SCIREA Journal of Physics

https://www.scirea.org/journal/Physics

November 25, 2019

Volume 4, Issue 6, December 2019

Cipher with random substitutions

Lisickiy K.E., Dolgov V.I., Lisickaya I.V.

Department of Information Systems and Technologies Security, Kharkov National University named after V.N. Karazin, Kharkov, Ukraine

lisitskaiv@ukr.net

Abstract

A new approach to constructing SPN block symmetric ciphers is presented, which allows random S-blocks to be used in ciphers without sacrificing strength.

Its basis is an improved construction of a cyclic transformation constructed using the principles of controlled substitutions, when the results of previous substitution transformations are fed to the inputs of the substitution transforms along with the current values of the segments of the input data blocks.

This allows you to activate almost all S-blocks of the second and subsequent cipher cycles and, as a result, improve the dynamic indicators of cipher arrival to the state of random substitution. Examples are given of constructing such ciphers and a number of modern ciphers, improved by replacing their first cycles with a cyclic transformation of a new design. The randomness indices of ciphers with improved cycles are estimated. The results of the analysis of their resistance indicators and the possibility of using random substitutions in ciphers are discussed. The results of an experimental verification of the effectiveness of using random S-blocks in new ciphers are demonstrated. It is concluded that the proposed construction of the cyclic function really allows one to construct ciphers in which substitutions from the output of the random substitution generator can be applied practically without selection without reducing the resistance.

Keywords: controlled S-blocks, dynamic indicators of the cipher's arrival to the state of random substitution, active S-blocks, random S-blocks, randomness indicators, strength indicators

I. INTRODUCTION

In this work, we will focus on modern designs of block symmetric SPN ciphers.

When talking about a resistant cipher, they primarily mean its resistance to differential and linear cryptanalysis attacks. It is generally accepted to evaluate the indices of resistance of block symmetric ciphers (BSC) to differential and linear attacks with the maximum values of differential and linear probabilities [1-3, etc.]. The enormous number of publications is devoted to the study of cipher resistance indicators and the influence of the properties of S-blocks on the indicators of their resistance.

We also contributed to the development of this area. We have proposed a new methodology for assessing the resistance of BSH to attacks of differential and linear cryptanalysis, based on the study of the properties of ciphers as random substitutions, which made it possible to determine the indicators of their resistance by calculation [4,5,6, etc.]

In accordance with the new methodology for assessing the resistance of block symmetric ciphers to attacks of differential and linear cryptanalysis, developed in [4], BCS resistance indicators are independent of S-blocks included in the cipher cyclic functions. Substitution transformations (S-blocks) affect only the number of cycles that ciphers arrive at the state of random substitution, and then only within one cycle. This is due to the fact that the maximum values of the resulting differential and linear probabilities are determined through the products of the differential and linear probabilities of the S-block ciphers included in the cyclic functions, and only activated S-blocks.

Active (activated) S-blocks are hereinafter referred to as S-blocks participating in the formation of real multi-path differential and linear characteristics of ciphers (having non-zero output differences or non-zero transitions of linear characteristics) [6].

Dynamic indicators of the arrival of the cipher to the state of random substitution refers to the minimum number of cycles of encryption after which the cipher comes to the state of random substitution (when the maxima of the differential and linear probabilities of the

cipher, as a substitution transformation, take stationary values that coincide with the values of maxima of random substitution of the corresponding degree)

Obviously, the minimum number of cycles for which the cipher comes to random substitution is denoted by the minimum number of active S-blocks of these cycles that ensure the stationary value of the maximum probabilities of differentials (respectively, the maximum probabilities of linear cases) of the cipher. Differential and linear dynamic indicators are the main indicators of the effectiveness of encryption transformation [6]. So it turns out that S-blocks of ciphers have a decisive influence on the efficiency of cyclic transformation (cipher). The more S-blocks are activated in a cyclic function, the fewer cycles the cipher can come to the stationary state of a random substation. So the whole point is that in the well-known constructions of block ciphers, not all S-blocks of cyclic functions are activated on the first cycles. In the Rijndael-256 cipher, for example, with a single-byte difference at the input of the cipher, on the first cycle one S-block of 32 is activated on the second 4 of 32, on the aunt is 16 of 32, on the fourth and subsequent cycles of 32 out of 32 (in fact, in the second and subsequent cycles of S-blocks, even less is activated). As analysis shows, the design solutions used in the construction of other modern ciphers also implement a step-by-step process of activating S-blocks of cyclic functions of different cycles when S-blocks of the current cycle do not provide activation of all S-blocks of the next cycle, as in the considered example with the Rijndael cipher.

It turns out that a huge number of publications on design S-blocks with high cryptographic indicators are practically aimed at actually winning one cycle in the encryption procedure. Note that for SPN ciphers with cyclic functions using single-layer permutation transformations, the minimum number of activated S-blocks of the first cycle is equal to one, and therefore, in the presented example, to increase the transformation efficiency, we can talk about increasing the minimum number of activated S-blocks in the second and third cycles.

It is believed at the same time that the high cryptographic properties embedded in the S-block will contribute to the achievement of increased cipher strength indicators.

Recall also that in accordance with the new methodology for assessing the strength of symmetric block ciphers, all ciphers, after several initial encryption cycles, regardless of the S-blocks used, become random substitutions. Recall that the Rijndael-256 cipher comes to a state of random substitution in five cycles [6].

The natural question arises whether all this colossal work on the selection and construction of “optimal” S-blocks is justified, if as a result, in all cases, we arrive at the same result (to the same values of the differential maxima and linear probabilities)? We think that other cryptographic indicators of ciphers as random substitutions will be close.

It turns out that the use of S-blocks with special properties actually reduces only to reducing the number of cycles the ciphers arrive at the state of random substitution (just by one cycle), and it is completely unclear whether the selected S-blocks on the full-cycle encryption length give any other advantages. In our opinion, the “weaknesses” of ciphers and S-blocks are leveled at the full-cycle encryption length. For this, the number of encryption cycles with a margin (strength margin) is selected.

So the idea came up to build encryption transformations (ciphers) with more efficient cyclic functions, allowing increasing the number of activated

Compared to traditional methods and without loss of durability, S-blocks of the second and subsequent cycles go to the use of S-blocks in ciphers directly from the output of the random permutation generator.

Now it has already been implemented in a number of our proposals [6-10] and patents [11-13], and we continue to develop this area.

The purpose of this work is to popularize and further develop the noted direction. In this article we will provide additional arguments and justifications for its justice and fruitfulness.

In fact, it will be about substantiating a new concept for constructing block symmetric ciphers - ciphers with random permutations

II. LITERATURE REVIEW.

The Rijndael cipher is still considered as the latest achievement in the design and development of block symmetric ciphers. It will be relevant to recall the thoughts and considerations presented in Susan Landau [14] on the study of algebraic aspects of the Rijndael (AES) development. We have already quoted it in our publication [6] and others, but in our view it deserves to be addressed again.

The work focuses on the design of block ciphers. The author traces the paths that led to the Rijndael cipher, which is now considered the last word in design and engineering decisions. It is argued that this development has become a natural result of the development of world cryptographic thought.

