Universal Journal of Electrical and Electronic Engineering 2(4): 206-215, 2014 http://www.hrpub.org
DOI: 10.13189/ujeee.2014.020409

On Ciphers Coming to a Stationary State of Random Substitution

Gorbenko I.D.*, Lisitskiy K.E., Denisov D.S.

Kharkiv National University of Radio Electronics, Ukraine
*Corresponding Author: gorbenkoi@iit.kharkov.ua

Abstract A new method of determining the real number of round cipher transition to indicators of random substitution is proposed. It is based on the accounting of the minimal number only those S-boxes which are used at the first rounds of their transformations and permit to activate all bytes of the latter from the dynamic point of view to the random substitution of cycle transformation. The results of this technique application for evaluation of dynamic indicators of transition to the indicators of random substitution of a number of modern ciphers including the ciphers presented at one time to the Ukrainian competition on the choice of the applicant to the National standard of block cipher.

Keywords A New Methodology of Provable Symmetric Block Cipher Security Evaluation, Dynamics of Ciphers Coming to the Stationary State, Inherent to a Random Substitution, Round Transformation Structure, Active S-Box, Differential and Linear Indicators of the Provable Security

1. Introduction

It is acknowledged in cryptographic literature that ciphers asymptotically (with the increase of the number of rounds) come to a uniform distribution of differential and linear probabilities (XOR transitions tables of total differentials and linear hulls). Moreover, all known approaches are built on the attachment of cipher security indicators to the differential and linear indicators of S-boxes, included into ciphers. The paper deals with a new method of evaluation of block symmetric cipher security indicators [1], being developed at the Department of Information Technology Security of KhNURE. According to this method, the indicators of cipher security against the attacks of differential and linear cryptanalysis do not depend on the properties, used in S-box ciphers, but are determined by the indicators of appropriate random substitutions, to which ciphers come after a few initial rounds of encryption. Moreover, according to the numerous experiments the dynamic indicators of cipher coming to random substitution indicators in many cases do not depend on either differential and linear indicators non linear substitution boxes, applied in ciphers as well. At this point the dynamic indicators mean the number of cipher rounds necessary for the laws of differential and linear cipher tables to begin repeating the laws of XOR tables distribution and tables of bias of linear approximations of random substitutions. In particular, it is proved [2,3] that as byte S-boxes in many modern ciphers can successfully (without reducing cryptographic indicators) be applied substitutions taken at random (selected without any limitations).

The main idea of this paper is to find the explanation to all these facts and to evaluate the real role of S-boxes in ciphers, as well as to find the explanation to the search of the improved designs which great attention is given to in cryptographic literature.

Some experts consider, for example, that S-boxes must influence the dynamic indicators of cipher coming to a random substitution.

The known experiments on determination cycle-by-cycle laws of distribution of maximal value of XOR tables and shift linear approximations of tables made for 16 bit values of inputs and outputs of full-scale ciphers and confirming that the large ciphers are random substitutions, sort of do not give the real values of cipher coming to the indicators of random substitution. For example, Mukhomor and Labyrynth ciphers as the results of the experiments show become random substitutions just from the first round [4]. The question is if it's possible to trust these results.

The problem of determining dynamic cipher indicators is of a great scientific interest itself, as on the basis of these indicators it's possible to determine which of the used round transformations are more efficient that may appear to be useful for improving technologies of block cipher designing.

In this paper attention is focused on the research of dynamic indicators of modern cipher cycle transformations depending on S-box properties and linear transformations accompanying them.

In this paper we consider the following three types of round transformations.

The first type of transformations is implemented in the form of pure SPN structure of one level type with different designs of linear transformations:

- MDS column transformation along with row shift (Rijndael, Kalyna, ADE and other ciphers);
- bitwise transformation and its modifications (Heys cipher, Serpent cipher and others);
- multilayer multimodule mixing (Belorussian cipher and others);

The second type of transformations is based on two levels. We mean the ciphers using Lai-Massey scheme at the upper level and linear transformations and the types considered above at the lower level (IDEA NXT (FOX), Mukhomor and other ciphers).

In the last type round function uses Feistel network (DES, GOST 28147-89, Kamelia, Labyrynth and other ciphers) for its building.

In contrast to the well-known approaches, connecting evaluations of indicators of cipher security against the attacks of differential and linear cryptanalysis accounting the whole number of active S-boxes in cipher, our approach gives the method of determining the real number of cipher round transformations to the indicators of random substitution. It is based on accounting the minimal number of only those active S-boxes which are used at the first rounds of cipher transformation and permit to activate all bytes of its output from the point of view of dynamics of cipher transition to a random substitution of cycle transformation. In the following rounds maximal values of differential (linear) characteristic features (the number of transition table TDR (LAT) maximal) become identical. A lot of transition values repeat corresponding laws of random substitution transition distribution (the further increase of the round numbers (the number of active S-boxes) doesn't result in changing the laws of distribution of XOR table transitions and linear approximation cipher table shifts).

The method used in this paper is applied for evaluating and comparing dynamic cipher indicators spoken above.

2. Analysis of Modern Cipher Properties at the First Rounds of Encryption

This paper deals with cipher differential indicators. Linear indicators because of the known property of duality, existing between differential and linear cryptanalysis [5] practically repeat the results relating to differential characteristics.

The idea of the given approach, as it has been noted above, is to evaluate the minimal number of active (used) S-boxes, which are necessary for the cipher to become a random substitution. This minimal number is determined by differential and linear indicators of S-boxes themselves, used in cipher, by the designs of round linear transformations and as well as by indicator values of cipher provable security, depending on the size of its bit input.

