I.J. Computer Network and Information Security, **2014, 1, 11-18**
Published Online November 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2014.01.02

On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers

Lisitskiy K.E.
National University of Radio Electronics, Kharkiv, Ukraine
dolgovvi@mail.ru

Abstract—The problem of determination of maxima distribution laws of full differentials and linear bias of block symmetric ciphers as substitution transformations is considered. Well-known theoretical results, published in literature, are given, as well as experiment results on making the laws of maxima distribution of full differential transitions and maximum biasess of linear hulls for reduced cipher model from Belorussian standard and cipher Kalina, which practically confirm theoretical calculations, are presented. The results testify that maximum values of differential and linear probabilities are concentrated close to their average values and for evaluation of indexes of cipher provable security it's enough to make a test of proximity of differential and linear cipher indexes, received for one arbitrarily taken cipher key corresponding to indexes of random substitutions.

Index Terms—Provable security, of index evaluation of provable security in block symmetric ciphers, distribution of maximums, mini versions ciphers

I. INTRODUCTION

This paper deals with a new methodology of index evaluation of provable security in block symmetric ciphers [1], according to which the properties of block symmetric ciphers can be evaluated on the basis of studying properties of their reduced models.

Here we want to remind one of the central theses of this methodology which is formulated as a statement:

All modern block ciphers[1] after a certain number of cycles independently of those used in S-blocks ciphers (here we don't mean their degenerated designs) acquire the properties of random substitutions, i.e. according to their combinatorial indexes (the number of inversions, increases and cycles) as well as according to the laws of transition table distribution of XOR differences (full differentials) and the distribution laws of bias linear approximation tables (linear hulls) they repeat the corresponding indexes of random substitutions. As a result the maxima values of full differentials and linear hulls meanings can be determined by calculations from the formulas for the distribution laws of transition probabilities for XOR tables and bias tables of linear approximations of appropriate random substitutions.

Herewith, the test of random indexes of large ciphers can be performed on the basis of the development and further analysis of random indexes of reduced models, permitting to make calculating experiments in acceptable (real) term.

This result is tested on a great number of reduced and large models of many modern ciphers [2-10 and others].

The experiments made however are tied to the limited set of encryption keys. Nevertheless, on the basis of these results the conclusion was made that cipher security indexes can be determined not by the averaging method over the set of keys but on the basis of maxima determination of differential and linear probabilities for any (one) arbitrarily taken cipher key.

We also recall that using this approach the evaluation of block symmetric cipher security indexes is proposed to do not with the help *MADP* (Maximum Average Differential Probability) and *MALHP* (Maximum Average Linear Hull Probability), as it is done in a great number of publications, but with the help of *AMDP* (Average Maximum Differential Probability) and *AMLHP* (Average Maximum Linear Hull Probability) which, as shown in paper [11] are more suitable to the problem solved.

In this paper we want to substantiate the validity of the conclusion, already presented in a number of works [2-10] that the block symmetric ciphers security against differential and linear attacks really can be determined not by the averaging method over a set of keys but on the basis of maximum determination of differential and linear probabilities for any (one) arbitrarily taken cipher key permitting too convince that maximum values of full differentials and cipher linear hulls coincide with the corresponding indexes of random substitutions.

The general approach to solving this problem is to study the behavior of cipher transformation on the whole set of cipher keys. Experimentally this approach is based on the evaluation with the help of computing experiments the maximum values of full differentials and linear hull biass for reduced cipher models for the whole set of cipher keys (the reduced cipher models permit to do it) and the determination of maximum experimentally obtained values and their number for the whole set of differential and substitution linear table as the ciphers themselves are considered.

Mathematically, this problem casts to the maximum distribution study on a great number of independent

[1] Here the cipher DES is not considered as a modern one because the transition to the random substitution is performed for separate cipher keys in 16 cycles because of the presents of 0-type characteristics.

random values.

This paper poses the problem of determination of the greatest possible values of transitions among a great number of table XOR differences and biasess tables of linear approximations of small cipher models for the whole set of encryption keys.