Thus, [14] notes a number of works and proposals made on the way to Rijndael. We will remind them here. Willi Meier and Othmar Staffelbach have suggested that certain examples of nonlinearities used by mathematicians may be suitable for a cryptographic system project [15]. Based on these ideas, Josef Pieprzyk proposed algebraic methods for the construction of nonlinear functions [16, 17,]. Kaisa Nyberg researched S-blocks and applied some of Pieprzyk's ideas when designing S-blocks [18]. Joan Daemen studied the cyclic functions in terms of differential and linear cryptanalysis of the cipher and proposed a new paradigm and broad-trace approach [19]. With other researchers, he used the wide footprint and Nyberg S-blocks in the SHARK cryptosystem [20]. Thomas Jakobsen and Lars Knudsen found an "interpolation attack" against simple algebraic ciphers such as SHARK [21]. Two developers Daemen and Vincent Rijmen of SHARK opposed Square cryptosystem [22]. Knudsen broke Square using a variety of attacking techniques [22]. Rijndael, notes the author of the cited work, rose from the dust of Square. The work then follows how these threads were woven by Rijndael.

Much attention has been paid to the analysis of the design methods of Rijndael new paradigm and approach, which is considered to have been developed by Joan Daemen and has been dubbed the broad-based strategy.

Speaking of wide track strategy, Susan Landau notes. It is easiest to perform cryptanalysis when a single (one) S-block is active in each cycle. Therefore, the designer of the cryptographic algorithm should strive to avoid the worst case of diffusion when there is a single active S-block. Obviously, the best that can be done by the designer in terms of reaching the upper limit is that the number of branches ß is $n + 1$, where n is the number of links (each link consists of m bits). A reversible linear mapping that achieves this effect is called optimal. Daemen and Rijmen managed to construct such a mapping. They have shown that separable maximum distance ciphers (MDS ciphers) provide a way to construct such optimal linear transformations. This mapping turned out to be significantly more effective than many other linear transformations used in ciphers. Recently, however, we have found a way to implement a broad-based strategy without separable ciphers [23].

The paper then discusses the goals of the project and the ways in which the authors managed to achieve them.

It is generally noted in [6] that Daemen and Rijmen have been able to create a design that has been able to gain the trust and support of most world-class experts and professionals.

Of course, the design principles applied by AES developers such as:

- simplicity of specification and simplicity of analysis;

- transparency of the solutions used;

- efficiency.

It should be noted that the principles used in the design of AES have become the basis for the construction of many new ciphers: Labyrinth, Camellia, Kalina, Muhomor, Grand Cru and others, and in particular, the basis for the construction of new state standards and the Kalina-2 cipher adopted in Ukraine [24] and the Kuznechik cipher adopted in Russia [25] (in the Kuznechik cipher it was possible to activate all S-blocks of the cycle function, but this is a 128-bit cipher and no one has proposed to multiply the MDS matrix 32×32).

The results of the analysis of these constructions, performed in [6], show that the cyclic transformations of ciphers of the specified series are constructed so that the linear and differential indices of the S-blocks that enter them influence the dynamic parameters of the arrival of the ciphers to the state of random substitution within one cycle. . In such ciphers, the minimum number of activated S-blocks of the first cycles is on the verge of providing the minimum number needed to reach the ciphers to the asymptotic values of the maxima of differential and linear probabilities. Therefore, changing the differential or linear indices of the S-blocks used in these ciphers influences the minimum number of cycle transformations required for the cipher to arrive at a state of random substitution. It turns out that for marked and many other modern ciphers with selected S-blocks, it is necessary to perform at least three to four cycles of encryption to arrive at random substitution (as already noted, not all S-blocks of cycle functions are activated in many ciphers). The natural question is whether it is possible to build a loop transformation that will provide an increased minimum number of S-blocks that are activated in the first cycles?

In general, our investigations into the possibility of increasing the number of S-blocks activated in the first cycles have shown that the approaches adopted in the construction of

modern ciphers are based on the use of single-layer cycle substitution transformations provide a minimum number of S-blocks activated in the first cycle equal to one. This result may be obvious, but we proved it experimentally.

The problem can only be solved by using positive transformations constructed using nonlinear operations (S-blocks), as is done, for example, in the cipher Labyrinth [26], but this is actually another cycle transformation. Therefore, it is necessary to either enter into the cipher a positive conversion that pulls on a positive cycle, or to use in the ciphers an advanced cycle transformation, which, unlike the existing approaches, allows to construct a cycle function with an increased number of activated S-blocks. In this work and this problem is solved. In this work and this problem is solved

III. MATERIALS AND METHODS

A Description of the construction of a cyclic function

Here we will first introduce the proposed option for constructing a cyclic function used in our developments. We take the materials of [6] as a basis. We, as in many of our publications, will be guided in this direction by the 256-bit implementation of the cipher.

First, recall the design of the cyclic function of the SHUP-1 cipher. It is shown in Fig. 1. Here is a diagram of an improved design in relation to the circuit from [6]. In this work, we describe the modernized design of the cipher, which was named the SHUP-1M cipher in [6].

In this case, the preliminary summation of the segments of the input data block at the input SL transformation of the first cycle is excluded. Summing the output of the last SL transform with the outputs of the previous SL transforms is also excluded, except for addition to the output of the first SL transform, because experiments have shown that these operations do not lead to an improvement in the randomness of the cipher.

An input data block of 256 bits is divided into eight sub-blocks of 32 bits each. Then, each subblock is added together with the corresponding part of the cyclic key, also presented in the form of eight 32-bit segments. Addition is performed modulo a segment. The resulting blocks are sequentially fed to the inputs of 8 SL transforms, which are included in the chain, so that the sum of the modulo two next (current) 32-bit data subblock and 32-bit segment from the output goes to the input of the current

SL transform previous SL transformation . Such inclusions of SL substitution transformations we called controlled substitutions, whence the name of the ciphers of this series is GUPs. Outputs 7 SL transforms go directly to the output of the cyclic function, and the output of the first SL transform goes to the output of the loop function after adding the last - 8th SL transform to the output

The main conversion of a cycle function is SL transformation. I repeat the construction of SL transformation the Mukhomor cipher [30] and am shown in Fig. 2.

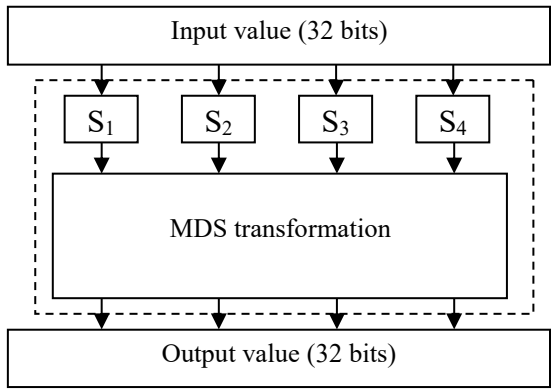

Fig. 2. - Scheme of SL- transformation

The 32-bit input is divided into 4 bytes, each of which is replaced according to the specified wildcard (S-block). The transformation uses 4 different tables, one per byte.