Considering (as it was done in the Biham's work on DES cipher analysis [6]), that probabilities of resulting differential characteristics are determined by probability products of transitions of active S-boxes included into them, let's submit for consideration the connection of the indicators pointed above as two evident ratios:

$$IPS_D = (DP^{\pi}_{\max})^k, IPS_L = 2^{k-1}(LP^{\pi}_{\max})^k. \quad (1)$$

Here $DP^{\pi}_{\max}$ and $LP^{\pi}_{\max}$ are maximum values of differential and linear probabilities of substitution transformation $\pi(x)$. IPS_D – Differential Indicator of Provable Security and IPS_L – Linear Indicator of Provable Security, $k = k_{\min}$ – is the minimal number of active S-boxes participating in forming cipher transition to random substitution.

Denotation of security indicators is our creation. Here could be used provable security indicators introduced in [7] as *AMDP* and *AMLHP* (Average Maximum Differential Probability and Average Maximum Linear Hull Probability, which are calculated by averaging corresponding maxima probabilities on a great number of encryption keys). But here we take into account the results of the paper [8], according to which the indicators of cipher security practically do not depend on key material, i.e. as security indicators can be considered maxima of the corresponding probabilities calculated for random (one) encryption key.

Now let's consider successively the peculiarities of round transformation realization, pointed above, and their connection with the dynamics of cipher transition to a random substitution state. Let's begin with the ciphers built on the basis of SPN structures of one level type (Rijndael, Kalyna, ADE and other ciphers).

1. For round transformation of 128 bit Rijndael cipher which has 16-byte S-boxes in each round, for every of 4 bytes (a tetrad) of these blocks MDS transformation is made with a branching factor 5 (MixColumns), ShiftRows and addition XOR with a round key for achieving by cipher the state inherent to a random substitution, it's necessary, firstly, for minimal number of active S-boxes $k_{\min}$ with the δ-uniformity indicator equal to 2^{-6} (differential indicator of S-boxes of Rijndael), to satisfy the equality (1), which in this case takes the form $(2^{-6})^k = 2^{-120}$ (here 2^{-120} is the value of indicator of provable security of (IPS_D) 128 bit cipher against the attacks of differential cryptanalysis [9]), and secondly, it's necessary for all S-boxes of the latter from the dynamics point of view of cipher coming to a stationary state, inherent to a random substitution, to be active. The fact itself of coming cipher to a random substitution in the method used is determined by the moment from which each output bit of round transformation becomes dependent on each input bit of the cipher.

From the given equation it follows that $k_{\min} = 20$. It means that the number of necessary round transformations for coming this cipher to a random substitution equals $r_{\min} = 3$. Actually in the first round we have minimum 1 active S-box, in the second one 1+4 = 5 active S-boxes, in the

third round we have 5+4×4 = 21, wherein all bytes on third round output are activated that is enough for covering the necessary minimal number of S-boxes $k_{\min} = 20$. The same result is achieved in the experiments with an encryption by Rijndael complete version of 16-bit data blocks [9].

The confidence in the results achieved can be confirmed by the experiments with a reduced cipher models for which calculations are made for the full set of bit inputs To confirm it table 1 gives the dependence of average maxima of total differentials ($AMDP^f \cdot 2^n$) on the number of encryption rounds r algorithm Baby-Rijndael by using semi-byte S-boxes with different $DP^s_{\max} = p$ values and MixColumns operation for the whole text (the most efficient variant of linear transformation), taken from the paper [10].

In the experiments for each cipher a sample of 30 different encryption keys was considered. For this reduced cipher model the equation (1), in the case of using semi-byte S-boxes with maximum differential value $p = 4$ (paper [10] denotations), takes the form $2^{-12} = (2^{-2})^k$ and, hence, $k_{\min} = 6$. If at the first round at least one active S-box is activated, then at each following round 4 active S-boxes will be activated. Thus, three cycles will be enough for cipher coming to the random substitution state. This is confirmed for S-boxes designed on the ideas of Labyrinth and AES ciphers [11] (third and fourth columns of Table 1).

For random S-boxes from the second table column (thought they have indicator $p = 4$) for cipher coming to a random substitution four cycles are required. This illustrates that for this cipher at one of the first rounds were not four but one or two active S-boxes. All other results may be explained as well. For example, for the last column of the table, despite the fact that $p = 12$, even in this case we have $r_{\min} = 4$. In this example differential characteristic is formed not only by maximum probable transitions of S-boxes (value 12 is the only value in the table of cipher differential differences). One more illustration of the relevancy of the proposed here and further results are the correlation indicators of full-scale cipher designs, submitted in [12]. They practically repeat the evaluations of cipher dynamic indicators described in this paper.

2. Now let's consider round transformation of 128 bit Kalyna cipher [13]. Pseudocode of Kalyna encryption procedure is given in fig. 1.

```
void UES_Encrypt(byte in [8*Nb], byte out [8*Nb],
byte subkey[Nr + 2][8*Nb])
{
byte state[ 8, Nb ] = in
        XORRoundKey(state, subkey[0])
for(round = 1 to Nr/2 step 1)
{
UES_S_boxes(state)
ShiftRows(state)
MixColumns(state)
Add32RoundKey(state, subkey[2 * round−1])
UES_S_boxes(state)
ShiftRows(state)
MixColumns(state)
XORRoundKey(state, subkey[2*round])
        }
        UES_S_boxes(state)
        Add32RoundKey(state, subkey[Nr + 1])
out = state
}
```

Figure 1. Pseudocode of Kalyna encryption procedure

According to the encryption procedure input data whitening (zero round) is initially performed i.e. bitwise XOR with 128 bit key. Then round transformations are used, in each of them ShiftRows procedure is initially performed. In ShiftRows transformations uniform distribution of bytes of two 64-bit columns is made (for 128-bit cipher). This is achieved by round shift of state rows, presented for 128 bit cipher by two 64 bit columns (each column consists of 8 bytes) to the right by one byte (for 128 bit cipher bytes from 4^{th} to the 7^{th} (the first column) change their positions with the bytes from 12^{th} to 15^{th} (the second column)).

