XOR table transitions and offsets of linear approximation tables [25,26]. For the byte substitutions, the corresponding extremal log-Weibull distributions were constructed. Using them, the values of the maxima of the differential tables and the offsets of the linear approximations of the byte random substitutions were substantiated. For differential tables of byte substitutions, the values of the maxima that occur most times are 8-10, and for the linear approximation tables it is 32-34.

However, it was not possible to find any particular advantages of substitutions selected with even rigid criteria used. By their cryptographic index, which are determined by known methods, including algebraic, they are not particularly distinguished against the background of other known structures. Therefore, all considered criteria for the selection of random substitutions in the submitted version had to be abandoned.

We then conclude that the Boolean function of the Boolean function is poor in relation to the use of S-blocks in modern ciphers.

Today, however, it can be noted that S-blocks of the Kalina-2 cipher, and some other modern ciphers, as the developers themselves noted, were chosen from random substitutions. S-blocks with high nonlinearity (125) and high algebraic immunity of 3 [27] have been sought, that is, the use of the Boolean algebra mathematical apparatus and is now receiving much attention when evaluating the cryptographic indices of S-blocks.

5. Algebraic indicators of random S-blocks.

However, we have chosen another way to choose S-blocks to use in ciphers. So, in the end, we move to a more refined mathematical model of random substitution, built on the properties of a sample of random substitutions (this model incorporates the found differential and linear laws of the distribution of transitions of the corresponding substitution tables) and constructed the extremal distributions of the XOR tables of transitions.

Therefore, attention is further focused on the use of random substitutions in the ciphers, that is, directly S-blocks from the output of the random substitution generator. It will be shown that they are likely to have good cryptographic performance from the list above.

The studies performed so far [3] have indeed proved that the deterioration of the differential and linear parameters of the S-blocks used in the ciphers can be compensated by the increase in the minimum number of activated S-blocks on their first cycles. In particular, the design of a cipher is proposed, whose cycle function is built using large-scale controlled S-blocks, called SL transforms, which allow activating almost all S-blocks of the second and subsequent cycles [3]. It is shown that due to this, the cipher and with random S-blocks becomes a random substitution on the differential and linear indices on the third cycle (128-bit Rijndael becomes a random substitution on the differential and linear indices on the fourth cycle [2]).

However, some experts object to the use of random S-blocks in ciphers; they believe that accidentally taken S-blocks will not guarantee high resistance to algebraic cryptanalysis methods, and therefore in the cryptographic literature the task of finding S-blocks with high cryptographic indicators are allocated in a separate direction for improving the ciphers. The question arises whether the indicators of algebraic immunity and algebraic degree of random S-blocks to the conditions for ensuring high rates of stability of modern ciphers? Is there a correlation between these indicators?

Some answers to our questions were found in the publication of the journal "Discrete Mathematics" [28]. From the article cited in this edition, A.A. Horodilov, dedicated to the presentation of Boolean properties and their relation to the methods of cryptanalysis, we want to highlight a few theorems (results), which are given below.

A mess about the non-linear functionality of functions. In the designations of robots [28] Theorem 6. Here you will go after number 3.

Theorem 3. (nonlinearity of the random function N_f). *There is a constant* c < 1 *such that for almost all Boolean functions f of n variables, the condition holds* $N_f \geq 2^{n-1} - 2c\sqrt{n}2^{n/2-1}$.

For example, for n = 8, c < 0.7 is obtained $N_f \geq 128 - 32$. The most probable nonlinearity of a random byte S block obtained in experiments is 128 – 34.

It is known that the nonlinearity of an arbitrary balanced function is the case, finding specific functions with high nonlinearity is a nontrivial problem. Use some kind of time-bound very complex methods o $N_f \leq 2^{n-1} - 2^{n/2-1}$ – 2. For n = 8 it turns out $N_f \leq 118$, but it is noted in [28], as is often f constructing such functions (methods of Sebery, K. Nyberg and others [1]). Today, we are following the path of filtering (selecting) random S-blocks using sufficiently large computing resources.

