computing@computingonline.net
www.computingonline.net

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

DIFFERENTIAL CRYPTANALYSIS OF THE LIGHTWEIGHT BLOCK CIPHER CYPRESS-256

Mariia Rodinko [1], Roman Oliynykov [1], Khalicha Yubuzova [2]

[1] V.N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
m.rodinko@gmail.com, roliynykov@gmail.com
[2] Satbayev University, Almaty, Kazakhstan, hali4a@mail.ru

Paper history:
Received 16 February 2019
Received in revised form 10 April 2020
Accepted 15 April 2020
Available online 14 June 2020

Keywords:
lightweight cryptography;
block cipher;
differential cryptanalysis;
differential characteristic;
difference distribution table;
differential probability.

Abstract: This paper presents the results of differential cryptanalysis of the lightweight block cipher Cypress-256. The method for searching multi-round differential characteristic of the block cipher Cypress-256 is proposed. The searching assumes 1) building a big set of one-round differential characteristics and search for possible combinations of one-round characteristics into multi-round ones; 2) extending one-round differential characteristics with the probability up to certain threshold into multi-round characteristics. The following experiments show that the most probable one-round differential characteristics have input differences with 4-6 active bits which are distributed between different words. Besides that, high-probable one-round differential characteristics, which output differences have a small Hamming weight, cannot be extended to build high-probable multi-round differential characteristics. Due to application of the method assuming extension of one-round differential characteristics into multi-round ones, the differential characteristic up to 6 rounds was built, so 10-round block cipher Cypress-256 is resistant to differential cryptanalysis according to the requirements of practical criterion.

1. INTRODUCTION

Symmetric primitives include block [1, 2] and stream ciphers [3, 4], hash-functions, etc. Over the past years there is an increased interest in researching and designing lightweight symmetric algorithms that is explained by rapid development of such technologies as Internet of Things, smart-cards, etc., i.e., those that have a limited power consumption [5, 6]. Besides that, National Institute of Standards and Technology announced a competition for the development of lightweight algorithms for use in simple electronic devices [7].

Recently, the post quantum lightweight block cipher Cypress was developed in Ukraine [8]. Cypress provides both fast encryption speed and high level of cryptographic strength by operating 256- and 512-bit blocks and keys.

Cypress is based on Feistel network with ARX round function. ARX-transformation becomes very popular while developing lightweight cryptographic primitives due to the simplicity of its operations (addition, rotation and XOR). Block ciphers like SPECK [9], TEA [10], LEA [11], etc. are based on ARX-transformation.

The problem faced by developers of ARX-ciphers is the difficulty of evaluation of cipher strength to differential and linear cryptanalysis because of the absence of the universal evaluation model for such ciphers. If SPN ciphers are usually based on S-box with strong cryptographic properties [12, 13], ARX-ciphers are usually designed more heuristically.

The previous papers devoted to Cypress analysis include the evaluation of cipher performance and avalanche properties [8] along with methods of searching for high-probable one-round differential characteristics of Cypress-256 [14].

In this paper we present methods for searching of multi-round differential characteristics of Cypress-256 based on several assumptions. Our research shows that the block cipher Cypress-256 is resistant to differential cryptanalysis.

2. THE BLOCK CIPHER CYPRESS-256

The lightweight block cipher Cypress-256 operates on 256-bit blocks using a 256-bit key. The round function operations are performed on 32-bit words. The number of rounds is 10.

A schematic representation of the round function is shown in Fig. 1 [8]. The round function is the ARX-transformation that contains eight additions modulo 2^{32}, eight additions modulo 2 and eight rotations.