Fig. 2 illustrates the order of performing ShiftRows transformations for 128 bit box.

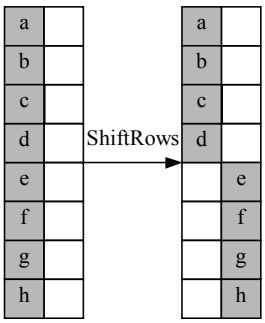

Figure 2. The order of byte distribution in performing ShiftRows transformation for 128 bit cipher

Table 1. Maxima values of total differentials for different S-boxes depending on the number of Rijndael algorithm cycles with MixColumns operation for the whole text.

Sbox / r	Sbox, Сл $p4$, F2	Sbox. $p4$ Labir.	Sbox AES, $p4$	Sbox $p6$, F0	Sbox $p6$, F2	Sbox DES, $p8$	Sbox $p12$, F0
1	16384,00	16384,0	16384,0	24576,0	24576,0	32768,0	49152,0
2	83,87	132,00	132,00	490,87	230,40	1152,00	5184,00
3	20,73	19,47	18,80	25,53	35,27	70,87	146,13
4	19,60	18,73	19,00	19,20	18,93	19,27	19,07
5	19,13	19,47	19,47	18,93	19,40	19,00	19,00

During successive MixColumns transformation the sequential processing of all current state columns is performed. Each column undergoes multiplication over GF(28) field of an initialization 8 byte vector by fixed matrix (8×8 MDS matrix transformation) with branching factor equal to 9. Cycle transformation ends with column addition with column-keys in odd rounds modulo 2^{32} (Add32RoundKey) and in even rounds modulo 2 (XORRoundKey). Here we gave detailed description of encryption procedure to understand the activated S-boxes. The input value of minimal active S-boxes number with δ-uniformity indicator, equal to 2^{-5}, (δ-uniformity indicator of Kalyna S-boxes) will be $k_{\min} = 24{,}2$ ($2^{-121} = (2^{-5})^k$).

Let's calculate the real at the minimum required number of active S-boxes for Kalyna cipher at the first rounds. Considering XOR, at the first round first at the least one S-box is activated. Byte from this S-box output goes to ShiftRows operation. By means of ShiftRows operation a byte can be shifted or can be left at its place, anyway we get two columns, one of which has an active byte. By MixColumns operation one active byte activates all bytes in a column. Combining with a round key using the addition modulo 232 changes nothing (here the addition with a key is applied for each column individually), so at the first round output we have 8 active bytes which activate 8 S-boxes of the next round. After ShiftRows operation of the second round in each column appear four active bytes which with the help of MixColumns operation on columns activate all the bytes of each column (each active byte of MixColumns operation can potentially activate eight bytes, but the total number of bytes in each column is only 16). As a result all 16 input bytes are active at the next (third) round, and at the three rounds are active 1+8+16 = 25

S-boxes, that is enough for covering the minimal their number $k_{\min} = 24$. Thus, for Kalyna cipher $r_{\min} = 3$.

In this case we have the bound of the necessary number of active S-boxes, so for S-boxes with greater value of δ-uniformity additional round will be required.

The experiments with the Kalyna cipher full version for 16 bit segments of inputs and outputs give the result $r_{\min} = 2$ [9]. It can be explained by the fact that when encrypting 16 bit segments the equation $2^{-12} = (2^{-5})^k$ must be viewed, for its realization three active S-boxes are enough. Two rounds of encryption completely solve this problem. Moreover, for random S-boxes with δ-uniformity indicator equal to 12/254 = 0,0469 we get $k_{\min} = 4$, so and in this case for coming to a random substitution two rounds appear to be enough.

3. The next example of modern (considered to be promising) cipher is a IDEA NXT (FOX) cipher [14, 15]. First let's consider the FOX-64 cipher version (with 64 bit inputs and outputs). f32 function of the inner level contains two layers with byte tetrads of S-boxes with intermediate dispersion part, which presents linear 4x4 multipermutation in the field GF(2^8), and three intermediate additions with round subkeys [14]. As a result, at the first round at least five S-boxes (one S-box of the first layer and four S-boxes of the second one) are activated. From the equation $(2^{-4})^k = 2^{-27}$ follows that $k_{\min} = 6{,}75$ and one can see that one round of f32 transformation is not enough for f32 coming to random substitution (2^{-27} is security indicator of 32 bit cipher). In the following round all its eight S-boxes will be activated and in this case there are 13 active S-blocks for two rounds. f32 function becomes a random substitution. But for 64 bit cipher equation (1) takes the form $(2^{-4})^k = 2^{-58}$ (here 2^{-4} is maximum value of differential probability of Fox cipher S-boxes), hence $k_{\min} = 14{,}5$. Thus we come to the conclusion that two FOX cipher rounds are not enough for covering minimal number of active S-boxes $k_{\min} = 14{,}5$ and hence for FOX-64 cipher we should expect $r_{\min} = 3$. At the same time, the experiments with full-scaled cipher with 16 bit transitions [16] give the result $r_{\min} = 2$. It remains to note that in this case we should view the equation $2^{-12} = (2^{-4})^k \rightarrow k_{\min} = 3$ and in this case five active S-boxes of the first cycle are enough for cipher coming to the state of random substitution. Evidently, in this case, we should consider that f32 function of inner level becomes random substitution after two rounds.