Our position is to find out that we want to realize realizable boundary values of the linear (that differentiation) levels of the LAT table, and also the XOR table does not require (recall that nonlinearity is uniquely related to the maximum offset value of the LAT table). Numerous experiments have shown that when stocked among the activated S-blocks in the first cycles, you can use randomly generated S-blocks in ciphers, even without checking their properties. A non-trivial task becomes trivial. As for other indicators of the main group of criteria, they remain at an acceptable level for random S-blocks, judging by the results of experiments. As for the other indicators of the main group of criteria, they remain at an acceptable level according to the results of the experiments for random S-blocks.

Let us focus, for example, on indicators of algebraic immunity of chance S-blocks. The cited work provides such well-known facts.

It is noted that the algebraic degree $\deg f$ is a natural upper bound for the algebraic immunity of the AI Boolean function f In addition, the following upper bound of algebraic immunity depends on the number of variables *n* of the Boolean function. This is Theorem 11 in [28]. Here she will go to number 4.

Theorem 4. (top estimate for AI). *For an arbitrary Boolean function f from n variables, the condition* $\mathrm{AI}(f) \le \lceil n/2 \rceil$, *where де* $\lceil k \rceil$ *– is an integer part of the number k is satisfied.*

It is known that this estimate is achievable. For *n* = 8, AI(*f*) ≤ 4 is obtained.

Although there are examples of functions with maximum algebraic immunity, it is known that this class of functions is very small. However, an interesting fact is that the algebraic immunity of arbitrary (random) function is quite high.

We also give Theorem 13 from [28]. Here she will go to number 5.

Theorem 5. (AI of a random function). *For any* $\alpha < 1$ *and for almost all Boolean functions of n variables, the condition is satisfied* $\mathrm{AI}(f) > n/2 - \sqrt{n/2 \cdot \ln(n/(2\alpha \ln 2))}$.

For *n* = 8, *α* = 0.7, AI(*f*) > 4–2,9 = 1,1 is obtained.

Theorem 14 of [28] gives a known exact lower estimate of the nonlinearity of a function due to its algebraic immunity. Here she will go to number 6.

Theorem 6. (link AI and N_f). The Boolean function *f* of *n* variables is a fair estimate.

$$N_f \ge 2 \sum_{i=1}^{\mathrm{AI}(f)-2} C_{n-1}^{i} .$$

For *n* = 8, it turns out $N_f \ge 58$.

Unfortunately, the results appear to be very blurred, but we could not find anything more specific.

In [28], a very important conclusion is drawn for us: the theoretical results show that in a *random Boolean function, most cryptographic parameters are close to optimal ones*.

6. Experiments

Above it is established that the distribution of even differences of random substitutions obeys Poisson law, and the displacements of the linear approximation tables are normal. Here are the results of the estimation of the randomness indices of the byte S-blocks from the output of the random permutation generator obtained by calculation and experimentally.

Table 1 shows the distribution of maximum values for the 256 bit substitutions calculated using the theoretical law of the distribution of the values of the XOR maxima of the sampling differences obtained in our work [3], and the results of the experiment.

Table 1. The distribution of the values of the maximums of the sample XOR differences of the substitutions of degree 2^8 obtained by calculation and experimentally

k^* (X_1, X_2)	Pr(k^*)	Estimated value Experiment	Estimated value Experiment
8	0,00004	0,01	0
10 (10,8)	0,368 – 0,00004 = 0,368	94	92
12 (12,10)	0,905 – 0,368 = 0,537	137	147
14 (14, 12)	0,9901 – 0,905 = 0,008	22	14
16 (16,14)	0,9967 – 0,9901 = 0,0066	1,71	3
18 (18,16)	0,9999– 0,9967 = 0,0032	0,819	0

From the presented results it follows that theoretical and experimental results practically repeat each other. This means that for the distribution of differentials of byte substitutions the Poisson probability distribution law, which was used in constructing the integral law of distribution of maxima for these substitutions, is indeed fulfilled.

Table 2, also borrowed from our work [3], presents the law of the distribution of the values of the maximum displacements for the plurality of byte substitutions obtained by calculation and experimentally.

It can be seen that in this case the results of the experiments practically repeat the results of the calculations. Note here that experiments in both the first and the second case were performed on substitutions taken from the output of the random permutation generator without any filtering.

Therefore, it can be assured that the values of the XOR maxima of the differences for the differential byte substitution tables are in most cases 8-10, and the values of the displacements maximums of the linear approximation tables are 32-34.