The first part of the paper gives theoretical foundations, which are the basis of determination of the maxima distribution laws of a great number of random independent values which are concretized for the distribution laws of independent values: Puasson and normal. The second part gives computational experiment results on the determination of distribution laws of maxima transition tables of full differentials and bias maxima of table linear approximations of reduced cipher models on an example of a new Belorussian cipher and cipher Kalina. At the end of the paper the discussion of the results obtained is given.

II. DISTRIBUTION OF MAXIMUMS

First of all we will be interested in mathematical aspects of solving the problem set.

Today, as it is turned out, there is a developed mathematical tool which solves this problem theoretically. We mean the paper [12] which has the appendix in which there is an appropriate material which we will use.

In the first part we will give our appendix translation from the paper which contains theoretical data which constitute the essence of the developed approach. The material of this appendix will be the basis on which we will build and validate our results. Further the translation itself of the part the appendix from the paper [12], which has the same name with this part of paper, is given.

Consider the case when all the values of the large number of independent random variables x have just the same distribution. We will consider that their distribution densities decrease exponentially at large meanings of x. Denote the number of such values 2^Y and use the model of integral distribution for every variable $D(X)$ as:

$$D(X) = 1 - e^{-f(X)} \tag{1}$$

with $f(X)$ – function which grows sub-exponentially. From order statistics [13,14] it is known that integral distribution of maximum number of variables is the product of the integral distributions of these variables. Thus we have:

$$D_{\max}(X) = D(X)^{2^Y} = (1 - e^{-f(X)})^{2^Y} \approx \approx e^{-2^Y e^{-f(X)}} = e^{-e^{\ln(2)Y - f(X)}} \tag{2}$$

We can approximate the function $\ln(2)Y - f(X)$ (as the authors of the paper [12] note) by linear function near the point where the function is close to zero. Let a be the solution of equation $\ln(2)Y = f(X)$ and let b be one divided by derivative of a function $f(x)$ in point a. Then is true.

$$D_{\max}(X) \approx e^{-e^{\frac{a-X}{b}}} \tag{3}$$

This distribution is well studied in the theory of probabilities, as it is marked in [12] and is known as the extreme values distribution, Fisher-Tippett distribution or log-Weibulla distribution [13,14]. The corresponding density is depicted in fig. 1, taken from [12]. Its peak is a and its width is proportional to b. This distribution has mathematical expectation $\mu(X) = a + b\gamma$ c $\gamma \approx 0{,}58$ and deviation $\sigma(x) = \frac{\pi}{\sqrt{6}} b \approx 1{,}3b$. Notes that the validity of expression (3) depends on the quality of linear approximation $f(x)$ near the point $(a,0)$.

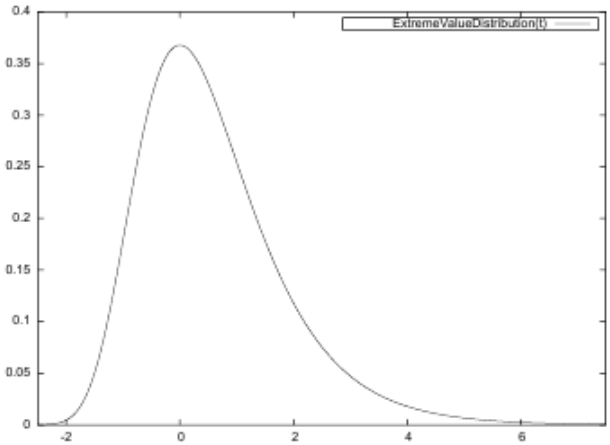

Figure. 1. An extreme value distribution when $a = 0$, $b = 1$.

