computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

BLOCK SYMMETRIC CIPHER WITH RANDOM S-BOXES

Konstantin Lisickiy [1,2], Victor Dolgov [1,2], Iryna Lisickaya [1], Kateryna Kuznetsova [1]

[1] V. N. Karazin Kharkiv National University, Svobody sq., 6, Kharkiv, 61022, Ukraine,
konstantin.lisickiy@mail.ru, dolgovvi@mail.ru, kate7smith12@gmail.com
[2] JSC "Institute of Information Technologies", Bakulin St., 12, Kharkiv, 61166, Ukraine

Paper history:
Received 8 January 2019
Received in revised form 17 March 2019
Accepted 22 March 2019
Available online 31 March 2019

Keywords:
controlled enlarged S-blocks;
dynamic cipher indicators;
active S-blocks;
random S-blocks;
indicators of randomness;
indicators of strength;
pipeline processing.

Abstract: This paper describes a new 256-bit block symmetric substitution-permutation cipher, called managed substitution cipher. This is a cipher with single-layer permutated transformations in each cycle. The management of substituted transformations occur by including them in a chain so that the output value of the previous SL transform is fed to the input of the current fortified 32-bit substituted transformation (SL conversion) along with the current value of the input data block through the adder for modulo 2. This enables to activate almost all S-blocks of the second cycle and subsequent cycles and eventually improve the dynamic indicators of the arrival of the cipher to the state of random substitution. The results of the evaluation of randomness indicators and the possibility of using random S-blocks are given. It is shown that such construction of cycled function allows us to use random substitutions without any selection in a cipher without reducing its strength.

1. INTRODUCTION

In our work [1], we propose the design of MSC-1 (managed substitution cipher) with improved indicators of the arrival to a random setting. The improvement of the indicators of the randomness of this cipher was achieved by using the cyclic functions of controlled substitutions during its construction. When the operations of non-linear and linear transformation of substitution-permutation network (SPN) cipher were combined into one common inseparable operation, built on the basis of including enlarged S-blocks (SL transformations) of the cycle function into a chain so that the next segment of the input data block after its addition for modulo 2 with the result of passing of the previous enlarged S-block would enter the input of the current S-block, there is where the name comes from. Here, the result of passing of the previous S-box was considered as a control input.

In this work, in order to increase the efficiency of the cycle transformation, we applied the operation of adding modulo 2 at the input of the first SL conversion at the input of the cycle function and suggested that it would help to exclude activation of only one S-block in the first cycle. However, as it turned out during the research process, this approach has proven to be erroneous. It allowed to increase the number of the activated S-blocks by activating a cipher by a single-byte difference, but did not rule out the possibility of activating one S-block of the first cycle in the case of several nonzero differences of the input data block. For instance, for eight input $\Delta X_1 = \Delta X_8 = \Delta \neq 0$, $\Delta X_2 = \Delta X_3 = \Delta X_4 = X_5 = \Delta X_6 = \Delta X_7 = 0$. This means that the "improvement" given in [1] is redundant, it does not work.

In general, the assertion turned out to be true, that for SPN ciphers with cyclic functions that use single-layer permutation transformations, the minimum number of activated S-blocks of the first cycle is one.

2. THE PURPOSE OF THE RESEARCH

The aim of this work is further improvement of the structure of ciphers with the managed substitutions, and also the additional basis of the real possibility of constructing of the 256-bit SPN ciphers by using casual substitutions practically without their selection. It will be realized due to the increasing of a minimum number of S-blocks, which are activated on the first cycles of SPN of ciphers.

Increasing of minimum number of S-blocks, activated on the first cycles, allows us to create ciphers with the diminished number of cycles of enciphering.

The set problem is to clarify the positions of the work [1] and to cite additional arguments that confirm their authenticity.

In this work we propose the modernisation of MCS-1 cipher, which we named the MSC-1M cipher, where the supplementary additions of segments of entrance block of data on the entry of SL transformation of the first cycle are excluded. Additions of exit of the last SL transformation with exits of the previous one are also eliminated, except the adding up with the exit of the first SL transformation.

Here we also have the opportunity to correct a number of other assertions and estimates made in the process [1], which are related with the erroneous assumptions noted above, although the general considerations regarding efficiency improvements proposed in the process [1] are preserved.

3. RELATED WORKS

Among leaders of technologies of the sectional symmetric enciphering in [1], two such developments were adopted: the Rijndael cipher, that won the AES and NESSIE competitions [2], and the IDEA NXT cipher, that appeared on the basis of the IDEA cipher (International Data Encryption Algorithm – the International algorithm of enciphering of data [3]), that was worked out as the offered standard of enciphering [4].

The work of Susan Landau [5], which is devoted to the analysis of the origins of the emergence of the new AES standard, the discussion and evaluation of the perspective of the major project decisions, that supported the standard by the world cryptographic community, was considered in the process of completing the review. This development became the appropriate result of development of world cryptographic idea.

In the cited work the attention is focused on projecting the sectional ciphers. The author observes the ways, which led to the Rijndael cipher, which is the last word in project and engineering solutions nowadays. This work-out became a result of development of world cryptographic thought.

A number of papers and proposals, performed on the way to Rijndael, are noted in [5]. They should be mentioned here.

