Differential properties of random substitutions

Roman Oliynykov, Oleg Oleshko, Konstantin Lisitskiy

Abstract - **Estimated ratio for determining the maximum of the full differentials of modern symmetric block ciphers is derived.**

Keywords – **Random permutation, Differential distribution table.**

I. INTRODUCTION

It is noted that in our previous paper [1] there were presented results of computational experiments to research differential properties of random permutations. In particular, it was found that the average value of the maximum of differential tables is a specific indicator of a fixed order permutation, independent of the cyclic classes, which belongs to the substitution. In this paper we solve the problem of analytical determination of the average maximum of difference distribution tables of random permutations. It is grounded that these results can be applied for the derivation of strength indexes of modern symmetric block ciphers.

II. DERIVIATION OF ESTIMATED RATIO

It is considered the problem of determining the probability $\Pr\left(\Lambda_\pi(\Delta X,\Delta Y)=2k\right)$ of obtaining the cell value $\Lambda_\pi(\Delta X,\Delta Y)$ of differential distribution table of random permutation π of order 2^m for transformation of the input difference ΔX into the corresponding output difference ΔY is equal to $2k$.

It is noted that the similar problem was solved in the paper of Luke O'Connor [2] in 1994. However, the manner of presentation of his paper, especially in the implementation of evidence and interpretation of final results, is seemed unsatisfactory from viewpoint of authors of present work and made appropriate description of our own position on the regarded problem.

Theorem, which determines this probability, is formulated in [3] in the following form.

Claim. For any non-zero fixed $\Delta X, \Delta Y \in Z_2^m$, assuming that the substitution of π is chosen with equal probability from the set $\pi \in S_2^n$ and $0 \le k \le 2^{m-1}$,

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

where the function $\Phi(d)$ is given by

$$\Phi(d)=\sum_{i=0}^{d}(-1)^i \cdot \binom{d}{i}^2 \cdot 2^i \cdot i! \cdot (2d-2i)!\,. \qquad (2)$$

Our report proposes a simpler and more transparent version of the proof of this and other theorems, followed by further interpretation of the results.

III. COMPARISON OF THE DERIVED AND EXPERIMENTAL RESULTS

Calculations carried out in accordance with proposed method, together with the results of computer simulation illustrates table 1.

TABLE 1

COMPARISON OF THE DERIVED AND EXPERIMENTAL RESULTS

m	$\Lambda_\pi(\Delta X,\Delta Y)=2k$	$2k$	Simulation
4	3,379 0,459	6 8	6,7 $\le (m+3)$
5	3,08 1,708	6 8	7,94 $\le (m+3)$
6	6,6 0,675	8 10	9,1 $\le (m+4)$
7	2,641 0,221	10 12	10,3 $\le (m+4)$
8	0,8748	12	11,4
9	3,474 0,248	12 14	12,5 $\le (m+4)$
10	13,8495 0,99	12 14	13,4 $\le (m+4)$
11	3,952 0,247	14 16	14,5 $\le (m+4)$
12	15,787 0,987	14 16	15,3 $\le (m+4)$

Our experiments (in small 16-bit versions of ciphers) show that the full-round encryption transformation (of any modern cipher) is asymptotically behave as a random permutation for different encryption keys. For AES/Rijndael cipher it is even enough to have 4 rounds for archiving such results.

IV. CONCLUSION

Thus, the differential properties of encryption transformations of modern symmetric block ciphers are the demonstration of the random permutations properties, and in this sense AES/Rijndael and ciphers submitted to the Ukrainian national public cryptographic competition, are equivalent (indistinguishable).

REFERENCES

[1] R.V.Oliynykov, K.E. Lisitskiy, "Research of differential properties of the various cycle classes permutations", 12th International scientific conference "Information security in information and telecommunication systems". Kiev: KPI, 2009.

[2] L. J. O'Connor, "On the Distribution of Characteristics in Bijective Mappings", Advances in Cryptology. EUROCRYPT'93.