After the replacement operation in the S-blocks 4 bytes (a_0, a_1, a_2, a_3) are fed to the input of a linear transformation that performs matrix multiplication by the MDS matrix (cipher matrix with the maximum permissible distance):

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 02 \cdot a_0 \oplus 03 \cdot a_1 \oplus 01 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 02 \cdot a_1 \oplus 03 \cdot a_2 \oplus 01 \cdot a_3 \\ 01 \cdot a_0 \oplus 01 \cdot a_1 \oplus 02 \cdot a_2 \oplus 03 \cdot a_3 \\ 03 \cdot a_0 \oplus 01 \cdot a_1 \oplus 01 \cdot a_2 \oplus 02 \cdot a_3 \end{bmatrix}$$

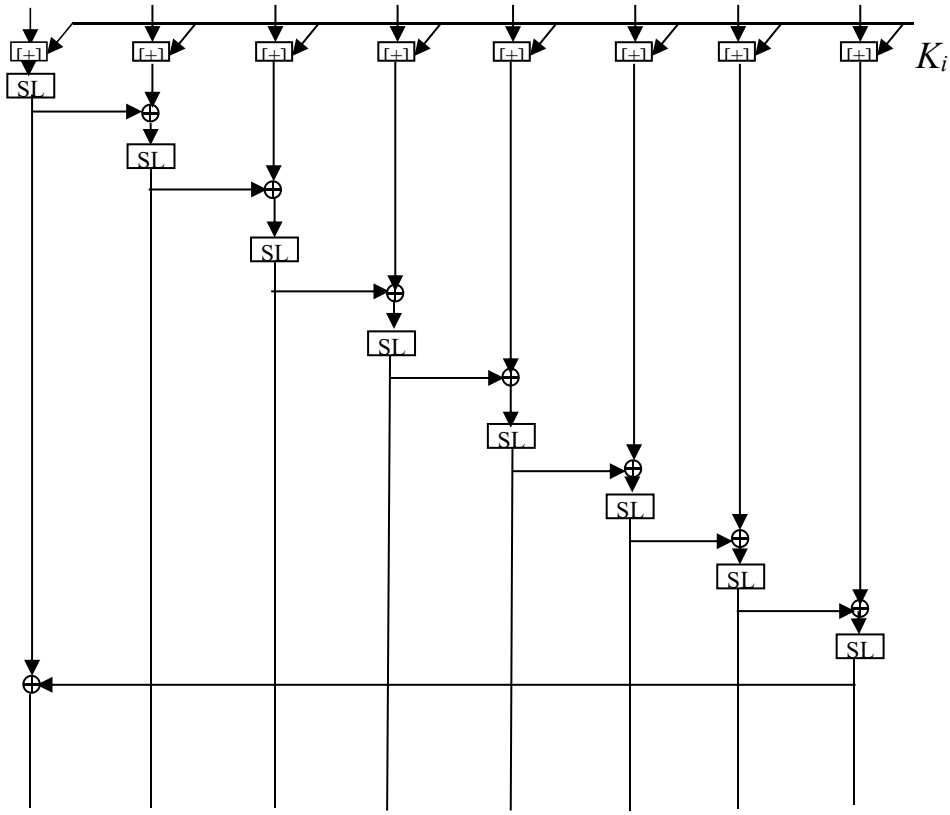

Fig. 1Block diagram of the cyclic transformation SHUP-1M

B Theoretical substantiation of the minimum number of activated S-blocks for the arrival of the cipher to the state of random substitution

In this section, we present the results of estimating the expected parameters for the transition of ciphers to the state of random substitution. We will continue to focus on ciphertext with 256-bit data blocks (keeping in mind the post-quantum cryptographic development period [31]).

The main considerations on this issue are given in our paper [6]. According to the idea of the approach developed in [6], it is necessary to estimate the minimum number of active (activated S-blocks), after which the cipher becomes a random substitution. This minimum number is determined by the differential and linear indices of the S-blocks themselves used in the cipher, the designs and properties of its cyclic transformations, as well as the values of the cipher proof strengths depending on the size of its bit input. In [32], this relationship between these indicators is defined as two relations:

$$IPS_D = (\,DP_{\max}^{\pi}\,)^k,\ IPS_L = 2^{k-1}\cdot\left(LP_{\max}^{\pi}\right)^k.$$

Here $DP_{\max}^{\pi}$ and $LP_{\max}^{\pi}$ are the maximum values of the differential and linear probabilities of the substitution transformations $\pi(x)$. IPS_D (Differential Indicator of Provable Security)

– Differential Evidence Security and IPS_L (Linear Indicator of Provable Security) – Linear Evidence Security, $k = k_{\min}$ – minimum active S-blocks involved in the formation of the transition of the cipher to a random substitution. Therefore, IPS_D must be used for calculations and IPS_L.

We use here the calculation method from our work [5], which allow us to conclude that for the arrival of the cipher to the state of random substitution, the expected maximum value of the number of differential transitions for the cipher with 256-bit input is close to 190, and the expected maximum value of the offset linear enclosures for a 256-bit input cipher is close to 2^{130}. Accordingly, we obtain that the maximum linear and differential probabilities for a 256-bit cipher are close to each other and them about $IPS_D \approx IPS_L = 2^{-248} \div 2^{-250}$.

Based on the above ratios, we can conclude that for a cipher with 256 bit input to arrive at the state of random substitution by differential indicators when using S-blocks with boundary indicators δ-uniformity $DP^{\pi}_{\max} = 2^{-6}$, (according to equality $2^{-248} = (2^{-6})^k$) will need to use $k_{\min} = 41$ S-block.

Similarly, in order to arrive at a state of random substitution in linear terms when using S-blocks with boundary values of nonlinearity equal $LP^{\pi}_{\max} = 2^{-6}$,

($2^{-250} = 2^{k-1} \cdot \left(2^{-6}\right)^k$) $k_{\min}$ = 50 S-blocks (for S-blocks of Muhomor cipher with a nonlinearity $LP^{\pi}_{\max} = 2^{-5}$ for all in this case we have $k_{\min} = 62{,}25$).

According to the known results, it turns out that in the original cipher Rijndael-256 is activated in four cycles of at least 53 S-blocks (1 on the first, 4 on the second, 16 on the third and 32 on the fourth). This allows the 256-bit Rijndael cipher to arrive at a random differential and linear substitution in three-four cycles.

C Use of random S-blocks

The question of using random S-blocks is fundamental to this work. As follows from the results of [32], the value of the minimum number of cycles of output of the cipher to the state of random substitution is directly related to the differential and linear properties of S-blocks.

As noted in [32], in the construction of differential and linear characteristics for arbitrary S-blocks in most cases transitions are used and not with the maximum possible values of

differential and linear transitions (maximum values are very small). Therefore, the real values of the probabilities of differential and linear characteristics will be determined by a random set of transitions involving transitions and not with minimum values of probabilities, which will reduce the number of S-blocks activated compared to the case of transitions with minimum values.

In connection with the mentioned in [6, 32-34 and others], the possibility of using random S-blocks in ciphers was evaluated.

In the table 1 presents the results of calculations of the number of transitions of different types in the 48 rows of the differential table of the random substitution borrowed from [6]. In our calculations, we use the maximum number of active S-blocks, which allows to realize the arrival of a cipher with 256 bit input on differentials

Table 1 Calculation of the number of transitions of different types in the 48 rows of the differential table of random substitution

Table transition values	The number of transitions of the differential table	Numeric Transformation s in a row	The number of transformation s in 48 rows
12	1	0,003906	0,19
10	10	0,039065	1,87
8	104	0,40625	19,5
6	830	3,24218	155,62

to random substitution. For differential indicators, it is equal to 48.

From the presented results it follows that 48 active S-blocks (active transitions) can be selected at random entrances to S-blocks at their consecutive start based on the use of

- twenty transitions with a value of 8;

- twenty-five crossings with a value of 6;

- twenty transitions with a value of 8;

- twenty-five crossings with a value of 6;

The most likely transitions are used; we believe that the entry into the first S-block will be the maximum possible.