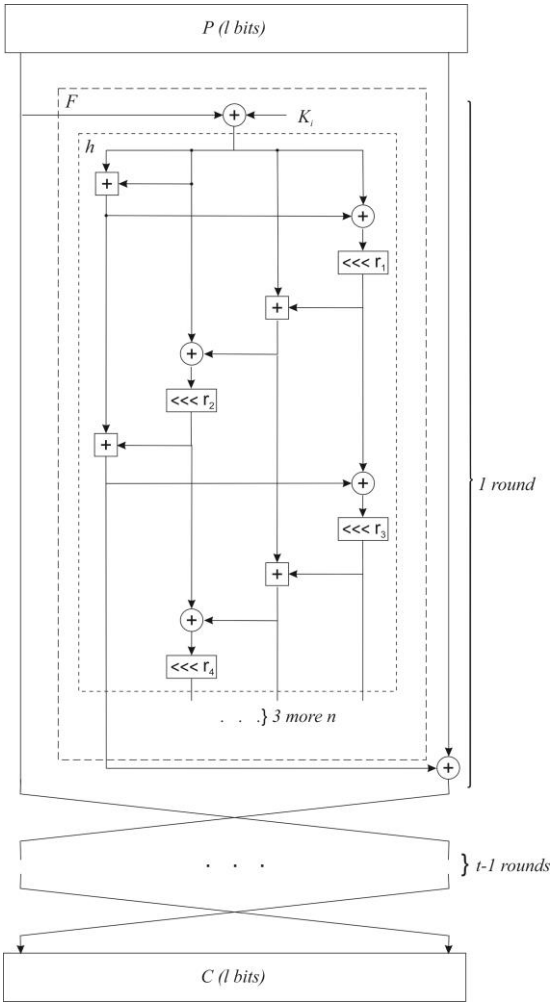

Figure 1 – Round function of Cypress-256

3. METHODS FOR ESTIMATING ARX-CIPHERS' STRENGTH TO DIFFERENTIAL CRYPTANALYSIS

Modulo addition in ARX-ciphers serves as the nonlinear operation, when round keys are usually entered using the XOR operation. Therefore, the cipher differential probability is determined by the probabilities of differences' propagation (calculated using the XOR operation) through modulo addition [15]. The module size is quite large compared with the size of S-boxes (typically 2^{32}-2^{64}), which, in terms of computational complexity, makes it impossible to construct a complete difference distribution table. Determining the minimum number of active branches is also a complicated task, since the alternation of simple (nonlinear and linear) operations, which is not based on a strong mathematical background, is difficult in terms of the analysis of its cryptographic properties.

A round of an ARX-cipher can contain several alternating linear and non-linear operations, while key-whitening is applied only at the beginning of each round. According to the classical theory [16], such a cipher is not a Markov cipher, because inputs to non-linear operations starting from the second one are not randomized by the key. Nevertheless, in the modern papers devoted to the differential cryptanalysis of ARX-ciphers the assumption that a cipher is a Markov cipher is made, and the probability of one-round differential characteristic is calculated as a product of probabilities of differences' propagation through the non-linear operations [15]. Such an assumption will not have a significant effect on the evaluation result, but greatly simplify the evaluation process (even so the single examples when a cipher behaves as a non-Markov cipher are presented in literature [17]). In any case, currently, it is unknown how to calculate the differential probability in case of the assumption that a cipher is not a Markov cipher. The results presented in this paper are also based on the assumption that the block cipher Cypress-256 is a Markov cipher.

An approach to design of ARX-ciphers which are provably secure against differential (linear) cryptanalysis was presented in [18]. When a wide trail strategy is applied to block ciphers based on S-boxes, a so-called long trail strategy is proposed for ARX-ciphers. A new strategy proposes to use S-boxes along with simple linear operations [18]. The application of the proposed approach to SPARX cipher allowed obtaining the estimation of the upper bound for SPARX differential probability.

Concerning estimation of existing ARX-ciphers, nowadays, there is no universal method for estimation of the upper bound of differential characteristic probability for ARX-ciphers. The existing estimation methods are usually based on the results of application of heuristic algorithms of searching for the best differential characteristics [15, 17]. The most known such methods are:

− the modified Matsui algorithm with application of partial difference distribution tables [15], the most developed among the existing methods;

− the method based on a search for probabilistic neutral bits [19] (currently it is applied to the stream ciphers Salsa and ChaCha);

– the method based on SAT solvers [17], which was also applied to Salsa.

The method based on application of partial difference distribution tables is the most used [15].

A difference distribution table (DDT) for the addition of *n*-bit words modulo 2^n contains the probabilities of transition of two input differences into the output difference after propagating through the non-linear operation.

Definition 1 [15, 20]. Let α, β and γ be fixed *n*-bit XOR differences. The XOR differential probability of addition modulo 2^n is the probability with which α and β propagate to γ through the addition operation, computed over all pairs of *n*-bit inputs (*x*, *y*):

$$\begin{aligned}\mathrm{xdp}^{+}(\alpha,\beta\to\gamma) = 2^{-2n}\cdot\#\{(x,y):\\ ((x\oplus\alpha)+(y\oplus\beta))\oplus(x+y)\} = \gamma.\end{aligned} \quad (1)$$

Calculation of probability by looking over all input pairs even for one transition is a computationally hard task. An effective algorithm for xdp^{+} calculation is proposed in [21].