Willi Meier and Othmar Staffelbach suggested that certain examples of non-linearities, used by mathematicians, might be convenient for a cryptographic systems project [6]. Based on these ideas, Josef Pieprzyk proposed algebraic methods for the construction of nonlinear functions [7, 8]. Kaisa Nyberg researched S-blocks and applied some of Pieprzyk's ideas, while designing S-blocks [9]. Joan Daemen studied the cyclic functions from the point of view of differential and linear cryptanalysis of the cipher and proposed a new paradigm of the wide trace approach [10]. He and other researchers used the wide footprint and Nyberg S-blocks in the SHARK cryptosystem [11]. Thomas Jakobsen and Lars Knudsen found an "interpolation attack" against simple algebraic ciphers, such as SHARK [12]. Two SHARK developers, Daemen and Vincent Rijmen, were opposed to the Square cryptosystem [13]. Knudsen hacked Square, by using various attacking methods [14]. Rijndael, as it was noted by the author of the cited work, rose from the ashes of Square. Further in the work it is traced, how these threads weaved Rijndael.

In the work, significant attention is paid to the analysis of the design methods of Rijndael of the new paradigm; an approach, that is considered to be developed by Joan Daemen, received the name of a broad-based strategy.

Saying about the broad-based strategy, Susan Landau notes that cryptanalysis is most easily performed when a single 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 thing that the designer can do in reaching the upper limit, is that the number of branches B is equal to $n + 1$, where n is the number of connections (each link consists of m bits). The reverse linear mapping that achieves this effect is called optimal. Daemen and Rijmen managed to build such mapping. They showed that separable codes with a maximum minimum distance (MDV codes) provide a way to construct such optimal linear transformations. This mapping is much more effective than many other linear transformations, used in ciphers before.

Further we will consider in detail the principles of the construction and properties of block symmetric IDEAs of similar ciphers [14], and also highlight the features of the construction of the Muchomor ciphers [15, 16], the block cipher from the Belarusian standard STB 34.101. 31-2011, the new standard of block symmetric encryption of Ukraine Kalina-2 [17] and the new Russian standard "Kuznechik" [18].

The review of the features of constructing these well-known structures is given in [1], we focus on the conclusions we made.

The main ones are the following [19-25]:

1. Large achievement of modern design solutions referring to the construction of ciphers should be considered as the implementation of a broad-based

strategy based on matrix multiplication in field extensions.

2. The design principles (noticed below), applied by the AES developers, are worthy of approval and support:

- Simplicity of the specification and the analysis;
- Transparency;
- Efficiency.

3. The newly promoted concept of flexible encryption is definitely a step forward in block-symmetric encryption technologies and can be easily implemented by using many other developments, and not just with the help of the IDEA NXT family of ciphers.

4. The approaches and the results of evaluation of indicators of cipher strength to attacks of differential and linear cryptanalysis, given in the publications, is approximated and needed to be clarified.

5. Nowadays there is an approach that allows us to determine the exact indicators of strength of block symmetric ciphers to attacks of differential and linear cryptanalysis by computing way. According to this approach, the IDEA NXT ciphers, mentioned here, considering their indicators, are at the level of strength indicators implemented by many other ciphers. Nevertheless, the considered development, as well as the code Kalina-2, in this respect has some advantages over many others (Rijndael and another ciphers, presented on the Ukrainian competition. In these three mentioned developments (Muchomor, IDEA NXT, Kalina-2), it is possible to implement dynamic indicators of cipher arriving to a random substitution, reduced by one cycle, compared to other known solutions.

6. In recent developments (Muchomor, IDEA NXT) there is a desire to improve the dynamic characteristics of ciphers arrival to the established (stationary) values of the maxima of complete differentials and linear case on the basis of increasing the number of S-blocks, used in cyclic functions, and creating mechanisms for increasing the minimum number of S-blocks, that are activated in the first cycles. This allowed us to bring the avalanche indicators of the ciphers of the latest developments to the depth of the avalanche effect, which is equal to two cycles (but these are not SPN ciphers).

Next we want to express new ideas and proposals, aimed at further improving the technologies of designing and developing block symmetric ciphers.

Today, looking back over the past period of the development of technologies of block symmetric encryption, associated with allocated ciphers, it can be noted that there has already been accumulated critical material, which suggests that not all solutions used by developers in these ciphers are the most perfect.

First of all, we want to pay attention to the fact that, despite the progressiveness of the solutions, adopted by the developers of modern ciphers, not all potential opportunities ensuring the effectiveness of the implementation of initial cyclical transformations are realized in them. Thus, according to the dynamic indicators of the arrival of random substitution, the 128-bit Rijndael cipher becomes a random substitution of the differential indices in the third cycle, and according to linear indicators – only in the fourth [21, 22]. This is due to the fact, that one byte of the input of the first cycle activates only one S-block of the first cycle, on the second cycle it activates four S-blocks and on the third one – all sixteen S-blocks. As a result, in three cycles, there are 21 active S-blocks as minimum, that allows the cipher to reach the state of random substitution in the third cycle by the differential indicators. But the cipher needs an additional fourth cycle for achieving the state of random substitution on the linear indicators. The 256-bit AES cipher comes in the form of random substitution with differential metrics in 4 cycles, and with linear values in 5-th. So, the broad-based strategy, implemented in the Rijndael cipher, has a weakness (activating only part of the S-blocks of the second and other cycles), which leads to the delay in the process of achieving the state of random substitution by the cipher. Similar Rijndael ciphers have similar disadvantages.

The ciphers of Kalina-2, Muchomor and the cipher from the Belarusian standard refer to the most progressive of the considered designs. These ciphers implement indicators of reaching the state of random substitution, which are close to the limit indicators (Cousins of Flies and ciphers from the Belarusian standard are not SPN ciphers).