Total of 48 transitions (48 active S-blocks). The calculations in this case lead to the result

$$\left(\frac{10}{256}\right)^2 \times \left(\frac{8}{256}\right)^{20} \times \left(\frac{6}{256}\right)^{26} = 2^{-250}.$$

Let us now consider the law of the distribution of transitions for the displacements of a linear approximation table. The total number of transformation s includes both positive and negative displacements. Using the results of [6, 32], we can calculate the number of transitions of different types in 65 rows of linear approximation table of random substitution, the calculation results of which are presented in table 2/

Considering further that the rows in the S-block are selected from the whole set of 256 rows, and the transitions on the S-blocks are random and carried out in the most probable way, we can estimate the probability of the cipher coming to the state of a random substitution with random S- blocks. The calculations for 65 S-blocks lead to the result.

From the results it follows that for 65 active S-blocks, when using them, the most likely transitions can be expected at random inputs into random S-blocks:

• - one transition with value 32;

• - three transitions with value 30;

• - eight transitions with value 28;

• - eighteen transitions with value 26;

• - thirty three transitions with value of 24.

The very first (one) S-block is taken with the maximum possible transition value (34).

$$2^{64} \times \left(\frac{34}{128}\right)^2 \times \left(\frac{32}{128}\right)^2 \times \left(\left(\frac{30}{128}\right)^2\right)^3 \times \left(\left(\frac{28}{128}\right)^2\right)^7 \times$$

$$\times \left(\left(\frac{26}{128}\right)^2\right)^{16} \times \left(\left(\frac{24}{128}\right)^2\right)^{36} = 2^{-236}.$$

We have not reached the maximum differential probability of the 256-bit cipher, but the obtained differential probability value makes it possible to count the cipher practically resistant to both attacks and linear cryptanalysis (cipher SCHUP-1 dials 65 cycles of 65-66 active S-blocks in three cycles.

That is, our cipher with advanced cycle transformations (SHUP-1, or SHUP-1M) comes to the state of random substitution and differential and linear indicators for three cycles, and

if we take the first cycle two-layer (SHUP-2, SHUP-2M), then such a cipher will come to a state of random substitution in two cycles.

Therefore, the proposed ciphers come to random substitution in three or two cycles and when used in ciphers randomly generated S-blocks with almost no filtering.

Enhanced transformation is more efficient than Rijndael and in terms of performance (decreases the number of intermediate modulo 2 modulations and eliminates byte multiplication operations) [6, 34]. In addition, the cipher SHUP-1 has fewer cycles.

IV EXPERIMENTS

To illustrate the increased transformation efficiency, we first present experiments to estimate the number of activated S-blocks in the first cycles of the SHUP-1M cipher with the cyclic function shown in Fig. 1

Note that at the inputs of the SL transform of this function, the input data segments are added together with the key segments modulo. This modular operation is carried out with discharge transfer. Therefore, when the last byte of the input of the SL transformation is activated (and in the experiment we activated the 31 and 32 bytes), the previous bytes will also be activated. Here we present the results of activating the cipher with two input bytes of the 31 and 32 (see Table 3).

Table 3 Distribution of activated S-blocks of the first cycle upon activation of the 31 and 32 input bytes at the input of the cipher

Number of active S-blocks	Number of options held	Estimation of their share in%
1	27350220	0,63
2	2726313690	63,47
3	1541237850	35,88

It is seen that when two bytes are activated at the cipher input, three bytes of the 8th SL transformation are activated. When activating the cipher with single-byte retrieval, you will be activated on the first cycle one or two bytes.

In the table 4 presents the results of experiments to determine the number of active S-blocks on the second cycle of the SHUP-1 cipher when two input bytes are activated numerically and in percent. It is seen that with a high probability the number of activated

S-blocks turns out to be close to 32. In almost 90% of cases, 65-66
S-blocks are activated in this cipher in three cycles, which is quite enough for it to come to a state of random substitution.

The SHUP-2M cipher will come to a state of random substitution in two cycles (65 activated S-blocks). The Rijndael cipher comes to a state of random substitution for 4 cycles.

Table 4 The number of active S-blocks for the second cycle when activating one (right) input byte in percent

Number of active S-blocks	Estimation of their numbers in %
1-25	0
26	0,000000232
27	0,00000149
28	0,0007133
29	0,00258
30	0,668
31	11,075
32	88,228

The results of the next experiment will be devoted to the analysis of indicators of statistical security of ciphers SHUP.

Here we will follow the methodology for the analysis of these indicators described in [35]. Using this technique, the correlation properties of block symmetric ciphers are evaluated as controlled by permutation keys.

Here we look at such statistical safety indicators as:

- the average number of output bits that change when one input bit (m_w) changes;

- degree of completeness (d_c);

- degree of avalanche effect (d_a);

- degree of strict avalanche criterion (d_{sa}),

considered for a different number of cycles and randomly taken encryption keys.

Definitions of these indicators can be found in [36].

In our case, in order to avoid leveling the differences between the individual bits, the avalanche effect was not considered as an average value for all bits, as in [35], but for each bit separately, and the minimum and maximum values were selected among the obtained values for each bit. If we take the average of all bits, we get results that repeat [35]. They are presented in separate table columns.

Further, in accordance with the approach described in [36], given a confidence probability, based on the student distribution table [37] for given values $P_0(\theta_1, \theta_2) = 0{,}999 \rightarrow \alpha = 0{,}001$ and n = 10000 (sample of input texts in our experiments) and the variance of the distribution law for 256-bit versions ciphers equal
σ_w^2 = 64 we get, respectively:

$$\frac{t \cdot S}{\sqrt{n}} = \frac{3{,}291 \cdot 8}{\sqrt{10000}} = 0.263$$

and, therefore, all values satisfying the conditions, respectively, can be considered as falling into confidence intervals:

$$128 - 0{,}263 \le m_w \le 128 + 0{,}263;$$

Similarly, estimates of the distribution parameters are performed when processing the results of other correlation indicators.

The following are the results of the research. Table 5 presents the results of the evaluation of statistical security indicators implemented in experiments with a cipher built on controlled SL transformations.

Table 5 Cyclical values of indicators of statistical safety of code SHUP-2

Round №	SHUP-2							
	$M_{\min}$	D_{min}	$M_{\max}$	D_{max}	m_w	d_c	d_a	d_{sa}
1	127,73	63,453	128,21	62,91	127,97	1	0,999479	0,992026
2	127,73	63,382	128,2	65,331	127,96	1	0,999482	0,992
3	127,76	64,862	128,19	63,409	127,98	1	0,999518	0,992047
4	127,74	65,081	128,22	63,156	127,98	1	0,999491	0,992015

5	127,81	63,227	128,22	64,299	128,01	1	0,999484	0,992027
6	127,73	64,11	128,2	64,721	127,96	1	0,999497	0,991971
7	127,73	65,464	128,26	62,903	128	1	0,999506	0,992003
8	127,71	63,476	128,22	66,24	127,97	1	0,999484	0,992081

In this table, the following notation is used

$M_{\min}$ – the minimum value of the mathematical expectation of the number of changed bits for some bit at the input; $M_{\max}$ – the maximum value of the mathematical expectation of the number of changed bits for some bit at the input; $D_{\min}$ and $D_{\max}$ are the variance of the number of changed bits in a bitwise estimate of the maxima and minima of the average values, m_w is the average number of changed bits, which is calculated as

$$m_w = \frac{M_{\min} + M_{\max}}{2}.$$

From the presented data it follows that the depth of the avalanche effect for the cipher under consideration is equal to the 1st cycle. Starting from the first cycle, the value falls within the established boundaries.