Moreover, according to the results of the substitution results with XOR maxima, differences of less than 12 are 99% (less than 10 are 93%).

Table 2. The distribution of values of the maximums of displacements for the set of byte substitutions, calculated 2^8 obtained by calculation and by experiment

k^* (X_1, X_2)	Pr(k^*)	Estimated value	Experiment
26	3.41 10^{-7}	0	0
28 (28,26)	5,6 10^{-4}– 3,41$10^{-7}$ = 5,6 10^{-4}	0,14	0
30 (30,28)	0,064 – 5,6 10^{-4} = 0,0638	16,3328	10
32 (32,30)	0,368–0,064 = 0,304	77,824	86
34 (34,32)	0,692 – 0,304 = 0,388	99,328	98
36 (36,34)	0,874 – 0,692 = 0,181	46,336	46
38(38,36)	0,9518 – 0,874 = 0,078	19,968	10
40 (40,38)	0,9821 – 0,9518 = 0,03	7,68	6
42 (42,40)	0,9933 – 0,9821 = 0,011	2,816	0
44 (44,42)	0,9975 – 0,9973 = 0,00028	0,07	0

In most cases, the offset maximums for linear tables of byte substitutions are 32-34. From the presented results, it follows that substitutions with a maximum displacement value of less than 36 are 94% (less than 34 are 76%).

Finally, it will be appropriate to give the results of experiments with random byte S-blocks obtained in [27], which are shown in Table 3 (with notations from this work).

Table 3. Cryptographic properties of randomly generated byte

Criterion	The value of	% generated S-blocks
Maximum DDT	8	0,004
Max Lat (Nonlinearity)	32(96)	11 (34)
	30(98)	0,15 (0,04)
	28(100)	0 (0,05).
The minimum degree of BF	7	30
Algebraic immunity	3	100

10 million random substitutions were generated. The table in brackets also shows our experimental results, but not for all criteria. We are particularly pleased with the indicators of algebraic immunity. According to our data, the S-block of the AES cipher has algebraic immunity 2.

However, there were experts who expressed doubts about the values of algebraic immunity.

Therefore, we developed our own program for calculating algebraic immunity [29]. The results obtained with its help, fully confirmed that all 100% accidental S-blocks have algebraic immunity equal to 3.

7. Discussion

The results of the studies confirmed that the substitutions from the output of the random permutation generator are likely to be good S-blocks. But given the still little experience of using random substitutions to build ciphers and being quite critical of this model for some specialists, it is suggested that an advanced random substitution model be considered as a random substitution from the output of a random substitution generator, which passes a positive check for compliance with at least four indicators

S-block and Boolean functions that form it:

1. The maximum value of the XOR junction is in the range of 8-10;
2. The maximum value of the displacement of the LAT is in the range 32-34 (i.e. the nonlinearity is 94-96);
3. The algebraic degree of Boolean functions of the S-block is not less than 7;
4. Algebraic immunity index of S-block is not less than 3.

It is a random substitution obtained without restriction, very likely to be suitable from the point of view of cryptographic applications. They have provided the best dynamic output of ciphers with strong linear transformations (which use at least one cycle function with controlled substitutions) to asymptotic indices of random substitutions The cipher of such construction, which allows to increase the minimum number of activated S-blocks of the second cycle almost to the maximum, is offered in [3].

Thus, the scientific novelty of the work is seen in the fact that for the first time the possibility of using S-blocks for the construction of ciphers from the output of the random substitution generator is substantiated.

8. Conclusions

There is a long way to go about justifying the criteria for the selection of random substitutions from the simplest combinatorial to sufficiently rigid additionally developed criteria, which are built on the use of estimates of the closeness of laws of distribution of XOR tables and displacements of tables of linear approximations to theoretical laws.

However, it was not possible to find any particular advantages of substitutions selected using even rigid criteria. By their cryptographic index, which are determined by known methods, including algebraic, they are not particularly distinguished against the background of other known structures. Therefore, all considered criteria for the selection of random substitutions in the considered version had to be abandoned. We have moved to a more refined mathematical model of random permutation based on the properties of a sample of random substitutions (this model incorporates and found the differential and linear laws of the distribution of transitions of the corresponding substitution tables and the corresponding laws of the distribution of maxima).