III. MAXIMUM OF *X* WITH POISSON DISTRIBUTION

If maximum is taken using variables with Poisson distribution, we must take into account discrete character of the last. However, we can obtain expressions for average and standard maximum deviation, if we bring closer Poisson distribution by continuous function. We can obtain the expression for function $f(x)$ and use it for search for values a and b. Then:

$$\Phi(i;\lambda) = \sum_{x=0}^{i-1} \text{Poisson}(x;\lambda) = 1 - \sum_{x \ge i} \text{Poisson}(x;\lambda) \tag{4}$$

For $i >> \lambda$, this expression permits close approximations [13,14] as:

$$\Phi(i;\lambda) \approx 1 - \left(1 - \frac{\lambda}{i}\right) \cdot \text{Poisson}(i;\lambda) \approx \approx \text{Poisson}(i,\lambda) = e^{-\lambda} \frac{\lambda^i}{i!}. \tag{5}$$

Then we use Stirling approximation for factorial [13, 14] and we will get the following expression for function $f(i)$:

$$f(i) = \frac{1}{2}\ln(2\pi) + \lambda + i\ln i - (1+\ln\lambda)i + \frac{1}{2}\ln(i)\,. \quad (6)$$

If we abstract the fact that i must be integer we can calculate the parameter a by solving the equation:

$$\ln(2)y = \frac{1}{2}\ln(2\pi) + \lambda + i\ln i - (1+\ln\lambda)i + \frac{1}{2}\ln(i)\,, \quad (7)$$

or, that is equivalent to:

$$i = \frac{\ln(2)y - \frac{1}{2}\ln(2\pi i) - \lambda}{\ln\left(\frac{i}{\lambda}\right) - 1}, \quad (8)$$

which may be solved iteratively. Derivative $f(i)$ is determined by:

$$\ln\left(\frac{i}{\lambda}\right) + \frac{1}{2i}. \quad (9)$$

Denoting solution a and using condition $a >> \lambda$, we get:

$$b = \frac{1}{\ln\left(\frac{a}{\lambda}\right)}. \quad (10)$$

It follows, that if a is much more than λ, standard deviation becomes less than 1.

As maximum distribution is discrete, the small value of standard deviation results in distribution concentrating in two integers close to a.

II.II. Maximum of X with normal distribution

Now consider a particular case for variable x with standard normal distribution. Following [12], In this case

$$D(x) \approx \int_{-\infty}^{\infty} Z(u)du \quad (11)$$

For large values x, this integral law will be close to [2,3]:

$$D(x) \approx 1 - \frac{1}{x}Z(x) \approx 1 - \frac{1}{x\sqrt{2\pi}}e^{-\frac{x^2}{2}} \quad (12)$$

Thus we can get the following expression for the function $f(x)$:

$$f(x) = -\ln\left(\frac{1}{x}Z(x)\right) = \frac{1}{2}\left(\ln(2\pi) + x^2\right) + \ln(x) \quad (13)$$

Parameter a_s (subscript s for standard) is the solution of the equation:

$$a_s = \sqrt{2\ln(2)y - \ln(2\pi) - 2\ln(a_s)}\,, \quad (14)$$

which can be solved iteratively, not paying attention to the right member in the first iteration. The derivative *f(x)* is determined as:

$$x + \frac{1}{x}\,, \quad (15)$$

and therefore,

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s}\,. \quad (16)$$

Roughly, maximum has distribution with average value $1{,}17\sqrt{y}$ and standard deviation $1{,}11/\sqrt{y}$. Now we can find values a and b for any normal distribution with average μ(X) and standard deviation σ changing for x on $\frac{X - \mu(X)}{\sigma}$. It gives:

$$a = \sigma as + \mu(X), \quad (17)$$

$$b = \sigma bs.$$

The above theoretical results are the ones that we will be guided by the experiments.

III. Theoretical and Experiment Evaluation of Maximum Distribution of Full Differentials of Ciphers Mini Versions.

Let's give theoretical evaluation of maximum values of total differentials of mini cipher with 16-bit input and 16-bit master key.