It should be mentioned that according to new method of estimating the evidence of the proof of block symmetric ciphers against the attacks of differential and linear cryptanalysis, has been proposed recently [1, 22], all ciphers (including Rijndael) asymptotically become random substitutions, and their strength indicators are not related with the properties of the S-blocks included in the cipher. S-blocks influence the dynamics of the arrival of the cipher to the state of random substitution only (the number of cycles, required for the cipher to come to the random substitution indicators by differential and linear indicators). We also pay attention to the practice of designing modern ciphers: the number of encryption cycles in them is chosen in such a way, that they are three/four times the number of cycles, required for the cipher coming by the differential and linear properties to the indices of random substitution (the supply of strength). For the AES competition, according to its requirements, the authors fixed the minimum length of the encrypted block equal to 128 bits (in the form of a square (state matrix) of 4×4 bytes), and for the 128-bit key the number of cipher circles is equal to 10, that is on the verge of strength. The using of S-blocks with worse differential and linear values outputs a cipher beyond the established strength reserve. Increasing the length of the input block and the keys leads to the solutions with an increased number of encryption cycles (for 196 and 256-bit AES 12 and 14 cycles, respectively). As it turned out, the linear transformation in the form of matrix multiplication, which was the basis for the implementation of the new broad-track strategy, is not the only realized transformation (with the maximum number of branches). Taking into account the conclusion made in [1], it is concluded that the dynamic indicators of ciphers can be improved.

In our view, one more disadvantage is the complicated circuits of deploying the keys in the considered ciphers, which is also noted in the work [1]. The desire to make schemes of deployment of key similar to the avalanche characteristics of the ciphers themselves, is not justified, in our opinion, as our experiments with reduced cipher models [1, 20] showed that ciphers and zero cyclic connections come to random substitutions in the same number of cycles as with non-zero cyclic connections (in regular mode of operation). The randomness indicators of the S-blocks themselves are quite sufficient to make the cipher a random substitution regardless of the values of the key bits.

The presented and not presented results allow us to characterize the state of modern technologies of designing the BSS (focusing on the most progressive of them by the following basic provisions [1, 26-35].

1. It is considered, that the indicators of cipher strength to attacks of differential and linear cryptanalysis are directly related to the values of differential and linear probabilities of nonlinear transformations (S-blocks) included in ciphers. Therefore, in the cryptographic literature, the scientific direction of research, related to the development and search of S-blocks with improved cryptographic indicators, has been developing intensively for a long time.

2. The most progressive solutions to constructing BSRs are the implementation of an iterative, multi-cycle, linear transformation that implements a broad-based strategy (Rijndael, IDEA NXT, Labyrinth, Camellia, Kalina, Muhomor, Grand Cru, etc.).

3. The practice of building block ciphers has determined the number of the used encryption cycles (strength reserve), which is three/four times the depth of the avalanche effect (the number of cycles required for the arrival of the cipher to the state of random substitution).

4. Constructs of cyclic transformations, applied in known ciphers, ensure the arrival of ciphers to the state of random substitution for a minimum number of cycles, exceeding three (the exception is the algorithm of block encryption from the Belarusian standard and the code of the Muholomor).

5. Almost all known developments are oriented on the use of S-blocks with boundary and close to the minimum achievable values of differential and linear indicators.

6. Achieved indicators on the speed of ciphers are characterized by the boundary values of specific costs of XOR operations (cycles), falling on one S-block, close to two (without the cost of execution of the procedure for deployment of keys).

7. The existing concept of constructing key deployment schemes for block symmetric ciphers is focused on the implementation of procedures that approach their own properties to a single cipher transform.

In recent developments (the algorithm of block encryption from the Belarusian standard and also the code of the Muchomor) there is the desire to increase the minimum number of S-blocks of the cyclic functions, that are activated by increasing the number of layers of S-blocks, included in it; but all of them are oriented on using the S-blocks with the values, differential and linear probabilities close to the limit (minimum achievable). To sum up, the task is to increase the minimum number of S-blocks that are activated on the second and other cycles. This work [1] formulated the ideas, that have been put into the developing approach, which allows us to consider it as a new method of constructing block symmetric SPN ciphers, by using of which the code of MSC-1 was built. As it was already noted, further analysis showed the possibility and need for its modernization. We called this upgraded cipher the MSC-1M cipher and further material is devoted to the description of this advanced design.

4. MATERIALS AND METHODS. DESCRIPTION OF CIPHER MSC-1M

Here we can mention the materials presented in [1] with respect to the MSC-1 cipher, since the design of the cipher MSC-1M is almost based on the elements of the design of the cipher MSC-1.

4.1 ALGORITHM PARAMETERS

MSC-1M supports a block length of 256 bits and encryption keys of 256 and 512 bits in length.

The encryption algorithm is a procedure consisting of an iterative encryption transform (cyclic transforms) and final randomization. The number of encryption cycles $N_r = 9$.

4.2 ENCRYPTION PROCEDURE

The input of the procedure is the cleartext and the encryption subkeys. The input data block is processed by the cyclic function a specified number of times (9 times), and finally, there is a randomization, which is performed by using an XOR operation with an additional (10th) cyclic subkey. The resulting data block is a ciphertext.

4.3 CYCLE TRANSFORMATION

The scheme of the cycle transformation MSC-1M is shown in Fig. 1.

The main transformation of the cyclic function is the SL transformation. It repeats the construction of the SL transformation of the Muchomor cipher. Its description is given in [1].

Other eight cycles repeat the construction of the first cycle (for the implementation of pipelined data processing, cycles, starting from the fourth one, are constructed without the addition of the operation of the output of the last SL transformation with the outputs of the previous SL transformations).