Even by application the effective algorithm because of the large size of module *n* the full DDT cannot be calculated in practice within a reasonable time. That's why in [15] authors propose to build a so-called partial DDT that contains differentials $(\alpha,\beta\to\gamma)$ with the probability which is equal to or exceeds the given threshold p_{thres} [15]:

$$(\alpha,\beta,\gamma)\in D \Leftrightarrow (\alpha,\beta\to\gamma)\geq p_{thres}. \quad (2)$$

Then it is proposed to build such a partial table for the whole round function and, using the modified Matsui algorithm, search for differential characteristics. This method was successfully applied to block cipher based on Feistel network with ARX-like round function: SPECK, TEA, etc. The method described above is more suited to ciphers with a fairly simple round function, which does not assume the division of the input value into words (for example, for most well-known lightweight cryptography algorithms [22-33]). This is explained by the fact that when themodulo addition and rotation operations are applied to the whole input value, constructing partial DDT for such a round function is simple enough.

4. BASIC ASSUMPTIONS CONCERNING THE DIFFERENTIAL CRYPTANALYSIS OF CYPRESS-256

Define the difference between a pair of texts by XOR operation ($\oplus$) and denote the addition modulo 2^{32} as $\boxplus$. Let us introduce the following assumptions.

Assumption 1. Cypress block cipher is a Markov cipher, so:

1) The probability of one-round differential characteristic averaged over keys $\mathrm{EDP}^{(1)}(\Omega)$ is equal to the product of probabilities of differences' transformations while propagating through eight modulo additions:

$$\mathrm{EDP}^{(1)}(\Omega) = \prod_{i=1}^{8}\mathrm{xdp}^{+}(\alpha_i,\beta_i\to\gamma_i), \quad (3)$$

where $(\alpha_i,\beta_i)-$ the differences at the input of *i*-th adder, γ_i- the difference at the output of *i*-th adder.

2) The probability of *r*-round differential characteristic averaged over keys is defined by the product of probabilities of one-round differential characteristics [16].

Let $(\Omega_1,\Omega_2,...,\Omega_r)$ be a set of one-round differential characteristics such that $\Omega_1=(\alpha,\beta_1),\Omega_2=(\beta_1,\beta_2),...,\Omega_r=(\beta_{r-1},\beta_r)$ and $\Omega=(\alpha,\beta_1,...,\beta_r)$. Then the probability $\mathrm{EDP}^{(r)}(\Omega)$ can be approximated as:

$$\mathrm{EDP}^{(r)}(\Omega) = \prod_{i=1}^{r}\mathrm{EDP}^{(1)}(\Omega_i). \quad (4)$$

Assumption 1 arises from generally accepted assumptions which are made to simplify obtaining evaluations for ARX-ciphers [15,17].

Assumption 2. While calculating the output difference γ, which is the result of transformation of the input differences α and β after propagation through the modulo addition operation, the output difference with the maximum probability is chosen:

$$\gamma = \boxplus(\alpha,\beta), \mathrm{xdp}^{+}(\alpha,\beta\to\gamma) = \max\Gamma, \quad (5)$$

where $\Gamma-$ the set of all possible output differences for (α,β).

In many cases, for a pair of input differences (α,β) there are exist several output differences with the maximum probability. If there are not so many such differences (≈5-10), then differential trails for all possible variants are calculated. If $\max\Gamma$ is small enough, the number of output differences with the maximum probability can be too large (thousands and tens of thousands). Then a random sampling is made from the set of differences

which have the maximum probability, and differential trails are built only for chosen differences.

Assumption 3. In Cypress-256 the input differences of one-round differential characteristics with high probability have a small Hamming weight, i.e., ≈3-7 active bits (which are in different words). Such an assumption is explained by the fact that input differences of the most probable transitions in DDT for modulo addition have a small number of active bits. Let us justify Assumption 3 in details.

Definition 2. The number of active bits *b* in the difference (α, β) which enters the adder's input, is the number of "1" which is contained in $\alpha \oplus \beta$.

Consider a partial DDT for addition modulo 2^{32} that contains transitions with the probability $\mathrm{xdp}^+(\alpha, \beta \to \gamma) \geq 1/2$. For the transitions with the probability $\mathrm{xdp}^+(\alpha, \beta \to \gamma) = 1$ (there are only four such transitions in DDT) the number of active bits in the output difference is equal to $b \leq 1$. Note that it is true for any *n*.

For transitions with the probability $\mathrm{xdp}^+(\alpha, \beta \to \gamma) = 1/2$ (for $n = 32$ there are only 744 such transitions) the number of active bits is limited by two, $b \leq 2$.