At the same time, we recognize that permutations are one of the important elements in the designs of modern encryption transformations, playing the role of an additional, if not the main, and mechanism for effective random mixing of data blocks.

The main result of the work is a refined model of random substitution. According to this model, a substitution is considered random if it belongs to an ensemble of substitutions whose maxima of XOR tables and offsets of linear approximation tables obey the law of distribution of Fisher-Tippet extreme values (log-Weibul). This allows random (byte) substitutions in ciphers to be used directly by substitutions formed by a random permutation generator.

The refinement concerns the use of additional selection criteria which, as it turned out, do not substantially limit the many substitutions formed by the random generator.

An important conclusion is that for a random Boolean function, most of its cryptographic parameters are close to optimal. It will be natural this conclusion to random S-blocks: for a randomly-taken S-block, most of its cryptographic parameters are close to optimal.

As a result, the problem of constructing ciphers in which random S-blocks can be used without loss of stamina becomes relevant, which found its first solution in our work [3] and in several others.

References

1. Dolgov V.I. Methodology for assessing the resistance of block symmetric ciphers to attacks of differential and linear cryptanalysis / V.I. Dolgov, I.V. Lisitskaya. // Monograph – Kharkov: Publishing house “Fort”. – 2013. – 420 p.
2. Lisitskaya I.V. Experimental data for determining the dynamic parameters of the arrival of block symmetric ciphers to the state of a random substitution / I.V. Lisitskaya, K.E. Lisitsky, M.Yu. Rodinko et al. // Radioelectronics, informatics, management Zaporozhye: ZNTU – 2017. – № 1 (40) – pp. 129-141.
3. Dolgov V.I. The new concept of designing block symmetric ciphers / V.I. Dolgov, I.V. Lisitskaya, K.E. Lisitsky // 0485-8972. – Radio Engineering – All-Ukrainian. bear. scientific-technical Sat. – 2016. – Issue 186. – pp. 132-152.
4. Claudia Peerez Ruisanchez A new algorithm to construct S-boxes with diffusion International Journal of Soft Computing, Mathematics and Control (IJSCMC),Vol. 4, No. 3, August 2015 DOI : 10.14810/ijscmc.2015.4303 41
5. Reynier Antonio de la Cruz Jim´enez Generation of 8-bit S-Boxes having almost optimal cryptographic properties using smaller 4-bit S-Boxes and finite field multiplication www.cs.haifa.ac.il/~orrd/LC17/paper60.pdf.
6. Dragan Lambić and Miodrag Živković Communicated by Žarko Mijajlovi Comparison of random S-box Generation methods. Publications de L’institut Mathematique Nouvelle série, tome 93 (107) (2013), 109-115 DOI: 10.2298/PIM1307109L.
7. Lisitskaya Irina Viktorovna. A methodology for estimating the block symmetric crypto migration based on the changes in models: dis. ... doctor. those. Sciences: 05.13.05 / Lisitskaya Irina Viktorivna. – Kharkiv. 2012 .– 293 p. – Bibliogr .: 294-293.
8. Shirokov O.V. Methods of formulating S-block constructions of a vipad type with reduced indexes for block symmetric ciphers: dis. ... cand. tech. Sciences: 05.13.21 / Shirokov Oleksiy Viktorovich. Kharkiv. 2010 .– 232 p. – Bibliogr .: 215-232.
9. Melnichuk Є. D. Methods for assessing cryptographic applicability of universities in non-linear deputy block symmetric ciphers: dis. ... cand. tech. Sciences: 05.13.21 / Melnichuk Evgeniy Dmitrovich. – Kharkiv. 2013. – Bibliogr .: 169-188.
10. Lisitskaya I.V. Estimation of the number of random permutations with a given distribution of pair differences of XOR tables and offsets of linear approximation tables. / I.V. Лисицкая, A.B. Shirokov, E.D. Melnichuk, K.E. Lisitsky // Applied Radio Electronics. – Kharkiv: KNURE. – 2010. – T. 9, № 3. – pp. 341-345.
11. Dolgov V.I. Random substitutions in cryptography. / V.I. Dolgov, I.V. Lisitskaya, K.E. Lysytsky // Radio electronic and computer systems. – 2010. – № 5 (46). – pp. 79-85.
12. Seberry J., Zhang X.M., Zheng Y. "Pitfalls in Designing Boxes (Extended Abstract)"//, Copyright © Springer-Verlag, 1998, pp. 383-396.
13. K. Nyberg. On the construction of highly nonlinear permutations. In Advances in cryptology - Proceedings of EUROCRYPT'92 (1993) vol. 740, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92-98.
14. Claudia Peerez Ruisanchez A NEW ALGORITHM TO CONSTRUCT S-BOXES WITH HIGH DIFFUSION International Journal of Soft Computing, Mathematics and Control (IJSCMC),Vol. 4, No. 3, August 2015 DOI : 10.14810/ijscmc.2015.4303 41