4.4 DECRYPTION PROCEDURE

The decryption algorithm is the inverse of the encryption algorithm. The ciphertext blocks and the encryption ciphers are supplied at the input of the algorithm. At the beginning of the decryption procedure, there is the removing of final randomization of the ciphertext, after that the cyclic functions process the received data block the necessary number of times (9 times) in the reverse order. The received data block is a cleartext block. It remains to be noted that when decrypting

- the decryption plugs are also supplied in the reverse order;
- inverse S-blocks are used as substitutions;
- in the SL transformation we use the matrix, which is inverse for the matrix used by encrypting.

A description of the key deployment procedure is also given in [1].

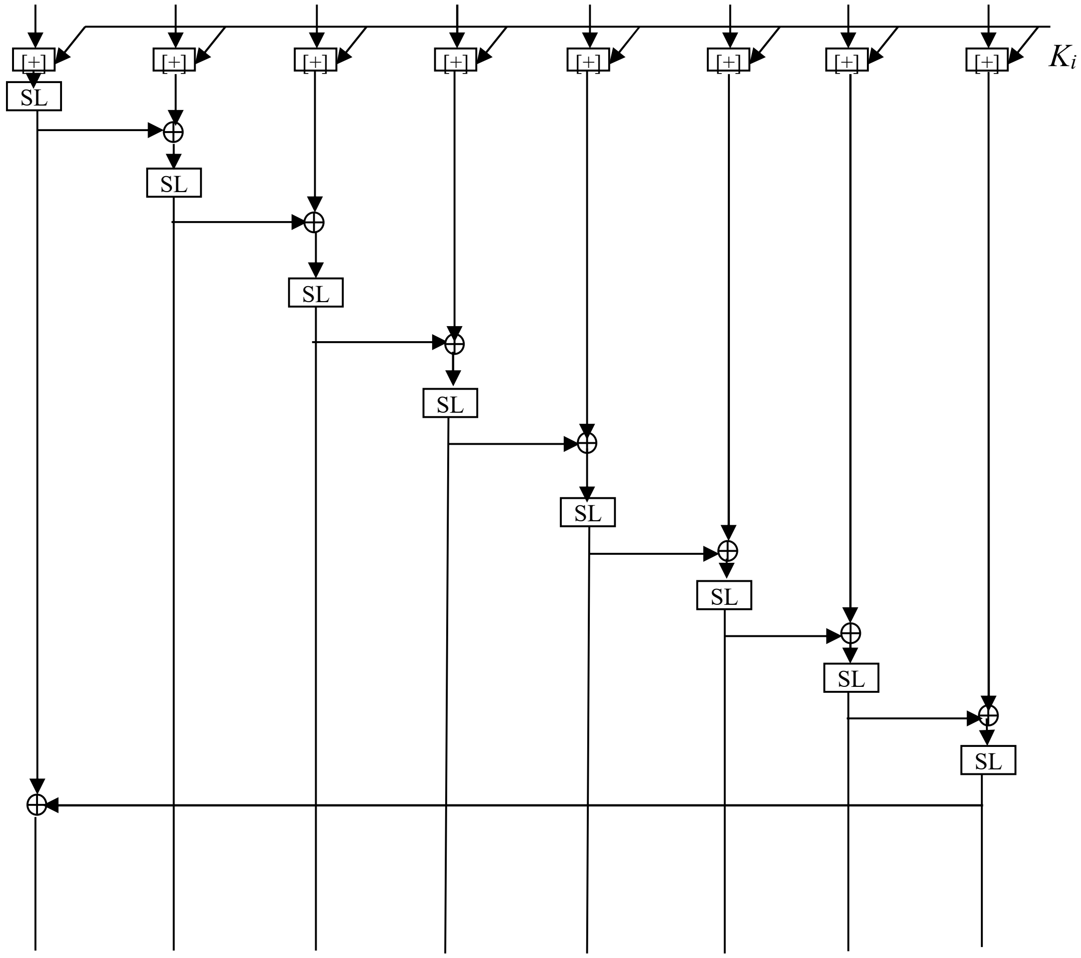

Figure 1 – Block diagram of the cycle transformation MSC-1M

5. INDICATORS OF RANDOMNESS MSC - 1M

In this section, we present the results of estimating the expected parameters of the transition of the MSC to the state of random substitution.

Here we use the considerations and calculations presented in our work [1].

As it is mentioned in [1], the maximum values of linear and differential probabilities (strength indicators) for a cipher with a 256-bit input are obtained close to each other and equal to approximately 2^{248} - 2^{250}.

According to the calculations in [1], for a cipher with a 256-bit input, it is required to reach the state of random substitution by differential indicators when using S-blocks with marginal indicators of δ-uniformity equal to $DP^{\pi}_{\max} = 2^{-6}$, (in accordance with equality $2^{-248} = (2^{-6})^{k}$) more than $k_{\min} = 41$ S-block.

Analogically, to reach the state of random substitution by linear indices when using S-blocks with nonlinearity indicators equal to $LP^{\pi}_{\max} = 2^{-6}$, we need ($2^{-250} = 2^{k-1}\cdot\left(2^{-6}\right)^{k}$) $k_{\min}$=50 S-blocks (for S-blocks of Muchomor cipher with nonlinearity indicator $LP^{\pi}_{\max} =$ 2^{-5}, we have $k_{\min} = 62{,}25$).

In our case, there is one active S-blocks of the first cycle and the second cycle, there are 28+33, and then each SL transformation contains 4th S-blocks, except one or two MDR transitions of conversions to the number of active bytes less than four. Then there will be 60+65 active S-blocks on three cycles, which consist of single-layer substitution transformations. This means, that for S-blocks with limiting differential and linear exponents $DP^{\pi}_{\max} = LP^{\pi}_{\max} = 2^{-6}$, MSC-1M comes to a random substitution with a margin in three cycles.