As shown in [15,16], the laws of distribution of transitions XOR cipher tables mini asymptotically repeat a law conversion XOR distribution table of random permutations, which just obeys Poisson law [16]. Even at the level presented in [2-10] experiments performed to a limited set of encryption keys, it is seen that the results are practically independent of the use-played keys (for different keys, we have one and the same distribution of transitions, and the keys only affect distribution of one and the same set of transitions within the differential table of ciphers).

In our case power of the set of random variables is equal to the number of differential table cells without null string and zero column i.e. $(2^n - 1)^2$ for substitution of power 2^{16} we obtain $y \approx 2n = 32$.

The equation (8) has the following form:

$$i = \frac{\ln(2)\cdot 32 - \frac{1}{2}\ln(2\pi i) - \frac{1}{2}}{\ln(2i) - 1}\,. \quad (18)$$

Table I gives this equation solution by method of sorting.

Thus, equation solution (18) is a = 10. And then $b = \frac{1}{\ln(20)} = 0{,}33$. Note that formula (8) by which we determined the value a, works with the transition half value of differential table. Therefore calculating average value we must double the result obtained. And then $\mu(X) = 2{\cdot}10 + 2{\cdot}0{,}4{\cdot}0{,}58 = 20{,}386$.

Table I. EQUATION SOLUTION (18) BY METHOD OF SORTING

i	$\frac{\ln(2)\cdot 32 - \frac{1}{2}\ln(2\pi i) - \frac{1}{2}}{\ln(2i) - 1}$
8	11,71
9	10,40
10	9,84
11	9,36

This value agrees well with the results of calculations and experiments are presented in [4, etc.].

We have already noted that, since the distribution of the maximum of the discrete, the low value of the standard deviation $b = \frac{1}{\ln(20)} = 0{,}333$ leads to the fact that the distribution is concentrated in two integer values near $\mu(X) \approx 2a$. In our experiments with small ciphers are two values: 18 and 20.

However, the formation of an integral of the distribution of the maxima of a random permutation of the differential table (3) we find that the expectation value 20 does not suit us, because in this case the number of peaks excluded is 18 (the probability of such values obtained almost zero, while the experiments show that this value is one of the most likely). Therefore, further calculations will be carried out for the value of a = 9 (this correction is permissible under and simplifications used to rounding.) In this case $b = \frac{1}{\ln(18)} = 0{,}346$. Then

$$\mu(X) = 2{\cdot}9 + 2{\cdot}0{,}346{\cdot}0{,}58 = 18{,}4.$$

As a result, we will use the final expression for the integral of the distribution of the maxima (3) as:

$$D_{\max}(X) \approx e^{-e^{\frac{9-X}{0{,}346}}},$$

or

$$D_{\max}(X) \approx e^{-e^{\frac{18-2\cdot X}{0{,}692}}}. \qquad (19)$$

The results of calculations by formula (19) is in good agreement with experimental results for random permutations, presented in our paper [4].

Table. II shows the results of calculations of the value distribution of maxima (for the whole set of keys), made in accordance with the expression (19).

Table II. Maximum Value Distribution Of Mini Cipher For The Whole Set 2^{16} Keys Calculated By The Expression (19)

k^* (X_1,X_2)	Pr(k^*)	Число значений	Эксперимент
18 (18,16)	0,366 – 1,2·10–8 = 0,368	24109	27724
20 (10,9)	0,9459 – 0,368 = = 0,5779	37876	28287
22 (22,20)	0,99691 – 0,9459 = = 0,051	3343	1912
24 (24, 22)	0,99982 – 0,99691 = = 0,0029	191	90
26 (26,24)	0,999990 – 0,99982 = 0,00016	10	2
28 (28,26)	0,9999995 – –0,999990 = $8{,}5\cdot10^{-6}$	0,5	0

In the right column of the table 2 the results for reduced model of Byelorussian cipher, obtained from the experiments, are presented. From presented results it follows that maximum maximorum value for reduced cipher models equals 26. This value, practically, doesn't differ from average maximum of differential substitution tables. Thereby we confirm the statement (proposed in [3] and other papers) that evaluation cipher provable resistance can be made on the basis of maximum value of differential and linear probabilities obtained for one (any) cipher key.