4. In 128 bit FOX cipher matrix multiplication by 8x8 MDS matrix is applied and again two layer non-linear transformation. Therefore we have 9 active S-boxes at the first round. After two rounds their number will be 9+16 =25 and thus in this case one more round $r_{\min} = 3$ (here $k_{\min} = 30$) is necessary.

5. The M-64 combining function of Mukhomor-128 cipher [17] contains three SL transformations, each of them includes the layer of non linear transformations implemented by 4 byte S-boxes and MDS transformation performing matrix multiplication of four S-boxes byte outputs (over the field) by 4×4 square matrix (similar transformation is performed in Rijndael cipher with the help of MixColumns operation, only in that case another polynomial is used when multiplying). At the M-64 combining function input addition modulo 2^{32} of 32 bit data boxes is applied. Here, however, scheme of including SL transformation provides activation of all 12 S-boxes and without addition with a round subkey. Taking into account all this for combining function we have the equation $(2^{-5})^k = 2^{-58}$, hence $k_{\min} = 11{,}6$ and M-64 per one round becomes a random substitution! (see table 2).

Table 2. Differential properties of M 64 transformation

M-64 trans-formation	Exp. 1	Exp. 2	Exp. 3	Exp. 4	Exp. 5	Exp. 6	Avera-ge value
Maximum value	18	20	18	18	20	20	19

It means that cipher combining function provides efficient mixing of all input 128 bits (additions modulo 2 of two left and two right 32 bit parts of input data box). Successive transformation of Lai-Massey scheme of upper bound spreads input bit mixing effect on the whole 128-bit data box (provides the dependence of output bits on all input bits). However, for covering minimal number of active S-boxes $k_{min} = 20$ one more round is necessary, therefore $r_{min} = 2$.

In accordance with the experiment results with 16-bit transitions Mukhomor cipher becomes a random substitution just from the first round: $r_{min} = 1$, which coincides with the expected evaluation for cipher with 16-bit transitions.

It should be noted that M-64 function can be used as cipher round function without Lei-Messi superstructure. This cipher with 64-bit input will possess the limit dynamic characteristics of coming to the state of random substitution.

6. Mukhomor-256 cipher combining function M-128 (256 input bites to the cipher) contains 8 SL transformations. Even if we assume that at the first round minimum 29 S-boxes are involved, which form all output round bytes (combining function) as active, the combining function will come to random substitution indicators per one round and with δ-uniformity indicators equal to 8 and 10 and 12 and 16 and even 20 (if $\delta = 16$ minimally required number of S-boxes is 30). This combining function can be also used for iterative 128 bit cipher designing without Lai-Massey superstructure. Such cipher will also have limit dynamic characteristics ($r_{min} = 1$).

7. Labyrynth cipher, using for round transformations designing, inserted Feistel-like structures [18], also gives indicators repeating Mukhomor cipher dynamics (in experiments it becomes a random substitution from the first round as well [19]). But we must keep in mind that in this cipher powerful before- and after-round transformations were used, which were designed with the help of S-boxes layers which can be considered as additional specific rounds. Therefore we suppose that in experiment results [10] initial data for Labyrynth cipher correspond to three rounds at once (all S-boxes of the third round are active). Here the first cycle, with initial IT and final FT transformations, contains 48 S-boxes.

Table 3 gives generalized experiment results for Muhomor, Kalyna, Labyrynth and ADE ciphers for 30 master-keys selected at random [9].

Table 4 gives cycle-by-cycle maxima values of cipher linear approximation table shifting for the same ciphers from [9] (for 16-bit segments).

One can see that linear indicators of cipher coming to a random substitution dynamics practically repeat differential ones.

Let us recall that the ciphers used have: Muhomor – 11 encryption rounds, Labyrynth – 8, Kalyna 128/256 – 14, AES 128/256 – 10 and Rijndael – between 10 and 14 rounds depending on box size and key length. In the tables all the experiments result in 10 encryption rounds.

Table 3. Cycle-by-cycle values of XOR tables maxima transitions for full versions of Ukrainian ciphers (16-bit segment encryption)

Number of rounds	Kalyna 30 keys	AES 30 keys	Labyrynth 1 key	Muhomor 30 keys
1	6711,6	1024	18	19,13
2	19,0	3891,2	20	18,8
3	19,13	19,07	18	19,4
4	19,2	19,07	20	19,13
5	19.27	18,87	20	19,07
6	18,87	19,13	20	19,6
7	19,47	19,27	20	19,27
8	19.2	19,13	18	19,13
9	19,0	19,07	18	19,13
10	19,33	19,33	18	19,276

Table 4. Cycle-by-cycle maxima values of cipher linear approximation table shifts with standard deviation values

Number of round	Kalyna 30 keys	Muhomor 30 keys	Laby-rynth 1 key	AES 1 key
1	11008,392± 1785,34	824,742± 20,1286	– 790	4096
2	817,271± 27,6348	818,621± 25,9742	839	9216
3	817,718± 21,3851	827,431± 21,2352	-816	826
4	814,19± 26,7792	824,193± 17,8115	832	808
5	837,349± 28,2712	831,753± 25,7731	885	812
6	810,733± 29,3801	814,155± 28,9121	810	834
7	820,384± 20,752	820,975± 20,2673	– 834	828
8	837,917± 23,2539	823,024± 18,853	835	822
9	809,273± 22,186	810,196± 22,9352	– 809	826
10	821,755± 25,5737	821,316± 25,849	– 806	802

8. GOST 28147-89 cipher repeating Feistel structure as well according to the experimental data comes to the state of a random substitution at 9-10 round [20].