6. ESTIMATION OF THE PROSPECTS FOR THE USE OF RANDOM S-UNITS IN THE MSC-1M

Here we use the results presented in [1]. Calculations, performed in [1] for 48 active S-blocks when selecting the maximum probable transitions in the rows of the differential table, lead to the following result:

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

This means that random S-blocks for this cipher are also provided for its three cycles to reach the state of random substitution.

For the linear approximation table of a random S-block in [1], calculations were performed for 70 randomly taken rows of the LAT table. The corresponding result is:

$$2^{69}\times\left(\frac{34}{128}\right)^{2}\times\left(\frac{32}{128}\right)^{2}\left(\left(\frac{30}{128}\right)^{2}\right)^{3}\times\left(\left(\frac{28}{128}\right)^{2}\right)^{8}\times$$

$$\times\left(\left(\frac{26}{128}\right)^{2}\right)^{18}\times\left(\left(\frac{24}{128}\right)^{2}\right)^{39}=2^{-257}.\ (2^{-233}).$$

In our cipher, the minimum number of active S-blocks on three cycles satisfies these boundaries with a large margin.

It should be mentioned in conclusion that the 256-bit Rijndael cipher comes to a state of random substitution, both in terms of differential and linear indices only on the fourth cycle.

7. INDICATORS OF COMPUTATIONAL COMPLEXITY

As in [1], when evaluating computational complexity, we will focus on the number of XOR operations performed by the cipher in the process of encryption and decryption. We will proceed from the fact that in order to perform SL transformation (matrix multiplication), three XOR operations are required [21, 22].

Then, in accordance with the structure of the cycle transformation (Fig. 1) we need to perform 1 + 82 + 24 = 41 XOR operations in one cycle of MSC-1M. For 9 cycles we receive the result: 419 + 8 = 377.

In AES-256, for 14 cycles there are 32+14 = 448 XOR, i.e. MSC-1M will be faster than AES.

But it does not take into account the consumption of the master-key deployment procedure.

8. PIPELINE DATA PROCESSING

Pipeline processing can be applied in an iterative cipher, if the operations of its cyclic function do not cover the whole cyclic transformation. Such operation in the ciphers of the series of MSC is the operation of adding the output of the last SL transform to the output of the first SL transform. While this operation is not performed, the cyclic conversion is not completed. Pipelining requires that the cyclic function being built in such a way, that its individual operations can be performed together (at the same time). Therefore, the operations, covering the entire cyclic function, should be excluded. As the experiments have shown, it can be done for the MSC cipher after the cipher has come to the state of random substitution. In particular, in the cipher MSC-1M, after the first three encryption cycles, its other cycles can be built by excluding from the cycle functions the addition operations of the outputs of the last SL transformations with the outputs of the first SL transformations, i.e., cycle transformations on cycles, starting with the third one, should differ from cycle transformations of the first two cycles.

In this case, after forming the output of the first SL transform of the third cycle, we can immediately form the output of the second SL transform of the third cycle, generate the output of the first SL transform of the fourth cycle. After forming the output of the second SL transform of the fourth cycle, form the output of the first SL transform of the fifth cycle, etc.

If we assume, that for a 32-bit platform it is necessary to spend time T sec. to perform the SL conversion operation, then for a separate line (cycle) of m SL transformations, it will be necessary to spend $m\ (T + T_R)$ sec. Here T_R is the time consuming on the performing adding operation of the data segments at the inputs of each of the SL transformations.

At pipelined processing, which start from the fourth cycle.

After the 1st SL transformation of the fourth cycle, while transforming the second SL of the fourth cycle, the first SL of the fifth cycle is calculated at the same time.

At the 3 SL transformation of the fourth cycle, the calculation of the second SL of the fifth cycle conversion and the first SL transformation of the sixth cycle are performed.

At the 4 SL transformation of the fourth cycle calculations of the third SL of the fifth cycle, the second SL of the sixth cycle and the first SL of the seventh cycle are performed.

At the 5 SL transformation of the fourth cycle, calculations of the fourth SL of the fifth cycle, the third SL of the sixth cycle, the second SL of the seventh cycle and the first SL of the eighth cycle are performed.

At the 6 SL transformation of the fourth cycle calculations of the fifth SL of the fifth cycle, the fourth SL of the sixth cycle, the third SL of the seventh cycle, the second SL of the sixth cycle and the first SL of the ninth cycle are performed.

At the 7 SL transformation the fourth cycle calculations of the sixth SL transform of the fifth cycle, the fifth SL transform of the sixth cycle, the fourth SL of the seventh cycle, the third SL of the eighth cycle and the second SL of the ninth cycle are performed.

At the 8 SL of the fourth cycle transformation, the calculations of the passage of the seventh SL of the fifth cycle, the sixth SL of the sixth cycle, the fifth SL of the seventh cycle, the fourth SL of the eighth cycle and the third SL of the ninth cycle are performed.

Then, counting of the transitions that go beyond the boundaries of the 4th cycle is done.

- on the next interval $T + T_R$ sec, the eighth SL transform of the fifth cycle, the seventh SL of the sixth cycle, the sixth SL of the seventh cycle and the fifth SL of the eighth cycle and fourth SL of the ninth cycle are calculated at the same time.
- on the next interval $T + T_R$ sec, the pass of the eighth SL of the sixth cycle, the seventh SL of the seventh cycle, the sixth SL of the eighth cycle and the fifth SL of the ninth cycle is calculated
- on the next interval $T + T_R$ sec, the pass of the eighth SL of the seventh cycle, the seventh SL of the eighth cycle and the sixth SL of the ninth cycle is calculated.
- on the next interval $T + T_R$ sec, the pass of the eighth SL of the eighth cycle and the seventh SL of the ninth cycle is calculated.
- on the next interval $T + T_R$ sec, the pass of the eighth SL of the ninth cycle conversion is calculated,

If the cipher is built by using 32-bit SL transformations, then we have a performance gain in calculating the last six encryption cycles for m = 8 SL transformations, l = 6 cycles

$$\frac{6\times 8}{8+6}=3,4$$

times, and taking into account the first three cycles we have:

$$\frac{9\times 8}{8+6+8\times 3}=1,9.$$

As a result, the gain is close to two.