In [20] it is presented the expression that describes the connection between bit positions of the input and output differences. The upper bound of differential probability for modulo addition operation is defined as [20]:

$$\Pr[\alpha, \beta \to \gamma] \leq 2^{-k}, \quad (6)$$

where $k = \#\{i : \neg(\alpha[i] = \beta[i] = \gamma[i]), 0 \leq i \leq n-2\}$, i.e., the number of bit positions excluding the most significant bit where the bits in differences α, β, γ are not equal.

Thereby, the minimization of the number of active bits in difference at the inputs of modulo adders increases the total probability of differential characteristic. In Cypress-256 the first three words of differences which are served at the input of the round function get on the entrance of modulo addition operation right away, and the fourth word – after application of XOR and rotation, so the assumption about a small number of active bits at the input of the round function is rationale.

Taking into account the influence of linear operations on the process of active bits distribution, it is assumed that 1-2 active bits at the input of the round function will spread well between different words at the output. The experiments have shown that 1 active bit at the input of the round function transfers into at least 7 active bits at the output (see Table 1). However, several active bits in different words can be destroyed by applying linear operations. So, approximately 3-7 active bits at the input of the round function which are distributed between different words allow obtaining a differential characteristic with high probability because they provide the optimal distribution of active bits to maximize the probabilities of transformations at modulo adders.

Table 1. The results of distribution of active bits for the round function of Cypress-256 block cipher

128-bit input difference (1 denotes the word which contains active bits)	Number of active bits at the output of the round function	
	Lower bound	Upper bound
1000	14	14
0100	19	19
0010	7	7
0001	10	10
1100	5	33
0110	12	26
0011	3	17
0101	9	29
1010	7	21
1001	4	24
1110	2	40
1101	5	43
1011	3	21
0111	2	36

5. SEARCHING FOR HIGH-PROBABLE MULTI-ROUND DIFFERENTIAL CHARACTERISTICS OF CYPRESS-256

In Cypres-256 a 128-bit input of the round function is divided to 32-bit words that pass through many additions, so partial DDT should contain differential with a low enough probability. Besides that the number of differential trains increases with each round. It seems it is more efficient not to build partial DDT, but calculate probabilities on-the-fly using the algorithm proposed in [21].

Several methods of searching for the most probable one-round differential characteristics of Cypress-256 are presented in [14]. The optimized method allowed obtaining one-round differential characteristic with probability ¼. Now we present the methods of searching for multi-round differential characteristics of Cypress-256 and the results of their applications.

The goal of search for differential characteristics is to find high-probable differential trails and prove that the probability of the best found (*r*-1)-round differential characteristic is $\mathrm{EDP}^{(r-1)}(\Omega) < 2^k$, where *k* is the key length. For Cypress-256 it is

proposed to build a sufficiently big set of one-round differential characteristics and search for possible combinations of one-round characteristics into multi-round ones. The method consists of the following steps.

1) Building the set of input differences Ξ which will be used for building one-round characteristics according to Assumption 3. Include to the set Ξ all possible combinations of 128-bit strings with a Hamming weight of 1-7 bits (128 is the length of the half block which is the input of the round function). Since we are interested in not only the most probable characteristics, the differences with a Hamming weight of 1-3 bits are also included to the set.

2) Building one-round differential characteristics for input differences from the set Ξ. Calculating output differences obtained after propagating the modulo addition operation according to Assumption 2. Calculating the probability $\mathrm{EDP}^{(1)}(\Omega)$ of one-round differential characteristic according to item 1 of Assumption 1. Note that for one input difference, usually, there are several differential characteristics.

3) Taking into account that the key length is 256 bits and the number of encryption rounds is 10, from all calculated differential characteristics include to the set Ψ those that have the probability $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-256/10} \geq 2^{-26}$.

4) If for input differences with some Hamming weight the calculation of all differential characteristics requires significant computational resources, then decrease the value $\mathrm{EDP}^{(1)}_{thres}(\Omega)$ for differential characteristics built for input differences with this Hamming weight.

5) Searching for combinations of one-round differential characteristics from the set Ψ into two-round (multi-round) ones.

Using available computational resources, the set Ψ that contains high-probable one-round differential characteristics was built. The results of constructing the set are presented in Table 2.

Table 2. The parameters of the set of high-probable one-round differential characteristics

Input difference Hemming weight	1	2	3	4	5	6
$\mathbf{EDP}^{(1)}_{thres}(\Omega)$, $\log_2 n$	-26	-26	-26	-26	-18	-10
$\mathbf{MEDP}^{(1)}(\Omega)$, $\log_2 n$	> -26	-14	-12	-6	-2	-3

Despite some characteristics have the input difference which matches the output difference of

Differential characteristics built for input differences with a Hamming weight of 4-6 bits have the high probability. Some of the obtained high-probable one-round differential characteristics are presented in Table 3.