The results obtained testify about rather good coincidence of theoretical and experimental results. Note that similar results were obtained by us and for other reduced cipher models (Kalina, Mukhomor, Rijndael and others).

IV. THEORETICAL AND EXPERIMENTAL EVOLUTION OF DISTRIBUTION OF DEVIATION OF MAXIMUMS OF LINEAR CORPS OF CIPHER MINI VERSIONS

Consider then what we get for distribution of deviation maximums reduced to 16-bit size of cipher model inputs.

In this case we will take as the basis approximation of the law of random substitution deviation (cipher) as a normal law, proposed in the paper [12].

According to the results of our work the theorem is true (with some our changes in designations):

Theorem. *For random n-bit substitution with n* > 5 *disbalance* Imv(*v.u*) *is the random value with distribution, which can be approximated in the form of normal law*

$$\Pr(\mathrm{Imb}(v, u) = 2x) \approx Z\left(\frac{x}{2^{(n-4)/2}}\right). \quad (20)$$

In our case disbalance is the bias of linear approximation table.

Using (14), for substitution of power 2^{16} we will obtain (in this case a set of random variables $(2^{16}-1)^2 \approx 2^{32}$, i.e. again y = 32):

$$a_s = \sqrt{2\ln(2)y - \ln(2\pi) - 2\ln(a_s)} = \\ = \sqrt{4\ln(2)n - \ln(2\pi) - 2\ln(a_s)};$$

$$a_s = \sqrt{\ln(2)64 - \ln(2\pi) - 2\ln(a_s)}, \quad (21)$$

$$b_s = \frac{a_s}{a_s^2+1} \approx \frac{1}{a_s} = \frac{1}{6} = 0{,}16.$$

Table III presents the results of equation solutions (21) by the selection method

Table III. Equation Solutions (21) By The Selection

a_s	$\sqrt{\ln(2)64 - \ln(2\pi) - 2\ln(a_s)}$
7	6,21 0,79
6,5	6,23 0,27
6,4	6,22 0,17
6,3	6,19 0,103
6,2	6,234 0,0349
6	6,24 0,24

In this case we need to do a small correction will result, focusing on the experimental data. We will consider the value a_s = 6.33, respectively, and

$$b_s = \frac{a_s}{a_s^2+1} \approx \frac{1}{a_s} = \frac{1}{6{,}33} = 0{,}1579 \quad (22)$$

(here we are already accounted for the results of this experiment, presented in Table. IV). Then, to have a degree 2^{16} of substitution and $\sigma = 2^{\frac{16-4}{2}} = 2^6$ in accordance with (17) we have

$$b = 64 \cdot 0{,}1579 = 10, 11,$$

and we arrive at the integral distribution law highs full differentials reduced 16-bit cipher model in the form:

$$D_{\max}(X) \approx e^{-e^{\frac{405-X}{10,1}}}, \quad (23)$$

or for actual results doubling table biases linear approximations

$$D_{\max}(X) \approx e^{-e^{\frac{810-X}{20,2}}}. \quad (24)$$

Table IV presents the results of calculations by defining distribution maximum values of linear hulls on the basis of the integral probability distribution law (24).

The presented results show that in this case the experimental data are close to the data calculated theoretically. Again, we can conclude that, in determining performance demonstrable resistance is possible to do a lin ear probability values obtained for the individual (any) key encryption.

Note that the results of previously performed theoretical and experimental evaluation of the values of the maximum biases of the linear approximation table random permutation of degree 2^{16} equal to 748 (estimated) and 720 (experiment) [18].