It is also seen that the one-bit values of the maxima and minima turn out to be very close to the average value.

We note here that for the variance values, the condition used above when determining confidence intervals is fulfilled $S^2 \approx \sigma_w^2$ with great accuracy.

Table 5 shows that in all cases half the bits of encrypted text with a deviation of $\leq \pm$ 0.21 are changed, which corresponds to 0.008%. It can also be seen that the deviation occurs in both directions. The results obtained show that avalanche effect indicators (depth of entry into cipher cycles and variance of deviations from the mean) are better than all known cryptographic algorithms. Almost on the first cycle, the SHUP becomes a random substitution for all indicators. This may be unexpected, but this effect can be explained by the fact that the proportion of texts that produce poor results in the total number of texts participating in the experiment is negligible.

Functions (ciphers) having a good degree of completeness, a good avalanche effect and satisfying the strict avalanche criterion must have values d_c, d_a, d_{sa} and satisfying the condition: $d_c \approx 1$, $d_a \approx 1$, $d_{sa} \approx 1$, which is practically fulfilled for our cipher.

Another experiment demonstrates the effect of randomly shuffling data blocks on the first cycles of the SHUP-1M encryption.

Next, the results of determining the loop-by-loop laws of distribution of the maxima of XOR transitions and maxima of displacements of the SHUP-1M cipher in the mode of its initialization with 16-bit input differences in accordance with the methodology of [38] are presented.

Table 6 lists the cyclical laws of distribution of maxima of XOR differences for 256-bit Rijndael cipher and SHUP-1M cipher in the mode of their initialization by 16-bit differences in accordance with the procedure [38]. The 31 and 32 input bytes were activated

The calculations for the Rijndael cipher were performed for 30 random encryption keys, and for the ShUP-1M cipher for one encryption key. It can be seen that for the Rijndael cipher, the data obtained for the reduced model of this cipher is stored [27], and the cipher

ShUP-1M shows the limit indicators from the first cycle.

Indeed, for S-blocks of the Muhomor cipher with a differential uniformity $LP_{\max}^{\pi} = 2^{-5}$, the encryption the equation for a 16-bit cipher has the form $2^{-12} = (2^{-5})^k$. This means that in order to come to a state of random substitution of a 16-bit cipher, 2 activated byte S-blocks are enough. And if for a Rijndael cipher with XOR the operation of introducing cyclic keys, the maximum transition value of the first cycle will be equal to 1024 (only one input byte is involved, and the second is zero), then in the case of SHUP-1M with the modular operation of introducing cyclic subkeys, 2^{32} most likely will be with one, two, or three S-blocks SL transforms activated by the input difference.

Thus, it turns out that these S-blocks are quite enough for the 16-bit cipher to become a random substitution already in the first cycle. If we talk about a full-blown cipher, it comes to the state of random substitution for three cycles. Now the result is clear for a cipher with random S-blocks.

Table 7 shows the cyclic distribution of the maxima of the displacements of the LAT table for a 256-bit cipher also in its initialization mode using 16-bit non-zero input and output masks in accordance with the methodology of [38].

Table 6 Cyclic values of the maximums of the full differentials during encryption16-bit blocks for the Rijndael cipher and the ShUP-1M cipher

Number cycles *r*	Cipher Rijndael		Cipher SHUP-1M	
	Differential transition maximum value	RMS deviation	The value of the maximum total differential with S-blocks of the Muhomor	Maximum differential value wit полного дифференциала random S-blocks
1	1024	0	20	18
2	3652,26	±630,312	18	20
3	19,0666	± 1,436	18	18
4	19,0666	±0,99777	20	20
5	18,8666	±1,23108	18	20
6	19,1332	±0,99106	20	20
7	19,2666	± 1,0934	2	20
8	19,1332	± 1,43139	20	18
9	19,0666	± 1,23648	18	18

The results indicate that, in this case, the SHUP-1M cipher in the normal mode of application comes to the state of random substitution for three cycles, which confirms the increased efficiency of this design. The experiments confirm the relationship of the number of activated S-blocks in the first cycles with the minimum number of encryption cycles necessary for the cipher to arrive at a random substitution state.

From the table it follows that there is a high probability that the number of activated S-blocks turns out to be close to 32. In almost 90% of cases 65-66 S-blocks are activated in a cipher in three cycles, which is quite enough for it to come in a state of random substitution... The SHUP-2M cipher will need two cycles to arrive at the state of random substitution.

V DISCUSSION OF RESULTS

Therefore, in accordance with the obtained results, the proposed design of a cycle function to use it to build ciphers and improve their existing structures allows to increase the minimum number of S-blocks that are activated during the first cycles and thereby reduce the processes of cipher arrival to one or two cycle's random substitution. Using this proposal, new ciphers called SHUP have been developed and Rijndael-256 and Kalina-256 have been upgraded. In particular:

Table 7 Cyclic values of the maximums of displacements of linear cases when encrypted with 16-bit blocks for the Rijndael cipher and the SHUP-1M cipher

Number cycles *r*	Cipher Rijndael		Cipher SHUP-1M	
	Bias maximum value	RMS deviation	The value of the maximum total differential with S-blocks of the Muhomor	The value of the maximum of the total differential with random S-blocks
1	110008,39	0	810	828
2	9284,27	± 657,454	825	820
3	818,47	± 26,8809	828	819
4	814,19	± 28,204	825	818
5	818,51	± 18,536	828	837
6	815,967	± 20,18	824	814
7	832,31	± 33,1887	820	822

- the SHUP-1 cipher (SHUP-1M), which provides activation for the first three cycles of about 33 S-blocks. Therefore, for a cipher to arrive at a state of random substitution, it is enough for four cycles

- the SHUP-2 cipher (SHUP-2M) provides activation for the first three cycles of about 65 S-blocks. It will take three cycles to arrive at the random substitution state.

- the Rijndael-256 with advanced first cycle with two shutter speeds controlled, with a minimum number of S-blocks activated in the first two cycles equal to 55, and in three cycles the number of activated S-blocks will already be equal to 87. This cipher with their relatives With S-blocks, it will be enough for two cycles to arrive at a cipher, and with a

random S-block the cipher will arrive at a random substitution in three cycles. This also applies to the Kalina-256 cipher with an advanced first cycle.

- the Kalina-256 with an improved first cycle has a minimum number of S-blocks, which are activated on the first two cycles, also close to 55, and three to 87.

The above results indicate that the use of random substitutions does not lead to the exceeding of the minimum number of cycles in which standard solutions ensure the arrival of ciphers to the state of random substitution, which allows to conclude that the improved ciphers when using random S-blocks do not concede to known structures are not stable not on speed. Moreover, the proposed solution gives a gain in the number of cycles of arrival to the state of random substitution for one or two cycles.

The data presented for estimating the prospects of using random S-blocks show that random S-blocks can be used without any reduction in stability, and, as the results of the experiments show, these random S-blocks can be taken directly from the output of the random substitution generator with virtually no validation.

An additional useful result is the possibility of increasing the speed of ciphers by reducing the number of cycles of encryption6.

VI CONCLUSION

The main scientific result of the robot is the following: the ability to activate the SPN ciphers, which can be used without any lower speed, but the S-blocks.