Table 3. The most probable one-round differential characteristics of Cypress-256

Input – output differences in 32-bit words, hex	$\mathbf{EDP}^{(1)}(\Omega)$, $\log_2 n$
0 80000000 800000 80008080 – 80000000 4000 80 80	-2
80000 80080000 80000000 80000000 – 800 4040040 80080000 80000	-3
0 80000000 1800000 80008080 – 80000000 4000 80 80	-3
180000 80080000 80000000 80000000 – 800 4040040 80080000 80000	-4
80000 80000 80800000 8080 – 80000800 4044040 80080080 80080	-5
80000000 0 80000000 80008000 – 88000000 40404404 808088 800088	-6
80000000 80000000 80800000 80 – 8000000 40400404 808008 800008	-6
80 80 80000080 8000 – 8 40040440 80800800 80000800	-7
8000 8000 8080 800000 – 800 4044040 80080080 80080	-7
80000000 80000800 800 800 – 800000 40040040 80000800 80000000	-7
0 80 80000000 808080 – 80 400000 8000 8000	-7
0 800000 8000 80800080 – 800000 40 80000000 80000000	-7
80000000 80000000 81800000 80 – 8000000 40400404 808008 800008	-7
0 100 1 1010100 – 100 800000 10000 10000	-8
0 200 2 2020200 – 200 1000000 20000 20000	-8
0 800 8 8080800 – 800 4000000 80000 80000	-8
0 1000 10 10101000 – 1000 8000000 100000 100000	-8
0 8000 80 80808000 – 8000 40000000 800000 800000	-8
180 80 80000080 8000 – 8 40040440 80800800 80000800	-8
100 80 80000000 808080 – 80 400000 8000 8000	-8
8000 8000 8180 800000 – 800 4044040 80080080 80080	-8
0 40 c0000000 404040 – 40 200000 4000 4000	-8
0 800000 18000 80800080 – 800000 40 80000000 80000000	-8
0 40000000 80400000 40004040 – 40000000 2000 40 40	-8

other differential characteristics, no combinations of one-round characteristics in two-round ones were found.

The next step in searching for multi-round characteristics includes extending one-round differential characteristics from the set Ψ to several rounds. Note that Feistel network architecture feature allows selecting the input difference so as to "skip" one encryption round, i.e., creating such a situation when at the certain round the value $\Delta X = 0,$ which transformation probability is 1, is served as the input to the round function.

In order to maximize the probability of differential characteristic for the first three encryption rounds, it is proposed to submit ΔX as a left half of the input difference and $\Delta Y = F(\Delta X) -$ as a right half. Because of this, the probability of differential characteristics for the first and the third rounds will be equal, and for the second round – will be equal to 1. The trail of propagating the input difference through 4 encryption rounds is presented in Fig. 2.

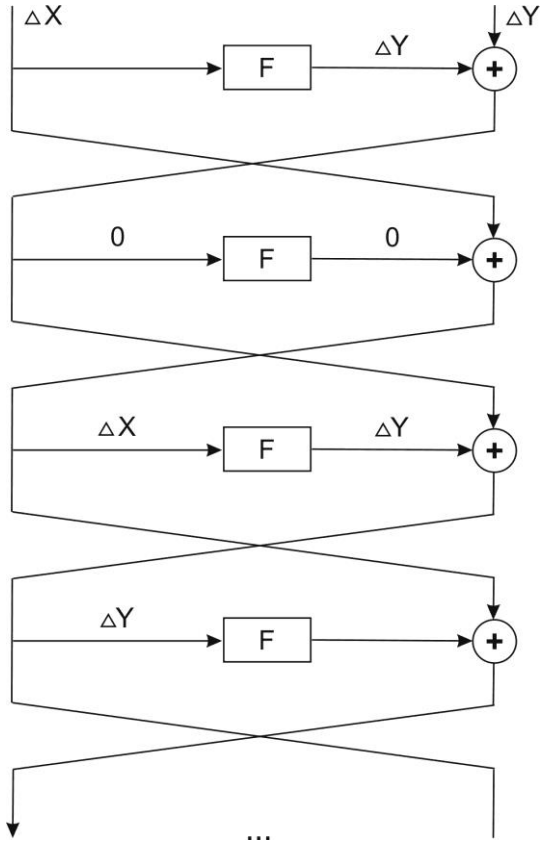

Figure 2 – Path of the input difference propagation for four encryption rounds

So, the search for the most probable multi-round differential characteristics of Cypress-256 consists of the following steps.