We see that in this case is almost the same as the results of experiments results. We now estimate the maximum values of the full differentials and linear hulls for 128-bit encryption

Table IV. RESULTS OF VALUE CALCULATIONS OF THE PROBABILITY DISTRIBUTION LAW (24) BY METHOD OF SORTING

k^* (X_1, X_2)	Pr(k^*)	Число значений	Эксперимент
< 768	$3{,}02\cdot10^{-4}$	20	27
770 (770,768)	$6{,}5\ 10^{-4} - 3{,}02\cdot10^{-4} = 3{,}48\ 10^{-4}$	23	21
772 (772,770)	$13\cdot10^{-4} - 6{,}5\ 10^{-4} = 6{,}5\ 10^{-4}$	42	44
774 (774,772)	0,00244–0,0013 = 0,0011	72	67
776 (776,774)	0,00431– 0,00244 = 0,00189	124	143
778 (778,776)	0,0072 – 0,0043 = 0,0254	190	149
…	…	…	
796 (796,794)	0,1334 – 0,108 = 0,01	1664	1696
…	…	…	
800 (800,798)	0,1918 – 0,1614 = 0,03	1991	2033
…	…	…	
808 (808,806)	0,3298 – 0,2937 = 0,036	2367	2382
810 (810,808)	0,368 – 0,3298 = 0,0382	2503	2476
812 (812,810)	0,4028 – 0,368 = 0,0348	2280	2354
814 (814,812)	0,4390 – 0,4028 = 0,0362	2374	2399
816 (816,814)	0,4746 – 0,4390 = 0,0356	2333	2467
818 (818,816)	0,5093– 0,4746 = 0,0346	2273	2359
820 (820,818)	0,5428 – 0,5093 = 0,3358	2200	2320
822 (822,820)	0,5752 – 0,5428 = 0,0324	2123	2243
…	…	…	
840 (840,838)	0,7977 – 0,7791 = 0,0186	1219	1259
…	…	…	
880 (880,878)	0,96954 – 0,9664 = 0,0031	205	186
…	…	…	
900 (900,898)	0,9886 – 0,98744 = 0,0011	76	57
…	…	…	
948 (948,946)	0,9989 – 0,99884 = 0,0001	7	4
950 (950,948)	$0{,}9990 - 0{,}9989 = 1{,}4\cdot10^{-4}$	9	6
…	…	…	
978 (978,976)	$0{,}99976 - 0{,}99973 = 2\cdot10^{-5}$	1	1
…	…	…	…
1008 (1008,1006)	$0{,}999946 - 0{,}999941 = 5\cdot10^{-6}$	0,327	1

ear probability values obtained for the individual (any) key encryption.

Note that the results of previously performed theoretical and experimental evaluation of the values of the maximum biases of the linear approximation table random permutation of degree 2^{16} equal to 748 (estimated) and 720 (experiment) [18].

We see that in this case is almost the same as the results of experiments results. We now estimate the maximum values of the full differentials and linear hulls for 128-bit encryption

V. DISTRIBUTION OF THE MAXIMUM DIFFERENTIAL AND BIAS FOR THE 128-BIT ENCRYPTION

Here we can only make a theoretical estimate of the expected results.

By analogy with the above we present first the solution of (18) by linear search.

Table V. EQUATION SOLUTIONS (18) BY THE SELECTION

i	$\frac{\ln(2)\cdot 256 - \frac{1}{2}\ln(2\pi i) - \frac{1}{2}}{\ln(2i) - 1}$
50	48
49	49,10
48	49,38
45	50,29

From Table V that as a solution, you can take i = 49. Then

$$b = \frac{1}{\ln(98)} = 0{,}218,$$

$$\mu(X) = 2\cdot 49 + 2\cdot 0{,}218\cdot 0{,}58 = 98{,}25.$$

As a result,

$$D_{\max}(X) \approx e^{-e^{\frac{98-2X}{0{,}436}}}. \quad (25)$$

Examples of calculations based on this formula illustrated in Table. VI.