It can be implemented by applying a new design to the cipher function, which can be used in a multi-cycle execution to construct individual constructions of the SHUP ciphers or as a (second) first cycle of any of the known ciphers, where the first cycle is constructed as a two-layer substitution transformation of the proposed kind. The basis for the construction of each layer was the use in its implementation of a chain of so-called controlled substitutions, when the substitutions are included in a serial chain, in which the segment of the output of the previous enlarged S-block (SL transformation) is added to the input of the current enlarged S-block (SL transformation).

The results show that this design of the loop transform has the feature that allows to activate almost all S-blocks of the second layer of the chain from the controlled substitutions. As a result, the minimum number of activated S-blocks reaches a maximum

that cannot be implemented by cycle functions built in the traditional way. Due to this it is possible to provide high cryptographic properties of ciphers even when using random substitutions. Stock by the number of activated S-blocks allows the transition of ciphers to the state of random substitution for the number of cycles that is one or two cycles smaller than traditional methods of constructing cycle functions, and this allows you to set and solve the problem of reducing the required number of cycles of encryption, that is, increase the speed upgraded encryption algorithms.

Thus, a new direction of improvement of modern block symmetric encryption technologies has been opened, which deserves support and development.

REFERENCES

[1] Keliher, H. Meijer, and S. Tavares, “New method for upper bounding the maximum average linear hull probability for SPNs,” Advances in Cryptology, Proceedings of Eurocrypt '01, LNCS 2045, B. Pfitzmann, Ed., Springer Verlag, 2001, pp. 420–436.

[2] F. Sano, K. Ohkuma, H. Shimizu, S. Kawamura. On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis / IEICE Trans. Fundamentals, vol. E86-a, NO.1 January 2003, pp. 37-46.

[3] S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon and I. Cho, Provable Security against Differential and Linear cryptana

[4] 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 s.

[5] Lisitsky K.E. Maximum values of full differentials and linear cases of block symmetric ciphers / K.E. Lisitsky // Technological audit and production reserves. – 2014. – No. 1/1 (15) – S. 47-52.

[6] Dolgov V.I. The new concept of block symmetric ciphers design / V.I. Dolgov, I.V. Lisitska, K.Y.e. Lisitskyi // DOI: 10.1615 / Telecom RadEng. v. 76, 2017, i. 2. pages 157-184.

[7] Dolgov V.I. Improved block symmetric cipher Kalina / V.I. Dolgov, I.V. Lisitskaya, K.E. Lissitzky // 0485-8972.– Radio engineering All-Ukrainian. inter. scientific and technical Sat – 2016. - Vip. 186. - S. 119-131.

[8] Lisitskaya Iryna Impruvd Rijndael / Iryna Lisitskaya, Konstantin Lisitskiy, Mariya Rodinko // Science and Education Studies “Stanford University Press” Volume II No. 1 (17), January- June – 2016. p. 608-618.

[9] Lisickiy K.E. Block cipher with improved dynamic indicators of the condition of a random substitution / K.E. Lisickiy, V.I. Dolgov, I.V. Lisickaya // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International Date of Conference: 10-13 Oct. 2017. Date Added to IEEE Xplore: 04 January 2018 ISBN Information: INSPEC Accession Number: 17484901 DOI: 10.1109 / INFOCOMMST.2017.8246424 Publisher: IEEE.– p. 391-395.

[10] [10] Lisickiy K.E. Cipher with improved dynamic indicators of the condition of a random substitution / K.E. Lisickiy, V.I. Dolgov, I.V. Lisickaya // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International Date of Conference: 10-13 Oct. 2017. Date Added to IEEE Xplore: 04 January 2018 ISBN Information: INSPEC Accession Number: 17484901 DOI: 1109 / INFOCOMMST.2017.8246424 Publisher: IEEE. p. 396-399.

[11] Pat. 118625 Ukraine, IPC H04L 9/06. H04L (2006.01). The way of critical re-creation of dviykhih tributes / Lisitsky K.Є. (Ukraine); Hairman Kharkivsky National University imeni V.N. Karazina. Publication of vidomety about a species of patent Patent 11.02.2019, Bull. No. 3. – 6 s. UA.

[12] Pat. 117158 Ukraine, IPC H04L 9/06. H04L (2006.01). The way of formulating cyclic keys for block symmetric ciphers / Dolgov V.I., Gorbenko I.D., Lisitsky K.Є. that inshi (Ukraine); hairline PAT IIT m. Kharkiv. Publication of the home of 06/25/2018, Bull. No. 12 is about a patent. – 6 s. UA.

[13] Pat. 111448 Ukraine, IPC H04L 29/14 (2006.01) H04L 9/14 (2006.01) H04L 9/06 (2006.01). The way of cryptographic re-creation of dvukh tributes / Gorbenko I.D., Dolgov V.I., Lisitska I.V. Lissitzky K.E. that inshi (Ukraine); Applicant JSC IIT metro Kharkiv. No. a201503976; declared 04/25/2015; publ. 04/25/2016, Bull. No. 8 – 20 s.

[14] Susan Landau. Polynomials in the Nation’s Service: Using Algebra to Design the Advanced Encryption Standard, February, 2004.

[15] W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, in Advances in Cryptology: Eurocrypt ’89, W. Meier and O. Staffelbach eds., Springer-Verlag, Berlin, 1989.

[16] J. Pieprzyk, Nonlinearity of exponent permutations, in Advances in Cryptology: Eurocrypt ’89, J. Pieprzyk, J Quisquater and J. Vandewalle, eds., Springer-Verlag, Berlin, 1990, pp. 89-92.

[17] J. Pieprzyk, On Bent Permutations, Technical Report CS91 / 11, Department of Computer Science, University of New South Wales; presented at International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas, 1991.

[18] K. Nyberg, Differentially uniform mappings for cryptography, in Advances in Cryptology: Eurocrypt ’93, T. Helleseth, ed., Springer-Verlag, Berlin, 1994, pp. 53-64.

[19] J. Daemen, Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis, Ph.D. thesis, Katholieke Universiteit, Leuven, Belgium, 1995.

[20] V. Ridjmen, J. Daemen, B. Preneel, A. Bosselaers, and E. De Win, The cipher SHARK, in Fast Software Encryption: Third International Workshop, D. Gollman, ed., Springer-Verlag, Berlin, 1996, pp. 99-112.

[21] T. Jakobsen and L. Knudsen, Attacks on block ciphers of low algebraic degree, J. Cryptology 14 (2001), pp. 197-210.

[22] J. Daemen, L. Knudsen, and V. Ridjmen, The Block Cipher Square, in Fast Software Encryption, E. Biham ed., LNCS 1267, Springer-Verlag, Berlin, 1997.

[23] Rodinko M.YU. The wide trail strategy with out separable ciphers / M.YU. Rodinko, K.E. Lisitskiy // Radio engineering All-Ukrainian. inter. scientific and technical Sat – 2015. – VIP. 181. - S. 40-45.

[24] Information technology. Cryptographic zahist infomatsiï. Algorithm of symmetric block rebuilding: DSTU 7624: 2014. - K .: Derzhspozhivstandart Ukrainy, 2015. – 238 p. – (National Standard of Ukraine).

[25] Information technology. Cryptographic information security. Block ciphers. GOST R 34.12 – 2015.– Moscow Standartinform. 2015. 21 s. (National Standard of the Russian Federation).