So, the described cipher, called MSC, is presented as the most promising solution for constructing modern ciphers.

9. EXPERIMENTS

The first part of the experiments is devoted to assessing the randomness indicators of the proposed cipher design. Here are the results of determining the per-cycle laws of the distribution of the XOR maxima of transitions and maxima of the cipher offsets in the mode of its initialization with 16-bit input differences in accordance with the procedure in [1].

Table 1 shows the cyclic distribution law of the XOR difference of the differences for a 256-bit cipher Rijndael in the mode of its initialization by 16-bit differences in accordance with the procedure in work [1].

Calculations for the Rijndael cipher are made for 30 random encryption keys, and for the Cipher MSC-1M for one encryption key. It can be seen that for the Rijndael cipher, the data obtained for the reduced model of this cipher [1, 22] are saved, and the cipher MSC-1M shows the boundary values already from the first cycle.

Indeed, for S-blocks of the cipher, the Amanita with the differential uniformity index = 2^{-5}, the avoidance of encryption for a 16-bit cipher is $2^{-12} = (2^{-5})^k$. This means that in order to reach the state of random substitution, a 16-bit byte S-block is enough for a 16-bit cipher. And if for the Rijndael cipher with XOR operation of introducing cyclic subkeys, the maximum transition value of the first cycle will be equal to 2048 (only one byte of input is enabled), then in the case of MSC-1M with a modular operation of introducing cyclic subkeys 2^{32}, pass one of the input bytes using zero differences fail (in the overwhelming majority of cases two bytes of input are activated at once). But still the minimum number of activated S-blocks of the first cycle is kept equal to one, as in the larger version of the cipher. Experiments confirm that for the conversion of a 256-bit cipher in the usual mode of its application to the state of random substitution at least three cycles are required, and for the Rijndael cipher – four.

Table 2 shows the cyclic distribution law of the maxima of the LAT table offsets for a 256-bit cipher Rijndael also in the mode of its initialization with 16-bit non-zero input and output masks in accordance with the procedure [1, 22].

Table 1. Per-cycle maximums for a 256-bit of total differentials when encrypting with 16-bit blocks of the cipher Rijndael and cipher MSC 1M

Number of cycles, *r*	Cipher Rijndael		Cipher MSC 1M	
	The maximum value of the total differential	RMS deviation	The maximum value of the total differential with S-blocks cipher Muhonor	Maximum value of total differential with random S-blocks
1	2048	0	2560	3072
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	± 1,431394	20	18
9	19,0666	± 1,23648	18	18

Table 2. Per-cycle maximums for a 256-bit of the bias linear hull when encrypting with 16-bit blocks for the cipher Rijndael and cipher MSC 1M

Number of cycles, *r*	Cipher Rijndael		Cipher MSC 1M	
	The maximum value of the bias linear hull	RMS deviation	The maximum value of the of the bias linear hull with S-blocks cipher Muchomor	Maximum value of of the bias linear hull with random S-blocks
1	4096	0	8192	9728
2	9284,27	± 657,454	825	805
3	818,467	± 26,8809	828	828
4	815	± 28,204	825	827
5	818,5	± 18,536	828	837
6	815,967	± 20,18	824	814
7	832,1	± 33,1887	820	822

Calculations for the Rijndael cipher were performed using 10 different encryption keys. For the MSC cipher, one randomly taken key is used for the entire set of cyclic transformations. The fourth column of the table shows the data for the cipher, which uses the Muchomor [15] cipher S-blocks, and the fifth uses random S-blocks taken from the output of the random substitution generator without any filtering. The results show that even in this case, the MSC-1M cipher in the normal application mode comes to a state of random substitution in three cycles, which confirms the increased efficiency of this design. Experiments confirm the connection of the number of activated S-blocks in the first cycles with the minimum number of encryption cycles necessary for the cipher to reach the state of random substitution.

10. DISCUSSION

In our view, a random substitution from the output of random substitute's generator can be a good S-block with the great probability. This is confirmed by numerous experiments. But taking into account still small research of using the random substitutions for constructing ciphers and the rather critical attitude of most specialists to this model, it is proposed to consider a random substitution from the output of the random substitute generators as an improved model of random substitution, which is tested for compliance with a minimum of four indicators of the S-block and Boolean functions that form it:

1. The maximum value of the XOR transition is in the range of 8-10.
2. The maximum value of the displacement of LAT is in the range 32-34 (that is, the nonlinearity is equal to 94-96).
3. Algebraic degree of Boolean functions is not less than 7.
4. The indicator of algebraic immunity of the S-block is not less than 3.

It is interesting that, as the experiments have shown in [1], random substitutions obtained without any restrictions, with a very high probability proved to be suitable in terms of cryptographic applications. They allowed to provide dynamic indicators of output of ciphers with strong linear transformations to asymptotic indicators of random substitutions, which are not inferior to the best (selected by special methods) S-blocks of practically all modern ciphers.