1) Define 256-bit input difference as such that consists of two 128-bit halves ΔX and ΔY.

2) Construct the set Z of 256-bit input differences for searching the multi-round differential characteristics in the following way. Define the input difference ζ_i form the set Z as $\zeta_i = (\Delta X_i \,|\, \Delta Y_i),$ where ΔX_i and $\Delta Y_i -$ input and output differences of *i*-th differential characteristic from the set Ψ correspondingly.

3) For each input difference ζ_i from the set Z build differential characteristics for j rounds provided that $\mathrm{EDP}^{(j)}(\Omega) > 2^{-256}$. Build the differential characteristic for each round according to the items (2)-(4) from the method presented above.

During the search, the random sampling mechanism was applied in two cases:

- while calculating output differences for modulo addition operation;
- while choosing the output of the round function between encryption rounds.

Due to the application of random sampling, $\mathrm{EDP}^{(j)}(\Omega)$ is an approximated value (calculation of all existing differential trails is a computationally hard task even for one input difference).

Using the described approach, one of the most probable differential characteristics with the following parameters was found:

1 round: $\Omega(a,b)$ = (00000000 80008000 00800080 00800080 80008000 40004000 00800080 00800080, 00000000 80008000 00800080 00800080 00000000 00000000 00000000 00000000),
$\log_2 \mathrm{EDP}^{(1)}(\Omega) = -10,\ \log_2 \mathrm{EDP}^{(1)}(\Omega) = -10;$

2 round: $\Omega(a,b)$ = (00000000 00000000 00000000 00000000 00000000 80008000 00800080 00800080, 00000000 00000000 00000000 00000000 00000000 80008000 00800080 00800080),
$\log_2 \mathrm{EDP}^{(1)}(\Omega) = 0,\ \log_2 \mathrm{EDP}^{(2)}(\Omega) = -10;$

3 round: $\Omega(a,b)$ = (00000000 80008000 00800080 00800080 00000000 00000000 00000000 00000000, 00000000 80008000 00800080 00800080 80008000 40004000 00800080 00800080),
$\log_2 \mathrm{EDP}^{(1)}(\Omega) = -10,\ \log_2 \mathrm{EDP}^{(3)}(\Omega) = -20;$

4 round: $\Omega(a,b)$ = (80008000 40004000 00800080 00800080 00000000 80008000 00800080 00800080, 80008000 40004000 00800080 00800080 c0204020 90009000 00a000a0 00800080),
$\log_2 \mathrm{EDP}^{(1)}(\Omega) = -27,\ \log_2 \mathrm{EDP}^{(4)}(\Omega) = -47;$

5 round: = (c0204020 90009000 00a000a0 00800080 80008000 40004000 00800080 00800080,

c0204020 90009000 00a000a0 00800080 5208d204 40444044 08820882 0a800a80),

$$\log_2 \mathrm{EDP}^{(1)}(\Omega) = -74,\ \log_2 \mathrm{EDP}^{(5)}(\Omega) = -121;$$

6 round: = (5208d204 40444044 08820882 0a800a80 c0204020 90009000 00a000a0 00800080, 5208d204 40444044 08820882 0a800a80 266e7071 a74313f2 0088e7e0 10fa6fd2),

$$\log_2 \mathrm{EDP}^{(1)}(\Omega) = -102,\ \log_2 \mathrm{EDP}^{(6)}(\Omega) = -223.$$

So, the most probable differential characteristic found for 6 rounds has the probability $\mathrm{MEDP}^{(6)}(\Omega) \approx 2^{-223}$.

Due to using the random sampling, $\mathrm{MEDP}^{(6)}(\Omega)$ can a bit vary in different experiments, but it does not sufficiently influence on the result because

$$\mathrm{MEDP}^{(7)}(\Omega) << 2^{-256}, 7 < (r-1). \qquad (7)$$

6. CONCLUSION

The block cipher Cypress-256 is resistant to differential cryptanalysis according to the requirements of practical criterion. One of the most probable differential characteristics was found for 6 rounds of Cypress-256 and has the probability $\mathrm{MEDP}^{(6)}(\Omega) \approx 2^{-223}$.

The experiments show that one-round differential characteristics, which output differences have a small Hamming weight (and, respectively, a high probability), cannot be extended to build a high-probable multi-round differential characteristic.

Research results can be useful for analyzing and evaluating the effectiveness of lightweight encryption algorithms, as well as in other practically important applications [34-41].

7. REFERENCES

[1] R. Oliynykov et al., "A new encryption standard of Ukraine: The Kalyna block cipher," *IACR Cryptology ePrint Archive*, 2015, 650.