For GOST cipher we have the equation $(2^{-5})^k = 2^{-58}$ (S-boxes of this cipher have $\delta = 6$, that corresponds to transition probability equal to $6/16 = 2^{-1,415}$). And then at the least required (theoretical) number of S-blocks for coming cipher to a state of random substitution is equal to 41. We must add that the round key in GOST cipher is introduced with the help of addition operation modulo 2^{32}. It means that in activizing one 4-bit segment (cipher input) after addition with the key may appear from one to several S-boxes active inputs due to the transfer of bits, and in the following rounds the activization picture will be more

difficult for understanding. It can be noted that on activation of the rightmost (the most significant byte) after addition modulo 2^{32} with the key only one byte remains active.

We will calculate here the number of active S-boxes without taking into account the addition with a round key.

One S-box of the first round results in activating two S-boxes of the following round at the next round, this activation being not complete (one S-box of the second round is activated by one bit of S-box output of the first round and the second - by three bits). At the next round four S-boxes are activated (two of which are activated by truncated S-boxes outputs). At the fourth round six S-boxes are already activated, at the fifth one – seven S-boxes and only at the sixth round all 8 S-boxes are activated, the part of which is activated by truncated outputs of S-boxes of the previous round. As a result we have 1+2+4+6+7+8+8+8 = 44, i.e., the cipher must come to a state of random substitution for 8 rounds (note that S-box activated by one bit becomes active in half the cases and by three bits in 7/8 of the cases). If we take it into account we will already come to 9-10 rounds. The real meaning of the round number is already formed accounting the influence the partial activation and round key bits as well (bits of a round key, resulting in bit transfering, increases the number of active S-boxes and the partial activation decreases the efficiency of bit mixing).

9. On multilayer mixing such as, for example, in Belorussian cipher [21], round transformation includes 28 bit S-boxes from which at the first round minimum 13 are activated (one of the four input branches is activated). Thus, in this case an additional round is required for activating all bytes of the second round output. The cipher comes to a random substitution at the second round [21]. Simultaneously it becomes evident that there is a stock for S-box using not only with minimal differential (linear) indicators.

10. Now let's consider bitwise linear transformation and its complications (Heys cipher, Serpent cipher and others).

Here we have recalled a proposal on building bitwise linear transformation which is described in H. Feistel's work [22] in 1973. It can be viewed as a prototype of wide trace strategy which is based on multiplication by MDS matrix, realized in Rijndael cipher [23]. As the first realization of this linear transformation can be viewed 16 bit professor Heys cipher [24], built for learning goals. For this cipher at best for semi-byte S-boxes with δ-uniformity indicator equal to 4 we obtain the equality $18\text{-}20/2^{16} = (2^{-2})^k$, and, hence, k = 5,913-5,838 = 6. For S-boxes with δ-uniformity indicator equal to 8 we have k = 12. If we take that on bitwise linear transformation with semi-byte S-boxes branching factor equal to 3 is realized (semi-byte S-box has on the average two single bites at the output), then we come to the conclusion that this cipher must come to a state of random substitution for three cycles (the first cycle has 1 active S-box, the second has 2, the third has four, as the result we obtain 7 active S-boxes). However, as the experiments with Heys cipher showed the results are the number of transition rounds to a random substitution, being within the range $6 \le r_{\min} \le 12$. And what's the reason?

The analysis shows that this type of transformation has obvious weak points manifested in the fact that on bitwise distribution of S-boxes outputs within the round with branching factor 3, the first round in this cipher are generally built as one-block transitions, and one-block transition characteristics naturally are more probable. Practically, branching factor close to two is realized. The necessary six S-boxes are obtained on six rounds. After six rounds, in the case which is of interest to us, multibox round characteristics (round transitions) are approximated to this value. The number of rounds coming to a random substitution is more than six is because of the fact that the first round transitions are being passed with high probability formed by summing great number of differential characteristics, participating in forming total differential. Besides, the differential properties of S-boxes themselves influence the dynamic of transition. After achieving asymptotic value of differential maximum, the increasing of round number doesn't result in changing this value. The subsequent round transitions are made with probability 1.

Table 5 gives maxima cycle-by-cycle distribution of total differential transitions of Heys cipher with S-boxes of DES cipher. The used S-box itself and its table of XOR differences is presented in table 6, and in table 7 maximum differentials are given and values of input and output (at the inputs of round S-boxes) cipher differences with different number of encryption cycles. In the given example maximum of the first cycle 32768 is formed by one of the four (any) S-boxes (note that 32768/65536=8/16, that just corresponds maximal probability of transition of S-box used (the first raw of S-box cipher DES)).

Table 5. Maxima cycle-by-cycle transition distribution of total differentials of Heys cipher for S-box {14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7}

S-box	The number of encryption rounds									
	1	2	3	4	5	6	**7**	8	9	10
E,4,D,1,2,F,B,8,3,A,6,C,5,9,0,7	32768	12288	2304	204	78	28	**18**	18	18	18

Table 6. S-box differential table {14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7}

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

Maximum element of difference table: 8
The number of such elements: 1

Table 7. The value of maxima differentials and input and output (at the outputs of round S-boxes) cipher differences at different number of encryption rounds

Round 1, Max. 32768, input b, Output 2
Round 1, Max. 32768, input b0, Output 10
Round 1, Max. 32768, input b00, Output 100
Round 1, Max. 32768, input b000, Output 1000
Round 2, Max. 12288, input b0, Output 32
Round 2, Max. 12288, input 10ff, Output 50
Round 3, Max. 2304, input b0b0, Output 5000
Round 4, Max. 204, input b, Output 100
Round 5, Max. 78, input f, Output 5000
Round 6, Max. 28, input b0, Output a
Round 7, Max. 18, input 65, Output c072
Round 7, Max. 18, input 3cb0, Output c336
Round 7, Max. 18, input 44ea, Output 3126
Round 7, Max. 18, input 6b48, Output 94bb
Round 7, Max. 18, input 6ff6, Output b650
Round 7, Max. 18, input 88ac, Output b15b
Round 7, Max. 18, input 901b, Output 00b3
Round 7, Max. 18, f577, Output e633

The second round (for one of the two possible options) is also built with one S-box at the first round with the most probable transition 8/16 (transition B $\rightarrow$2), and one S-box at the second round with transition probability 6/16 (transition 2$\rightarrow$5) so that probability of two-cycle characteristics is equal to $(4/16)\cdot(8/16) = 48/16^2 = 12288/65536$.