TABLE VI. EXAMPLES OF CALCULATIONS USING FORMULA (25)

$2i$	$e^{-e^{\frac{98-2X}{0{,}436}}}$
96	2,035828665659390555880640669272 8e-44
98	0,368
100	0,990024312861776321390710003798 91
102	0,999999000861533295139221936592 55
104	0,999899919319259798068726688340 32
106	0,999999990025760160015160338175 33
108	0,999999999900428804426781088460 06
126	0,999999999999999999999999999901 96

The presented results show that in this case, would be the most severe (more likely) the two values of the maxima: 98 and 100. The remaining value of the maximum, which in this case is a representative set to be significantly less likely.

Based on the fact that the total number of cells in a differential table for 128-bit encryption $(2^{128} - 1)^2 = 1{,}157920892373161954235709850086 9e+77$, we can conclude that the expected value of the largest maximum will be close to 192.

In assessing the strength of ciphers to differential cryptanalysis attacks can focus on the maximum value obtained for a chance to take a key encryption, which leads to the resulting probability. $\frac{98 \div 100}{2^{128}} = 2^{-121}$.

For the linear approximation table 128-bit encryption, we have (see Table VII):

Table VII. SOLUTION OF (21) IN THE MANNER OF SELECTION FOR 128-BIT

a_s	$\sqrt{2\cdot\ln(2)\cdot 256 - \ln(2\pi) - 2\ln(a_s)}$
17	18,638 (1,638)
18	18,635 (0,635)
19	18,6323 (0,367)
20	18,62 (1,38)

And, therefore, $a_s = 19$. Then

$$b_s = \frac{a_s}{a_s^2 + 1} \approx \frac{1}{a_s} = \frac{1}{19} = 0{,}0526,$$

as for 128-bit encryption $\sigma = 2^{(n-4)/2} = 2^{62}$, arrive at the result

$$a = 19\cdot 2^{62} = 2^{4{,}25}\cdot 2^{62} = 2^{66} = 87747997204358712186.$$

We have a value close to the calculated for a random permutation of degree in 2^{128}. [19] And further

$$b = \sigma b_s = 2^{62}\cdot 0{,}0526 = 2^{57}.$$

This leads to the conclusion that the value of the maximum displacement will be concentrated around the value of 2^{62}, and the maximum linear probability come to value $\left(\frac{2^{66}}{2^{128-1}}\right)^2 = 2^{-122}$, which is consistent with previous results [19].

VI. CONCLUSION.

As the result of theoretical and experimental research made, the laws of maximum distributions (extreme distributions) XOR tables and bias tables of linear approximation transitions are established. In accordance with the results obtained for small cipher models we have come to the conclusion that practically all modern ciphers have rather small range of maximum changes of total differential and maximums of linear corps deviations so that it's possible to use the results of maximum differential probabilities and maximum linear probabilities calculated for arbitrarily taken (one) cipher key for evaluation of provable resistance indexes of these ciphers. It is confirmed experimentally that cryptographic transformations inherent SPN cipher designs (ciphers with square S-blocks), are balanced in the sense that the quality of transformations made by them practically doesn't depend on encryption keys.

For cipher as well as for random substitution of maximum differential values and linear halls maximums are not unexpected values. They obey to the integral law of distribution of extreme values of a set of independent random variables *x*, having one and the same distribution.

REFERENCES

[1] Lisitskaya I.V. Methodology for assessing resistance of block symmetric ciphers. / I.V. Lisitskaya // Automated control systems and automation devices, 2011, № 163, pp. 123-133.

[2] Dolgov V.I. Differential properties of symmetric block cipher submitted to the Ukrainian competition. / V.I. Dolgov, A.A. Kuznetsov, S.A. Isaev. // Electronic modeling. – 2011.– Vol. 33, № 6. – pp. 81-99.