[26] Golovashich S.A. Specification of the Labyrinth Symmetric Block Encryption Algorithm / S.A. Golovashich // Applied Radio Electronics. - Kharkov: KhTURE. - 2007. – Volume 6, No. 2. - S. 230-240. "Fort".

[27] Daemen and V. Ridjmen. The Design of Rijndael: AES - the Advanced Encryption Standard, Springer-Verlag, Berlin, 2002.

[28] X. Lai. On the design and security of block ciphers / X. Lai. // volume 1 of ETH Series in Information Processing. Hartung-Gorre Verlag, 1992.

[29] X. Lai. A proposal for a new block encryption standard. / X. Lai and J. Massey. // In I. Damg˚ard, editor, Advances in Cryptology - EUROCRYPT'90, volume 473 of Lecture Notes in Computer Science, pages 389–404. Springer-Verlag, 1991.

[30] Gorbenko I.D. Perspective block symmetric cipher "Fly agaric" - the main position and specificity / I.D. Gorbenko, M.F. Bondarenko, V.I. Dolgov, R.V. Олійников та інші // Applied Radioelectronics. - Kharkov: KhTURE. - 2007. - Volume 6, No. 2. – S. 147-157.

[31] The state standard of the Republic of Belarus. STB 34.101.31-2011. Information Technology. Information security Cryptographic algorithms for encryption and integrity control. It was enforced by resolution of the State Standard of the Republic of Belarus dated January 31, 2011 No. 5. Publishing House of the Gosstandart, Minsk. – 2011 .-- 35 p.

[32] Gorbenko I.D. On the dynamics of the arrival of block symmetric ciphers to random substitution / I.D. Gorbenko, K.E. Lisitsky // Radio engineering: All-Ukrainian. inter. scientific and technical Sat - 2014 .– Vip. 176. - S. 27-39.

[33] Gorbenko I.D. Refined indicators of the arrival of ciphers to the state of random substitution / I.D. Gorbenko, Lisitskaya I.V., Lisitsky K.E. // Applied Radio Electronics. - Kharkov: KNURE. – 2014. – Vol. 13, No. 3. – S. 213-216.

[34] Lisickiy K.E. Block cipher with improved dynamic indicators of the condition of a random substitution / K.E. Lisickiy, V.I. Dolgov, I.V. Lisickaya // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International Date of Conference: 10-13 Oct. 2017. Date Added to IEEE Xplore: 04 January 2018 ISBN Information: INSPEC Accession Number: 17484901 DOI: 10.1109 / INFOCOMMST.2017.8246424 Publisher: IEEE. – p. 391-395.

[35] Pascale S. The degrees of completeness, of avalanche effect, and of strict avalanche criterion for MARS, RC6, Rijndael, Serpent, and Twofish with reduced number of rounds. / S. Pascale // Siemens AG, ZT IK 3. April 3, 2000.

[36] Lisitskaya I.V. Comparative analysis of the mechanisms of formation of the avalanche effect in DES and GOST 28147-89 / I.V. Lisitskaya, A.S. Bondarenko, T.V. Tsepurit // Information-Keruyuchi systems for out-of-town transport. – 1999. – No. 3. – S.24-30.

[37] Bronstein I.N. Math reference book for engineers and college students. / I.N. Bronstein, K.A. Semendyaev // Publishing house M :. Science – 1980, 976 pp.

[38] Lisitskaya I.V. Large ciphers − random substitutions. Comparison of the differential and linear properties of ciphers submitted to the Ukrainian competition and their reduced models / I.V. Lisitskaya, A.A. Nastenko, K.E. Lisitsky // Automated control systems and automation devices. – 2012.– Iss. 159. – S. 4-10.

If we assume that for the 32-bit platform to perform the SL transformation operation, it is necessary to spend the time *T*, then for a separate line (cycle) of *m*
SL transforms, it will be necessary to spend *mT* sec.

In pipelining, each next *s*-th cycle will start with a delay (s−1) *T* sec, $1 \leq s \leq r$. As a result, if *rm* sec is required to process r cycles for one-stream encryption, then for parallel processing of r cycles it will be sufficient to spend m + r − 1 second. Therefore, the gain in speed that can be achieve will be:

If the cipher is constructed using 32-bit SL transformations, then for $r = 7$, $m = 8$ we have a gain in the speed of computing the last seven encoding cycles

$$\frac{mr}{m+r-1} = \frac{8\times 7}{8+6} = \frac{56}{14} = 4$$

Times, and taking into account the first cycle, we have:

$$\cdot \frac{mr+m}{m+r-1+m} = \frac{8\times 8}{2\times 8+6} = \frac{64}{22} = 2{,}9 \cdot$$

As a result, the gain is almost three times.

Thus, the ciphers described by the PMC are present as the most promising solutions for building modern ciphers.

CONCLUSIONS.

The new cipher described in the paper, called the PCM, seems to be a promising solution for building a modern SPN cipher. He possesses the best-known ciphers with dynamic

exponents of arrival to random substitution [4-40]. In practice, it becomes an accidental substitution after only two cycles. According to other indicators of persistence, this cipher inherited all the high indices characteristic of the "Amanita" cipher [2]. We also note an important feature of the cipher, which is that in the cipher, random
S-blocks can be using with little or no reduction in the dynamic cipher arrival rates to random substitution.

REFERENCES

[1] Dolgov V.I. Novaya kontseptsiya proektirovaniya blochnykh simmetrichnykh shifrov / V.I. Dolgov, I.V. Lisitskaya, K.E. Lisitskii // 0485-8972. – Radiotekhnika – Vseukr. mezhved. nauchn.-tekhn. sb. 2016. – Vip.186. – S. 132-152. (in Russian).

[2] Gorbenko I.D. Perspektivnii blokovii simetrichnii shifr «Mukhomor» – osnovni polozhennya ta spetsifikatsiya / I.D. Gorbenko, M.F. Bondarenko, V.I. Dolgov, R.V. Oliinikov ta inshi // Prikladnaya radioelektronika. – Khar'kov: KhTURE. – 2007. – Tom. 6, №2. – S. 147-157. (in Ukrainian).

[3] Matematicheskaya entsiklopediya: V 5 t. / Gl. red. Vinogradov I.M. - M.: Sovetskaya entsiklopediya, 1979. - T.2: D-KOO. - 278 s. (in Russian).

[4] Gorbenko I.D. Svoistva i vozmozhnosti optimizatsii kriptograficheskikh preobrazovanii v AES – RIJNDAEL / I.D. Gorbenko, D.A. Chekalin // Radiotekhnika. Vseukr. Mezhved. nauch.-tekhn. sb. 2001. Vyp 119. S. 36-42. (in Russian).

[5] Kuznetsov, O., Gorbenko, Y., Kolovanova, I. Combinatorial properties of block symmetric ciphers key schedule. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 55-58. DOI: 10.1109/INFOCOMMST.2016.7905334

[6] Kuznetsov, O., Lutsenko, M., Ivanenko, D. Strumok stream cipher: Specification and basic properties // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016,, pp. 59-62.

[7] Kuznetsov, A.A., Smirnov, A.A., Danilenko, D.A., Berezovsky, A. The statistical analysis of a network traffic for the intrusion detection and prevention systems // Telecommunications and Radio Engineering. - Volume 74, 2015, Issue 1, pages 61-78. DOI: 10.1615/TelecomRadEng.v74.i1.60

[8] Karpenko O., Kuznetsov A., Sai V. Stasev Yu. Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. - Volume 71, 2012 Issue 1. pages 91-98.