15. Dragan Lambić and Miodrag Živković Communicated by Žarko Mijajlovi Comparison of random S-box Generation methods. Publications de L'institut Mathematique Nouvelle série, tome 93 (107) (2013), 109–115 DOI: 10.2298/PIM1307109L.
16. Rodinko M.Yu. Cyclic properties of block symmetric ciphers / M.Yu. Rodinko, K.E. Lisitsky // Materials of the XVI International Youth Forum "Radio Electronics and Youth in the 21st Century" – Kharkov – 2012, T. 7. – pp. 142-144.
17. Sachkov V.N. Introduction to combinatorial methods of discrete mathematics. - M.: Science - 1982 – 384 p.
18. Lisitskaya I.V. The experimental verification of the operability of new selection criteria for random substitutions / I.V. Lisitskaya, K.E. Lisitsky, A.V. Shirokov et al. // Radio electronics and computer system, – 2010. – No. 6 (47). – pp. 87-93.
19. Oleinikov R.V. Differential properties of permutations / Oleinikov R.V., Oleshko O.I., Lisitsky K.E., Tevyashev A.D. // Applied Radio Electronics. – 2010. – T. 9. – No. 3. – pp. 326-333.
20. Dolgov V.I. Properties of linear approximation tables of random permutations. / V.I. Dolgov, I.V. Lisitskaya, O.I. Oleshko // Applied Radio Electronics. – Kharkov: KNURE. – 2010. – T. 9, No. 3. – pp. 334-340.
21. Lisitsky K.E. "The law of the probability distribution of displacements of approximation tables of random permutations" Radio engineering-All-Ukrainian. inter. scientific and technical Sat – 2017. – V. 189. – pp. 81-89.
22. Lisitskaya I.V. "Properties of the distribution laws of XOR tables and tables of linear approximations of random permutations." News of the Kharkiv National University of Economics the name V.N. Karazina. –.2011. – No. 960, – Vip.16. – pp. 196-206.
23. Joan Daemen, Vincent Rijmen Probability distributions of Correlation and Differentials in Block Ciphers. / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1-38.
24. Lisitsky K.E., Melnichuk E.D. "Refined mathematical model of random permutation. "Automated control systems and automation devices. "2013, Issue. 162, pp. 22-28.
25. K. Lisickiy, "On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers," International Journal of Computer Network and Information Security, vol. 6, no. 1, pp. 11–18, Nov. 2013. doi:10.5815/ijcnis. 2014.01.02.
26. Lisitsky K.E. "Maximum values of complete differentials and linear enclosures of block symmetric ciphers. " Technological audit and production reserves. – 2014.– №1 / 1 (15). – pp. 47-52.
27. Rodinko M.Yu. Improvement of the method for optimal S-boxes generation / M.Yu. Rodinko, R.V. Oliynykov, T.O. Hrinenko // Applied Electronics. – Kharkov: KNURE. – 2015. – Vol. 14, No. 4. – pp. 315-320.
28. Gorodilova A.A. From cryptanalysis to the cryptographic property of a Boolean function / A.A. Gorodilova // Applied Discrete Mathematics. – 2016. – No. 3 (33). – pp. 16-41.
29. Lisickiy, K. Kuznetsova, Y. Malenko, S. Kavun, O. Zavgorodnia, and Y. Tarasenko, "Accelerated Method for Calculating the Algebraic Immunity of S-Boxes," 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Jul. 2019. doi:10.1109/ukrcon.2019.8879943.