[3] Kuznetsov A.A. Linear properties of symmetric block cipher submitted to the Ukrainian competition. / A.A. Kuznetsov, I.V. Lisitskaya, S.A. Isaev // Applied radioelectronics. – 2011. – Vol. 10, №2 – pp. 135-140.
[4] Lisitskaya I.V 32-bit block mini-version of a symmetric cryptographic algorithm for converting the information Muchomor. Estimate of the maximum value of the full differential of the cipher. / I.V. Lisitskaya, I.F. Stavitskiy // Scientific statements of Belgorod State University – 2011. – № 7 (102). – Issue 18/1 – pp. 177-186.
[5] The cryptographic properties of the reduced version of the cipher Muchomor. / I.V. Lisitskaya, O.I. Oleshko, S.N. Rudenko and others. // Special Telecommunication Systems and Information Protection. Scientific Papers, Kyiv. – 2010. – Issue 2(18). – pp. 33-42.
[6] Dolgov V.I. Research differential and cyclic properties of the reduced models of the cipher Labyrynt / V.I. Dolgov, I.V. Lisitskaya, A.V. Grigiriev, A.V. Shirokov // Applied radioelectronics. – 2009. – Vol. 8, №3 – pp. 283-289.
[7] Dolgov V.I. The mini version of the block symmetric cryptographic algorithm for converting the information to a dynamically controlled cryptoprimitives (Baby-ADE). / V.I. Dolgov, A.A. Kuznetsov, R.V. Sergienko, A.L. Belokovalenko // Applied radioelectronics – 2008. – Vol. 7, №3 – pp. 215-224.
[8] Lisitskaya I.V Large ciphers – random permutations / I.V. Lisitskaya, A.A. Nastenko // Interdepartmental Scientific and Technical Collection "Radiotechnica".– 2011. – Issue 166. – C. 50-55.
[9] Dolgov V.I. The study of cryptographic performance reduse models ciphers DES and GOST / V.I. Dolgov, J.A. Makarchuk, A.V. Grigoriev, E.V. Drobat'ko // Applied radioelectronics – 2011. – Vol. 10. – № 2. – pp. 127–134.
[10] The cryptographic properties of the reduced version of the cipher Kalina/ V.I. Dolgov, R.V. Oleinikov, A.U. Bol'shakov, and others. // Applied radioelectronics, 2010. – Vol. 9. – № 3. – pp. 349-354.
[11] Lisitskaya I.V.. A comparison of the effectiveness of superblocks some modern ciphers. Radioelektronika. Informatika. Upravlinnya. Zaporizhzhya 1(26)' – 2012. – pp. 37- 43.
[12] Joan Daemen, Vincent Rijmen Probability distributions of Correlation and Differentials in Block Ciphers. / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1–38.
[13] W. Feller An Introduction to Probability Theory and Its Applications, Vol.1. Wiley & Sons. 1968.
[14] Mathworld. http: //mathworld. wolfram.com/.
[15] Oleinikov R.V. Differential properties of substitutions/ / Р.В. Олейников, O.I. Oleshko, K.E. Lisitskiy, A.D. Teviashev // Applied radioelectronics –2010. – Vol. 9. – № 3. – pp. 326-333.
[16] Lisitskaya I.V. Properties of the distribution laws XOR tables and tables of linear approximations of random permutations. News of Kharkivskogo natsionalnogo universitetu imeni VN Karazina.– 2011. – №960, Issue 16. – pp. 196-206.
[17] Lisitskaya I.V. Symmetric block cipher, and Markov processes. / I.V. Lisitskaya // Applied radioelectronics. – 2012. – Vol. 11, № 2 – pp. 137-143.
[18] Dolgov V.I. Table properties of linear approximations of random permutations./ V.I. Dolgov, I.V. Lisitskaya, O.I. Oleshko // Applied radioelectronics. – 2010. – Vol. 9, № 3. – pp. 334-340.

Lisitskiy Konstantine is a student of the Kharkov National University of Radio Electronics; the specialty is Information Computer Systems Security. His main research interests include information security.

How to cite this paper: Lisitskiy K.E.,"On Maxima Distribution of Full Differentials and Linear Hulls of Block Symmetric Ciphers", IJCNIS, vol.6, no.1, pp.11-18,2014. DOI: 10.5815/ijcnis.2014.01.02