[9] Yuriy Izbenko, Vladislav Kovtun, Alexandr Kuznetsov. The design of boolean functions by modified hill climbing method // Information technology – New Generation, 2009. ITNG'2009. Proceedings of the 6th International Conference on Information Technology: New Generations, April 27-29, Las Vegas, Nevada, USA., pp: 356-361. DOI: 10.1007/s10559-007-0052-8

[10] Naumenko, N.I., Stasev, Yu.V., Kuznetsov, A.A. Methods of synthesis of signals with prescribed properties // Cybernetics and Systems Analysis, Volume 43, Issue 3, May 2007, Pages 321-326.

[11] Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1 – 11. DOI: 10.1007/s10559-007-0021-2

[12] Stasev Yu. V., Kuznetsov A.A. Asymmetric Cipher-Theoretical Schemes Constructed with the Use of Algebraic Geometric Ciphers // Cybernetics and Systems Analysis, Volume 41, Issue 3, May 2005, Pages 354 – 363. DOI: 10.1007/s10559-005-0069-9

[13] Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. - Volume 75, 2016 Issue 2. pages 169-178.

[14] Oliynykov R., Gorbenko I., Dolgov V., Kaidalov D. Improvement for distinguisher efficiency of the 3-round Feistel network and a random permutation // Proceedings of the 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS'2011, 2011, pp 743 - 746.

[15] Gorbenko, I.D., Dolgov, V.I.,Rublinetskii, V.I.,Korovkin, K.V. Methods of Information Protection in Communications Systems and Methods of Their Cryptoanalysis // Telecommunications and Radio Engineering. - Volume 52, 1998 Issue 4, pages 89-96.

[16] Gorbenko, I., Ponomar, V. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application // EasternEuropean Journal of Enterprise Technologies. - Vol 2, No 9 (86) (2017), pages 21-32.

[17] Gorbenko, I., Hanzia, R. Examination and implementation of the fast method for computing the order of elliptic curve // EasternEuropean Journal of Enterprise Technologies. - Vol 2, No 9 (86) (2017), pages 11-21.

[18] Gorbenko, I.,Yesina, M.,Ponomar, V. Anonymous electronic signature method // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 47-50. DOI: 10.1109/INFOCOMMST.2016.7905332

[19] Gorbenko, Y., Svatovskiy, I., Shevtsov, O. Post-quantum message authentication cryptography based on error-correcting ciphers // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 51-54. DOI: 10.1109/INFOCOMMST.2016.7905333

[20] Gavrylko, R.O.,Gorbenko, Yu.I. A physical quantum random number generator based on splitting a beam of photons // // Telecommunications and Radio Engineering. - Volume 75, 2016 Issue 2, pages 179-188. DOI: 10.1615/TelecomRadEng.v75.i2.70

[21] Kazymyrov, O.,Oliynykov, R.,Raddum, H. Influence of addition modulo 2n on algebraic attacks // Cryptography and Communications. – April 2016, Volume 8, Issue 2, pp 277–289.

[22] Kaidalov, D.,Oliynykov, R.,Kazymyrov, O. A method for security estimation of the SPN-based block cipher against related-key attacks // Tatra Mountains Mathematical Publications. Volume 60, Issue 1, Pages 25–45.

[23] Oliynykov, R.,Oleshko, O.,Lisitskiy, K. Differential properties of random substitutions // Modern Problems of Radio Engineering, Telecommunications and Computer Science - Proceedings of the 10th International Conference, TCSET'2010, February 23-27, 2010, Lviv-Slavske, Ukraine, p 75.

[24] Ruzhentsev V., Oliynykov R., Properties of Linear Transformations for Symmetric Block Ciphers on the basis of MDS-ciphers // Proceedings of the 6th International Conference on Network Architecture and Information System Security SAR-SSI 2011, pp. 193-196.

[25] Ruzhentsev, V.,Oliynykov, R., Stupak, V. Construction of MDS-matrix for linear transformation of symmetric block ciphers // 2010 International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv-Slavske, 2010, pp. 284-284.

[26] Rodinko, M.,Oliynykov, R.,Gorbenko, Y. Improvement of the high nonlinear S-boxes generation method. // 2016 Third International Scientific-Practical Conference

Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 63-66.

[27] Grachev, V.M., Esin, V.I., Polukhina, N.G., Rassomakhin, S.G. Technology for developing databases of information systems // Bulletin of the Lebedev Physics Institute. 05/2014; 41(5):119-122.

[28] Grachev, V.M., Esin, V.I., Polukhina, N.G., Rassomakhin, S.G. Data security mechanisms implemented in the database with universal model // Bulletin of the Lebedev Physics Institute. May 2014, Volume 41, Issue 5, pp 123-126.

[29] Lavrovska, T., Rassomahin, S. Physical model of pseudorandom ciphers in multidimensional Euclidean space. // 016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 67-70. DOI: 10.1109/INFOCOMMST.2016.7905337

[30] Krasnobayev V.A., Yanko A.S., Koshman S.A. A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. – January 2016. – Volume 52, Issue 1, pp. 145-150.

[31] Krasnobayev V.A., Koshman S.A., Mavrina M.A. A Method for Increasing the Reliability of Verification of Data Represented in a Residue Number System // Cybernetics and Systems Analysis. – November 2014, Volume 50, Issue 6, pp 969–976.

[32] Andrushkevych, A., Kuznetsova, T., Bilozertsev I., Bohucharskyi, S. The block symmetric ciphers in the post-quantum period. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 43-46. DOI: 10.1109/INFOCOMMST.2016.7905331

[33] Oleksandr Potii, Oleg Illiashenko, Dmitry Komin. Advanced Security Assurance Case Based on ISO/IEC 15408. // Theory and Engineering of Complex Systems and Dependability Advances in Intelligent Systems and Computing Volume 365, 2015, pp 391-401.

[34] Potii A.V., Pesterev A.K. A System Approach to Certification of Pseudorandom Numbers Generators Used in Information Protection Systems // Telecommunications and Radio Engineering. - Volume 52, 1998 Issue 4. pages 97-102.

[35] Brumnik R., Kovtun V., Okhrimenko A., and Kavun S. (2014). Techniques for Performance Improvement of Integer Multiplication in Cryptographic Applications, Mathematical Problems in Engineering, vol. 2014, Article ID 863617, 7 pages, 2014.

[36] Trydid, O., Kavun, S., Goykhman, M. (2014). Synthesis concept of information and analytical support for bank security system. Actual Problems of Economics,11(161), 449-461.

[37] Irina Lisitskaya, Tatiana Grinenko, Stanislav Bezsonov. Differential and Linear Properties Analysis of the Ciphers Rijndael, Serpent, Threefish with 16-bit Inputs and Outputs // EasternEuropean Journal of Enterprise Technologies. - Vol 5, No 4 (77) (2015), pages 50-54.

[38] Dolgov, V.I.,Lisitska, I.V.,Lisitskyi, K.Ye. The new concept of block symmetric ciphers design // // Telecommunications and Radio Engineering. - Volume 76, 2017 Issue 2. pages 157-184.

[39] Nelasa, A., Dolgov, V., Pogorily, A. Digital signature protocol for corporate network // 2008 International Conference on "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET), Lviv-Slavsko, 2008, pp. 396-397.

[40] Mitrophanov, Yu.I.,Dolgov, V.I. Dynamic control of service rates in queuing networks // Automatic Control and Computer Sciences. - December 2008, Volume 42, Issue 6, pp 311–319.