[2] Pub, NIST FIPS. "197: Advanced encryption standard (AES)," *Federal Information Processing Standards Publication*, 197.441: 0311, 2001.

[3] I. Gorbenko, A. Kuznetsov, M. Lutsenko and D. Ivanenko, "The research of modern stream ciphers," *Proceedings of the 2017 4th IEEE International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, 2017, pp. 207-210.

[4] O. Kuznetsov, M. Lutsenko and D. Ivanenko, "Strumok stream cipher: Specification and basic properties," *Proceedings of the 2016 Third IEEE International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*, Kharkov, 2016, pp. 59-62.

[5] N. Mouha, "The design space of lightweight cryptography," *Proceedings of the NIST Lightweight Cryptography Workshop*, 2015, pp. 1-19.

[6] A. Kuznetsov, Y. Gorbenko, A. Andrushkevych and I. Belozersev, "Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2," *Proceedings of the 2017 4th IEEE International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkov, 2017, pp. 203-206.

[7] Lightweight Cryptography. Project Overview [Online]. Available at: https://csrc.nist.gov/projects/lightweight-cryptography

[8] A. Andrushkevych, Y. Gorbenko, O. Kuznetsov, R. Oliynykov, M. Rodinko, "A prospective lightweight block cipher for green IT engineering," in: Kharchenko V., Kondratenko Y., Kacprzyk J. (eds) *Green IT Engineering: Social, Business and Industrial Applications. Studies in Systems, Decision and Control*, Springer, Cham, vol 171, 2019, pp. 95-112. DOI: 10.1007/978-3-030-00253-4_5

[9] R. Beaulieu et al., "The SIMON and SPECK lightweight block ciphers," *Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1-6.

[10] D. J. Wheeler and R. M. Needham, "TEA, a Tiny Encryption Algorithm," *Proceedings of the International Workshop on Fast Software Encryption*, Springer, Heidelberg, 1995, pp. 363–366.

[11] D. Hong, et al., "LEA: A 128-bit block cipher for fast encryption on common processors," *Proceedings of the International Workshop on Information Security Applications*, Springer, Cham, 2013, pp. 3-27.

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

[13] M. Rodinko, R. Oliynykov, Yu. Gorbenko, "Optimization of the high nonlinear S-boxes generation method," *Tatra Mountains Mathematical Publications*, vol. 70, no. 1, pp. 93-105, 2017.

[14] M. Rodinko, R. Oliynykov and R. Eliseev, "Search for one-round differential characteristics of lighweight block cipher Cypress-256," *Proceedings of the 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2018, pp. 312-315.

[15] A. Biryukov, V. Velichkov, "Automatic search for differential trails in ARX ciphers," *CT-RSA*, vol. 8366, pp. 227-250, 2014.

[16] X. Lai, J. L. Massey and S. Murphy, "Markov ciphers and differential cryptanalysis," *Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 1991, pp. 17-38.

[17] N. Mouha,, and B. Preneel, "Towards finding optimal differential characteristics for ARX: Application to Salsa20," *Cryptology ePrint Archive*, Report 2013/328, 2013.

[18] D. Dinu et al., "SPARX: A family of ARX-based lightweight block ciphers provably secure against linear and differential attacks," *Proceedings of the ASIACRYPT'16*, pp. 1-21, 2016.

[19] J. P. Aumasson et al., "New features of Latin dances: analysis of Salsa ChaCha and Rumba," *Lecture Notes in Computer Science*, vol. 5086, 2008, pp. 470-488.

[20] H. Lipmaa, J. Wallén, and P. Dumas, "On the additive differential probability of exclusive-or," in: Roy, B.K., Meier, W. (eds.) *Proceedings of the International Workshop on Fast Software Encryption, Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol. 3017, 2004, pp. 317-331.

[21] H. Lipmaa and S. Moriai, "Efficient algorithms for computing differential properties of addition," *Proceedings of the International Workshop on Fast Software Encryption*, Springer, Berlin, Heidelberg, 2001, pp. 336-350.

[22] B. Liu, L. Li, R. Wu, M. Xie and Q. P. Li, "Loong: A family of involutional lightweight block cipher based on SPN structure," *IEEE Access*, vol. 7, pp. 136023-136035, 2019.

[23] D. Sehrawat, N. S. Gill and M. Devi, "Comparative analysis of lightweight block ciphers in IoT-enabled smart environment," *Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, India, 2019, pp. 915-920.

[24] I. Khairullin and V. Bobrov, "On cryptographic properties of some lightweight algorithms and its application to the construction of S-boxes," *Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Saint Petersburg and Moscow, Russia, 2019, pp. 1807-1810.