Three-cycle characteristics is generally built as the sum of probabilities of many one-box (or even two-boxes) characteristics. In the given case at the first round two S-boxes the first and the third are launched (both have transitions B$\rightarrow$2 with probability 8/16). These two S-boxes activate the third S-box of the second round by their one-bit outputs (transition A$\rightarrow$8 with probability 8/16), which in its turn activates the first S-box of the third round (transition 2$\rightarrow$5 with probability 6/16). In this case we have the only three-cycle characteristics, whose probability is equal to $(8/16)^2\cdot(6/16)^2 = (48^2/16^4) = 2304/65536$.

For four rounds the situation will be complicated for the analysis and we will stop here.

The result of six rounds for Heys cipher is the limit. It can be obtained for S-boxes for which at every round transition the minimal maximum value equal to 4 for semi-byte S-boxes is realized. This minimal number of encryption rounds is received in all the experiments made for today. After achieving stationary state one box transitions "sink" in multiboxes ones. Note as well, that exactly six encryption rounds are typical for S-boxes called in [25] as perfect. All of them have, as noted above, the extreme property, which lies in the fact that characteristics of "one-box type" are permitted in them.

The grand total for Heys ciphers with bitwise linear transformation will be the fact that in all these ciphers at the first rounds one-box round transitions are permitted, and that is why the round number for coming to a random substitution $r_{\min} \geq 6$.

11. 128 bit Serpent cipher, developed by R. Anderson, E. Biham and L. Knudsen [26] is a SPN iterative scheme with 32 semi-byte S-boxes in each round and linear transformation based on the addition (XOR) from three to nine S-boxes bit outputs. The round subkeys are also introduced by means of XOR operation. Linear transformation is selected in the way that every S-box

activates 16 S-boxes of the next cycle by its one-bit outputs.

The basic criterion in linear transformation development was maximum influence acceleration of every input bit and a key on every ciphertext bit. As the algorithm authors themselves note [26], such influence is achieved even after three rounds of Serpent algorithm.

The analysis shows that due to the initial bit permutation at the first round on the average two S-boxes are activated. Then at the second round 32 S-boxes are activated, at the third round 32 S-boxes more are activated (during three rounds we obtain that 2+32+32=66 S-boxes are activated). On the other hand, $2^{-121} = (2^{-2})^k \rightarrow k_{\min} = 60$. According to the results of the experiments with 16-bit transitions [9] Serpent cipher actually shows $r_{\min} = 3$ rounds which were claimed by the authors of the development.

In table 8 we summarize the results obtained.

Table 8. The minimal round number for cipher coming to stationary state of random substitution according to differential indicators

Cipher	$r_{\min}$
Rijndael-128	3
Kalyna-128	3
FOX-64	3
FOX-128	3
GOST 28147-89	9-10
Heys-16	6-12
Mukhomor-128	2
Belorussian cipher	2
Serpent	3
Labyrynth	≥ 3
Cipher with cycle function M-64	1
Cipher with cycle function M-128	1

There are some notes concerning linear cipher indicators. Here we have already referred to the duality principle for differential and linear cipher indicators, which lies in the fact that these properties possess duality (in a sense repeat each other). Let's recall at least differential and linear iterative characteristics of DES cipher [27, 28], which are repeated with the accuracy up to mirroring. It can also be noted that the indicators of provable cipher security against the attacks of linear and differential cryptanalysis proved to be also close to each other [9]. The numerous experiments obtained testify, that analogous results concern the cipher coming to a state of random substitution and for linear indicators (see, for instance, the results given in table 4).

In conclusion, however, we want to stress that non-linear cipher transformations (S-boxes), nevertheless, play a very important part in symmetric ciphers. Without them a fast and efficient mixing mechanism of data box bits can't be obtained. The substitutions themselves are powerful random sources, making additional and, the most important thing, non-linear mixing data boxes segments, without which a good cipher can't be built. The results presented, just testify that neither differential nor linear indicators of separate S-boxes are the determining factors in cipher coming to a random substitution state, and more significant is the result of their mutual random impact on data transformed. In the sequence (multiplication) of substitution transformations the individual substitution properties are leveled i.e. become unimportant.

3. Conclusion

The most important conclusion from the results presented consists in our finding the explanation of one of the central ideas of the new developing methodology on cipher coming to random substitution properties after some initial number of encryption rounds despite S-boxes used. Besides, the explanation of the property of independence of dynamic indicators of ciphers transitions to random substitutions on differential and linear properties used in S-box ciphers was obtained during the experiments for many ciphers. In many ciphers as non-linear transformation can successfully be used substitutions formed by a random generator. For these ciphers the search of substitution with improved cryptographic indicators loses any sense. This is achieved due to the fact that cycle transformations of a number of ciphers have a stock of activated S-boxes relative to their minimal number, necessary for cipher coming to a random substitution state. Simultaneously the results presented confirm the trust to the results on the evaluation of differential and linear indicators of full-scale ciphers and their reduced models, obtained in numerous experiments [2-4, 16, 19, 20, 21 and many others].