From the previous results of determining the randomness of the considered cipher, we can conclude that the proposed construction of the cipher really allows to use in it random S-blocks without any reduction of strength [21, 22, 36-40]. The algebraic properties of S-blocks of modern block ciphers are investigated in [23-25], their influence on sustainability to algebraic cryptanalysis is shown. In [22, 27], combinatorial properties of non-linear knots in the context of the security evaluation of various encryption modes and key schedules were investigated. In [22, 30-36], the influence of S-blocks on avalanche effects, differential and linear properties of block ciphers is investigated. The papers [35, 37] are dedicated to the study of the properties of nonlinear replacement nodes in modern stream ciphers in comparison with the "Strumok" algorithm proposed as a new standard of stream encryption in Ukraine [37].

As a conclusion, we should mention two more our works [39, 40], which are devoted to the further development of this approach. Here we are talking about the improvement of existing designs of modern ciphers, based on using a new structure of the first cycle, constructed by using managed substitutions (enlarged S-blocks).

This research might promote the improvement of various methods of information security, as well as other practical use [41-43]. In particular, the suggested cipher MSC-1 promotes developing the new way in creating symmetric algorithms [1]. The usual of managed substitutions improves dynamic characteristics, that is, in our opinion, increases the speed of promising ciphers on the basis of MSC.

11. CONCLUSIONS

The new cipher, described in this work, is called MSC and seems to be a promising solution for building a modern 256 bit SPN cipher. It possesses the best known SPN cipher dynamic indicators to reach the state of random substitution. According to other indicators of strength, this cipher has all the important indicators of the Muchomor cipher [15]. We also should note an important feature of the cipher, that is, in the cipher the random S-blocks can be taken in almost without reducing the dynamic indicators of its transition to a random substitution.

12. REFERENCES

[1] V.I. Dolgov, I.V. Lisitska, K.Ye. Lisitskyi, "The new concept of block symmetric ciphers design," *Telecommunications and Radio Engineering*, vol. 76, issue 2, pp. 157-184, 2017.

[2] J. Daemen, V. Rijmen, *AES Proposal: Rijndael*, USA, 1998. http://www.nist.gov/aes.

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

[4] X. Lai, J. Massey, "A proposal for a new block encryption standard," *in I. Damgard, editor, Advances in Cryptology - EUROCRYPT'90, vol. 473 of Lecture Notes in Computer Science*, Springer-Verlag, 1991, pp. 389-404.

[5] S. Landau, *Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard*, February, 2004.

[6] W. Meier, O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Advances in Cryptology: Eurocrypt'89*, W. Meier and O. Staffelbach eds., *Lecture Notes I Computer Science*, vol. 434, Springer-Verlag, Berlin, 1989, pp. 549-562.

[7] J. Pieprzyk, J. Quisquater, J. Vandewalle, "Nonlinearity of exponent permutations," *Proceedings of the Advances in Cryptology: Eurocrypt'89*, Springer-Verlag, Berlin, 1990, pp. 89-92.

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

[9] K. Nyberg, "Differentially uniform mappings for cryptography," *Proceedings of the*

Advances in Cryptology: Eurocrypt'93, T. Helleseth, ed., Springer-Verlag, Berlin, 1994, pp. 53-64.

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

[11] V. Ridjmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, "The cipher SHARK," *Proceedings of the Third International Workshop on Fast Software Encryption:* D. Gollman, ed., Springer-Verlag, Berlin, 1996, pp. 99-112.

[12] T. Jakobsen, L. Knudsen, "Attacks on block ciphers of low algebraic degree," *J. Cryptology*, vol. 14, pp. 197-210, 2001.

[13] J. Daemen, L. Knudsen, V. Ridjmen, "The block cipher square," in *Fast Software Encryption, E. Biham ed., Lecture Notes in Computer Science*, vol. 1267, Springer-Verlag, Berlin, 1997.

[14] P. Junod, S. Vaudenay, "FOX: a new family of block ciphers," in *H. Handschuh and A. Hasan, editors, Selected Areas in Cryptography: 11th International Workshop, SAC 2004*, Waterloo, Canada, August 9-10, 2004, vol. 3357 of *Lecture Notes in Computer Science*, pp. 114-129. Springer-Verlag, 2004.

[15] *Open competition of symmetric block cryptographic algorithms of Ukraine* [Online]. Available:http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=49027&cat_id=38710 (in Ukrainian)

[16] State standard of the Republic of Belarus. STB 34.101.31-2011. Information Technology. Information security Cryptographic encryption and integrity control algorithms. Publishing house of Gosstandart, Minsk, 2011, 35 p. (in Russian)

[17] *A New Encryption Standard of Ukraine: The Kalyna Block Cipher*. [Online]. Available: https://eprint.iacr.org/2015/650.pdf

[18] Information technology. Cryptographic protection of information. Block ciphers. GOST R 34.12 - 2015. Moscow, Standardinform, 2015, 21 p. (in Russian)

[19] N. Ferguson, B. Schneier, *Practical Cryptography*, John Wiley & Sons, 2003, 432p.

[20] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997, 794 p.

[21] I.D. Gorbenko, V.I. Dolgov, V.I. Rublinetskii, K.V. Korovkin, "Methods of information protection in communications systems and methods of their cryptoanalysis," *Telecommunications and Radio Engineering*, vol. 52, issue 4, pp. 89-96, 1998.

[22] I. Lisitskaya, T. Grinenko, S. Bezsonov, "Differential and linear properties analysis of the ciphers rijndael, serpent, threefish with 16-bit inputs and outputs," *Eastern European Journal of Enterprise Technologies*, vol. 5, no. 4 (77), pp. 50-54, 2015.