[25] E. Marsola do Nascimento and J. A. Moreira Xexeo, "A flexible authenticated lightweight cipher using Even-Mansour construction," *Proceedings of the 2017 IEEE International Conference on Communications (ICC)*, Paris, 2017, pp. 1-6.

[26] R. S. Mahantesh and S. Mohapatra, "Design of secured block ciphers PRESENT and HIGHT algorithms and its FPGA implementation," *Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, 2018, pp. 1113-1118.

[27] S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganne and R. Tourki, "Performance evaluation and design considerations of lightweight block cipher for low-cost embedded devices," *Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, 2016, pp. 1-7.

[28] O. Kara and M. F. Esgin, "On analysis of lightweight stream ciphers with Keyed update," *IEEE Transactions on Computers*, vol. 68, issue 1, pp. 99-110, Jan. 2019.

[29] M. Yoshikawa, Y. Nozaki and K. Asahi, "Vulnerability evaluation accelerator for lightweight ciphers," *Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, New York, NY, 2016, pp. 377-381.

[30] M. A. Philip and Vaithiyanathan, "A survey on lightweight ciphers for IoT devices," *Proceedings of the 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy)*, Kollam, 2017, pp. 1-4.

[31] C. A. Lara-Niño, M. Morales-Sandoval and A. Díaz-Pérez, "An evaluation of AES and present ciphers for lightweight cryptography on smartphones," *Proceedings of the 2016 International Conference on Electronics,*

Communications and Computers (CONIELECOMP), Cholula, 2016, pp. 87-93.

[32] B. J. Mohd and T. Hayajneh, "Lightweight block ciphers for IoT: Energy optimization and survivability techniques," *IEEE Access*, vol. 6, pp. 35966-35978, 2018.

[33] C. Zhao, Y. Yan and W. Li, "An efficient ASIC Implementation of QARMA lightweight algorithm," *Proceedings of the 2019 IEEE 13th International Conference on ASIC (ASICON)*, Chongqing, China, 2019, pp. 1-4.

[34] C. A. Lara-Nino, M. Morales-Sandoval and A. Diaz-Perez, "Novel FPGA-based low-cost hardware architecture for the PRESENT block cipher," *Proceedings of the 2016 Euromicro Conference on Digital System Design (DSD)*, Limassol, 2016, pp. 646-650.

[35] K. Runovski, H.-J. Schmeisser, "On the convergence of fourier means and interpolation means," *Journal of Computational Analysis and Applications*, vol. 6, issue 3, pp. 211-227, 2004.

[36] B. P. Tkach, & L. B. Urmancheva, "Numerical-analytic method for finding solutions of systems with distributed parameters and integral condition," *Nonlinear Oscillations*, vol. 12, issue 1, pp. 113-122, 2009. doi:10.1007/s11072-009-0064-6

[37] R.K. Chornei, V.M. Hans Daduna, P.S. Knopov, P. "Controlled Markov fields with finite state space on graphs," *Stochastic Models*, vol. 21, issue 4, pp. 847-874, 2005. doi:10.1080/15326340500294520

[38] L. Dalmasso, F. Bruguier, P. Benoit and L. Torres, "Evaluation of SPN-based lightweight crypto-ciphers," *IEEE Access*, vol. 7, pp. 10559-10567, 2019.

[39] I. K. Dutta, B. Ghosh and M. Bayoumi, "Lightweight cryptography for Internet of insecure things: A survey," *Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2019, pp. 0475-0481.

[40] A. Heuser, S. Picek, S. Guilley and N. Mentens, "Lightweight ciphers and their side-channel resilience," *IEEE Transactions on Computers*, pp. 1-20, 2020.

[41] N. A. Gunathilake, W. J. Buchanan and R. Asif, "Next generation lightweight cryptography for smart IoT devices: Implementation, challenges and applications," *Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, 2019, pp. 707-710.

***Mariia Rodinko**, PhD student at Information Systems and Technologies Security Department at V.N. Karazin Kharkiv National University. Scientific interests: block ciphers analysis and development.*

***Roman Oliynykov**, a Professor at Information Systems and Technologies Security Department at V.N. Karazin Kharkiv National University. Scientific interests: analysis and development of symmetric primitives, software security, blockchain.*

***Khalicha Yubuzova,** Master of Technical Sciences, a Lecturer of the Academic Department "Cybersecurity, Information Processing, and Storage" at the Satbayev University (Almaty, Kazakhstan). Research interests: information security, cryptography, QKD, network technologies.*