Note here, that in the paper the evaluations of the necessary minimal number of S-boxes are given as well, with the orientation on their at most probable transitions, however, it's evident that the real characteristics will include evidently not maximum probable transitions. It means that sensitivity to differential and linear indicators of S-boxes will become more and more undistinguished. The Differential and linear properties of many ciphers really can be considered independent of differential and linear properties of S-boxes, that is proved by the results of numerous experiments.

Nevertheless, there are ciphers in which round transformations are built in the way that linear and differential indicators of S-boxes, included in them, influence (within one or two rounds), on dynamic indicators of cipher coming to a state of random substitution. These ciphers with small values of active S-boxes numbers necessary for the corresponding transition (Rijndael cipher, Kalyna and some others). In such ciphers the necessary number of active S-boxes is on the bound of providing the number of round transformation denoting minimum. And therefore, the change of differential and linear indicators of S-boxes can influence on minimally necessary number of

round transformations for coming cipher to a random substitution and it means that random S-boxes can be not optimal for the application in the cipher. In these cases it's possible to pose and solve the problems of S-boxes optimization according to linear and differential indicators. True, a problem of not using maximal type transitions in building differential transition characteristics remains unsolved. If they are available the necessary minimal number of rounds for coming to random substitution can be unchangeable for S-boxes with differential and linear indicators.

The results also confirm that the undisputed champion's in transition dynamics to stationary state, inherent to a random substitution is Muhomor-128 Belorussian cipher, which after two round encryptions becomes random substitution what can't be realized by all other known ciphers.

It can be achieved due to the fact that applied design of mixing SL transformations, on which round function of Mukhomor-128 is built, repeats the ideas put in its time in building cipher of controlled substitutions in paper [30] (8 SL transformations are used in a round, each of which contains 4 S-boxes), boosted by introducing additional feedbacks, that

It is possible to achieve due to the fact that the cyclic functions of these ciphers contain the number of S-boxes, significantly exceeding the minimum required number of them, the following equation of encryption, and a construction for a linear transformation allows permits to provide the limit branch factor of cycle function (one input byte activates (per one round) all output bytes!).

It means that in Muhomor-128 cipher at least twice less the number of encryption cycles than it is proposed in the specification [18].

Taking into account that according to the results of testing speeds of AES, Muhomor and GOST-28147-89 given in [29], the Muhomor cipher in full version demonstrates the speed indicators close to cipher AES, we come to the conclusion that decreasing the number of acceptable encryption rounds makes Muhomor cipher undisputed leader among many known ciphers and according to speed indicators. It can be noted here that by reducing the number of rounds, other indicators of Muhomor cipher security remains at the high enough level. And for reduced round construction the security evaluations against the integral cryptanalysis, a boomerang attack, an interpolation attack, a related-key attack will be right, given in [31]. The approach developed gives additional (new) arguments for justification of its correctness.

Other ciphers show at best the minimal round number of coming to random substitution equal to two (FOX-128, Muhomor-128 and Belorussian cipher), and Rijndael cipher becomes random substitution only at the third round.

Summing up, we can also note, that limit dynamic characteristics will also have the ciphers using round functions M-64 and M-128, which are the bases for building Muhomor cipher series.

Acknowledgements

The authors are grateful to prof. Dolgov V.I. for discussion of the results and critical remarks which improved the work.

REFERENCES

[1] Gorbenko I.D. The new ideology estimate the resistance of block symmetric ciphers to the attacks of the differential and linear cryptanalysis / I.D. Gorbenko, V.I. Dolgov, I.V. Lysytskaya, R.V. Oleynikov // Applied electronics, – 2010. – Vol. 9, № 3. – pp. 212-320. Ukraine.

[2] Lysytskaya I.V. Importance of S-Blocks in Modern Block Ciphers / I.V. Lysytskaya, E.D. Melnichuk and K.E. Lysytskiy. // I.J. Computer Network and Information Security, 2012, 10, 1-12. ISSN: 2074-9104.

[3] Dolgov V.I. S-blocks for advanced ciphers. / V.I. Dolgov, E.D. Melnichuk. // Radio engineering – 2012. – Issue. 171. – pp. 121-133. Ukraine.

[4] Lysytskaya I.V. Large ciphers - random permutations. A comparison of differential and linear properties of ciphers submitted to the Ukrainian competition and scale models / I.V. Lysytskaya, A.A. Nastenko, K.E. Lysytsky. // Automated control systems, electrical automation. – 2012.– Issue. 159. – pp. 13-21. Ukraine.

[5] Mitsuru Matsui. On Correlation Between the Order of S-boxes and the Strength of DES . Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings. V. 950. p. 366-375.

[6] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 4(1): 3-72, 1991.

[7] Lysytskaya I.V. A comparison of the effectiveness of superblocks some modern ciphers / I.V. Lysytskaya // Radioelectronics. Informatics. Office. Zaporozhye 1(26)' – 2012. – pp. 37-43. Ukraine.

[8] Lysytskaya I.V. On the significance of cryptographic schemes key shedule in ensuring the resistance the symmetric block cipher to the attacks of the differential and linear cryptanalysis / I.V. Lysytskaya, A.A. Nastenko, K.E. Lysytsky. // Electronics and Computer Science. – 2012 – № 3(58). – pp. 56-65. Ukraine.

[9] Dolgov V.I. Methodology for assessing resistance of block symmetric ciphers to the attacks of the differential and linear cryptanalysis: monograph / V.I. Dolgov, I.V. Lysytskaya. – Kharkov. Publishing house "Fort", – 2013. – 420 p. Ukraine.