[23] O.O. Kuznetsov, Yu.I. Gorbenko, I.M. Bilozertsev, A.V. Andrushkevych, O.P. Narizhnyi, "Algebraic immunity of non-linear blocks of symmetric ciphers," *Telecommunications and Radio Engineering*, vol. 77, issue 4, pp. 309-325, 2018.

[24] B. N. Tran, T. D. Nguyen and T. D. Tran, "A new S-box structure to increase complexity of algebraic expression for block cipher cryptosystems," *Proceedings of the 2009 International Conference on Computer Technology and Development*, Kota Kinabalu, 2009, pp. 212-216.

[25] A. Kuznetsov, R. Serhiienko, D. Prokopovych-Tkachenko, Y. Tarasenko, "Evaluation of algebraic immunity of modern block ciphers," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 288-293.

[26] S. Sulaiman, Z. Muda, J. Juremi, "The new approach of Rijndael key schedule," *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Kuala Lumpur, 2012, pp. 23-27.

[27] A. Kuznetsov, I. Kolovanova, T. Kuznetsova, "Periodic characteristics of output feedback encryption mode," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 193-198.

[28] M. McLoone, J. V. McCanny, "High-performance FPGA implementation of DES using a novel method for implementing the key schedule," *IEE Proceedings - Circuits, Devices and Systems*, vol. 150, no. 5, pp. 373-378, Oct. 2003.

[29] A. Andrushkevych, Y. Gorbenko, O. Kuznetsov, R. Oliynykov, M. Rodinko, "Prospective lightweight block cipher for green IT engineering," *in: V. Kharchenko, Y. Kondratenko, J. Kacprzyk (eds) Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control*, vol 171. Springer, Cham, pp. 95-112, 2019.

[30] F. H. Nejad, S. Sabah, A. J. Jam, "Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on

rounds keys," *Proceedings of the 2014 International Conference on Computational Science and Technology (ICCST)*, Kota Kinabalu, 2014, pp. 1-5.

[31] M. Rodinko, R. Oliynykov, "Open problems of proving security of ARX-based ciphers to differential cryptanalysis," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 228-231.

[32] H. Liu, C. Jin, "Lower bounds of differential and linear active S-boxes for 3D-like structure," *The Computer Journal*, vol. 58, no. 4, pp. 904-921, April 2015.

[33] C. U. Bhaskar, C. Rupa, "An advanced symmetric block cipher based on chaotic systems," *Proceedings of the 2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Vellore, 2017, pp. 1-4.

[34] M. Rodinko, R. Oliynykov, Y. Gorbenko, "Improvement of the high nonlinear S-boxes generation method," *Proceedings of the 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology* (PIC S&T), Kharkiv, 2016, pp. 63-66.

[35] O. Kuznetsov, O. Potii, A. Perepelitsyn, D. Ivanenko, N. Poluyanenko, "Lightweight stream ciphers for green IT engineering," *in: V. Kharchenko, Y. Kondratenko, J. Kacprzyk (eds) Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control*, vol 171, Springer, Cham, 2019, pp. 113-137.

[36] D. D. Ismoyo, R. W. Wardhani, "Block cipher and stream cipher algorithm performance comparison in a personal VPN gateway," *Proceedings of the 2016 International Seminar on Application for Technology of Information and Communication (ISemantic)*, Semarang, 2016, pp. 207-210.

[37] I. Gorbenko, O. Kuznetsov, Y. Gorbenko, A. Alekseychuk, V. Tymchenko, "Strumok keystream generator," *Proceedings of the 2018 IEEE 9thInternational Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, 2018, pp. 294-299.

[38] P. Jindal, B. Singh, "Analyzing the security-performance tradeoff in block ciphers," *Proceedings of the International Conference on Computing, Communication & Automation*, Noida, 2015, pp. 326-331.

[39] K. Lisickiy, V. Dolgov, I. Lisickaya, "Block cipher with improved dynamic indicators of the condition of a random substitution," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PICS&T)*, Kharkov, 2017, pp. 391-395.

[40] K. Lisickiy, V. Dolgov and I. Lisickaya, "Cipher with improved dynamic indicators of the condition of a random substitution," *Proceedings of the 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 396-399.

[41] V. Dolgov, I. Ishchenko, "Proposals of using chameleon-signature in Ukrainian prototype of combined PKI," *Proceedings of the 2010 International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET)*, Lviv-Slavske, 2010, pp. 303-303.

[42] V. Krasnobayev, A. Kuznetsov, S. Koshman, S. Moroz, "Improved method of determining the alternative set of numbers in residue number system," in: *O. Chertov, T. Mylovanov, Y. Kondratenko, J. Kacprzyk, V. Kreinovich, V. Stefanuk," (eds) Recent Developments in Data Science and Intelligent Analysis of Information. ICDSIAI 2018. Advances in Intelligent Systems and Computing*, vol. 836, Springer, Cham, 2019, pp. 319-328.

[43] R. R. Bhat, V. Panchami, "A novel and robust symmetric block cipher for hand-held mobile devices," *Proceedings of the 2016 Online International Conference on Green Engineering and Technologies (IC-GET)*, Coimbatore, 2016, pp. 1-5.

__Konstantin Lisickiy,__ graduate student of the Department of security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography and cybersecurity.

__Victor I. Dolgov,__ Doctor of Sciences (Engineering), Full Professor, Professor of the Department of security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography and authentication, cybersecurity.

***Iryna V. Lisickaya,** Doctor of Sciences (Engineering), Full Professor. Professor of the Department of security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of scientific interests: cryptography and authentication, cybersecurity.*

***Kateryna O. Kuznetsova,** Researcher of the Department of security information systems and technologies of the V. N. Karazin Kharkiv National University. Areas of interests: security information systems and technologies.*