[10] Dolgov V.I. Variations on the theme of the cipher Rijndael, / V.I. Dolgov, I.V. Lysytskaya, A.V. Kazimirov // Applied electronics 2010, Vol. 9, № 3, pp. 321-325. Ukraine.

[11] The study of nonlinear properties of cryptographic units replacing small versions of some ciphers. / V.I. Dolgov, A.A. Kuznechov, I.V. Lysytskaya and other // Applied electronics, – 2009. – Vol. 8, № 3. – pp. 268-277. Ukraine.

[12] Lysytskaya I.V. Large ciphers - random permutations.

Comparison of statistical security block symmetric ciphers submitted to the Ukrainian competition / I.V. Lysytskaya, A.A. Nastenko, K.E. Lysytsky. // Eastern European journal of advanced technology. – 2012. – Vol. 6, №9(60) – pp. 11-21. Ukraine.

[13] Promising symmetric block cipher "Kalyna" – basic terms and specifications / I.D. Gorbenko, V.I. Dolgov, R.V. Oleynikov, etc. // Applied electronics. – 2007. – Vol. 6. – № 2. – pp. 195-208. Ukraine.

[14] P. Junod, FOX specifications version 1.1. / P. Junod and S. Vaudenay. Technical Report EPFL/IC/2004/75, Ecole Polytechnique F´ed´erale, Lausanne, Switzerland, 2004.

[15] Principles and properties of building a symmetric block ciphers like IDEA / I.D. Gorbenko, V.I. Dolgov, R.V. Oleynikov and other // Applied electronics. – 2007. Vol. 6, № 2, pp. 158-173. Ukraine.

[16] Lysytskaya I.V. Differential properties of the cipher FOX. / I.V. Lysytskaya, D.S. Kaidalov // Applied electronics, 2011, Vol.10, № 2. pp. 122-126.

[17] Promising symmetric block cipher "Muhomor" – the provisions of the basic and specification / I.D. Gorbenko, M.F. Bondarenko, V.I. Dolgov and other // Applied electronics. – 2007. – Vol. 6, №2. – pp. 147-157. Ukraine.

[18] Golovashich C.A. Specification of block symmetric encryption algorithm "Labyrinth". // Applied electronics. – 2007. – Vol. 6, №2. – pp. 230-240. Ukraine.

[19] Lysytskaya I.V. The large ciphers – random substitution. / I.V. Lysytskaya, A.A. Nastenko // Interdepartmental Scientific Technical Collection – Radioteknik, – 2011. – Issue. 166. – pp. 50-55. Ukraine.

[20] Lysytskaya I.V. The large ciphers – random substitution. A comparison of differential and linear properties of ciphers submitted to the Ukrainian competition and scale models / I.V. Lysytskaya, A.A. Nastenko, K.E. Lysytsky. // Automated Control System and Devices – 2012.– Vol. 159. – pp. 4-10. Ukraine.

[21] Study of random block cipher of the Belarusian standard СТБ 34.101.31-2011 / V.I. Dolgov, R.V. Oleynikov, I.V. Lysytskaya and other // Special Telecommunication Systems and Information Protection. Issue. 7 (21), Kyiv. – 2012 p. – pp. 38-51. Ukraine.

[22] H. Feistel, Cryptography and computer privacy, Scientific American, Vol. 228, No. 5, pp. 15–23, May 1973.

[23] J. Daemen and V. Rijmen. AES Proposal: Rijndael. 1st AES Conference, California, USA, 1998. http://www.nist.gov/aes.

[24] H. M. Heys. A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, v 26, N 3, 2002, p. 189-221.

[25] Markku-Juhani O. Saarinen Cryptographic Analysis of All 44-Bit S-Boxes. 2008.

[26] R. Anderson, E. Biham, and L. Knudsen, Serpent: A flexible block cipher with maximum assurance, The First Advanced Encryption Standard Candidate Conference, Proceedings, Ventura, California, August 1998, p 1-10.

[27] Lysytskaya I.V. Ensuring the resistance DES cipher to linear cryptanalysis attacks Selection requirements for S units are protected from attacks on the characteristics of nullable, chetyrehtsiklovye shestitsiklovye and iterative approximation. / I.V. Lysytskaya, A.C. Bondarenko, A.I. Kolubelnikov // Interdepartmental Scientific Technical Collection – Radioteknik, – 2001. – Issue. 119. – pp. 177-190. Ukraine.

[28] Dolgov V.I. Ensuring the resistance DES cipher to differential cryptanalysis, the overlap of iterative characteristics nullable and chetyrehtsiklovyh iterative characteristics. / V.I. Dolgov, I.V. Lysytskaya, V.I. Ruzhentsev // Interdepartmental Scientific Technical Collection – Radioteknik – 2001. – Issue. 120. – pp. 192-197. Ukraine.

[29] Justification of requirements and development of major decisions and building a promising properties BSSH "Muhomor"./ M.F. Bondarenko, I.D. Gorbenko V.I. Dolgov and other / Applied electronics. – 2007. – Vol. 6, №2. – pp. 174-185. Ukraine.

[30] Pat. 53949 Ukraine, IPC H April 29/14. Method not determined cryptographic transformation of data blocks. V.I. Dolgov, S.V. Supronyuk., I.V. Lysytskaya; applicant and patentee Kharkiv National University of Radio Electronics. – №2002032372; appl. 26.03.2002, publ. 17.02.2003, Bull. Number 2/2003. – 3 p. : Il. 5. Ukraine.

[31] Justification of requirements and development of major decisions and building a promising properties BSSH "Muhomor"./ M.F. Bondarenko, I.D. Gorbenko V.I. Dolgov and other / Applied electronics. – 2007. – Vol. 6, №2. – pp. 174-185.