An Approach to Search for Multi-Round Differential Characteristics of Cypress-256

Mariia Rodinko, Roman Oliynykov
Department of Information Systems and Technologies Security
V.N. Karazin Kharkiv National University
Kharkiv, Ukraine
m.rodinko@gmail.com, roliynykov@gmail.com

Abstract — **In this work it is considered the differential cryptanalysis of the lightweight block cipher Cypress that was recently developed in Ukraine. Firstly, a cryptanalysis model for Cypress block cipher is introduced. Then a method for searching for multi-round differential characteristics for Cypress-256 is proposed. The method includes the construction of a big set of one-round characteristics with further combination of them. The application of the proposed method reveled no match within the constructed set that is good for Cypress-256 from the point of view of its strength to differential cryptanalysis. The analysis of constructed set showed that inputs with the minimal Hemming weight are not always leads to high probable characteristics (especially, multi-round ones) and the most popular characteristics with a high probability have inputs with 5-6 active bits.**

Keywords — block cipher; Cypress; differential cryptanalysis; lightweight cryptography

I. INTRODUCTION

The symmetric cryptography is one of the most popular topics in information security. Symmetric ciphers provides confidentiality which is a very important property in the modern world. Ukraine has a national standard of Kalyna block cipher [1]. Stream ciphers are also investigated [2] and Strumok stream cipher is developing [3].

Nowadays, the great interest is devoted to lightweight block ciphers [4] which are simple and fast for implementation in devices with low power consumption [5]. Such ciphers are SPECK [6], TEA [7] etc. Recently, the lightweight block cipher called "Cypress" was developed in Ukraine [8]. Cypress has a good performance and simple implementation; good statistical properties; a strong key schedule etc.

The next task is to evaluate Cypress's strength to differential attacks. In [9] we proposed the methods for searching one-round differential characteristics with high probability for Cypress-256 where the best characteristic with probability ¼ was found.

The goal of this paper is to start to evaluate probabilities of multi-round differential characteristics of Cypress-256. Firstly, we bring a scheme of Cypress block cipher. Then we introduce the cryptanalysis model that includes some assumptions we are based on (the assumptions agreed upon the recent results in the area of ARX-ciphers differential cryptanalysis). Then we propose the method for searching for multi-round differential characteristics with high probability that assumes the construction of a set of one-round characteristics. We also analyze the constructed set and give some examples of characteristics.

II. THE ARX-CIPHERS DIFFERENTIAL CRYPTANALYSIS

The main problem faced by developers of ARX-ciphers is a cipher's strength evaluation to differential [10] (linear) cryptanalysis. If we talk about "classical" block ciphers based on the wide trail strategy [11] like AES [12], Camellia [13], Kalyna etc., there is a known theoretical approach to evaluate strength of such ciphers to differential (linear) cryptanalysis. For most ARX-ciphers such a theory is absent because of their "naive" design. The exceptions are SPARX block cipher designed according to the long trail strategy and LAX block cipher [14]. These ciphers are designed so that to have provable bounds against differential and linear cryptanalysis. For the rest ARX-ciphers the approach to evaluating provable bound is absent.

Thus, the existing methods of ARX-ciphers' strength evaluation to differential cryptanalysis are heuristic ones and for r-round cipher reduce to an experimental search for the most probable (r-1)-round differential characteristics. As we know, differential properties of nonlinear transformation (namely, difference distribution tables) define cipher differential characteristics. Usually, for "classical" block ciphers such transformations are represented by byte-to-byte S-boxes, for which calculation of difference distribution tables is a simple task. In ARX-ciphers a nonlinear transformation is addition modulo 2^n, where n is usually equals to 32 or 64. To build a full difference distribution table (DDT) for 32- or 64-bit addition operation is infeasible. The problems devoted to ARX-ciphers differential cryptanalysis is also discussed in [15].

To overcome the mentioned problem, in [16] it was proposed to build a partial DDT which contains differentials with some predefined probability. By merging such partial tables for different operations, authors proposed to build a partial DDT for the whole round function. Then using modified Matsui method they build multi-round differential characteristics. This approach was successfully applied to block ciphers SPECK, TEA, XTEA etc.

To develop methods for searching for one-round differential characteristics for Cypress-256 presented in [8], we relied on results obtained in [16, 17]. Now we present our approach to multi-round differential characteristics search for Cypress-256. However, we do not follow the original version of the method presented in [16]: we do not build a partial DDT for the round function and do not use the modified Matsui method, but make calculations on the

978-1-5386-6611-1/18/$31.00 ©2018 IEEE

fly. This is due to the large input size to the round function and some particular qualities of the design [9, 15].

III. Cypress Block Cipher

Cypress block cipher is a lightweight block cipher based on Feistel network along with ARX round function. Cypress supports 256- and 512-bit blocks and keys, but the further analysis will concentrate around Cypress-256.

The detailed scheme of Cypress block cipher is presented in Fig 1 [8].

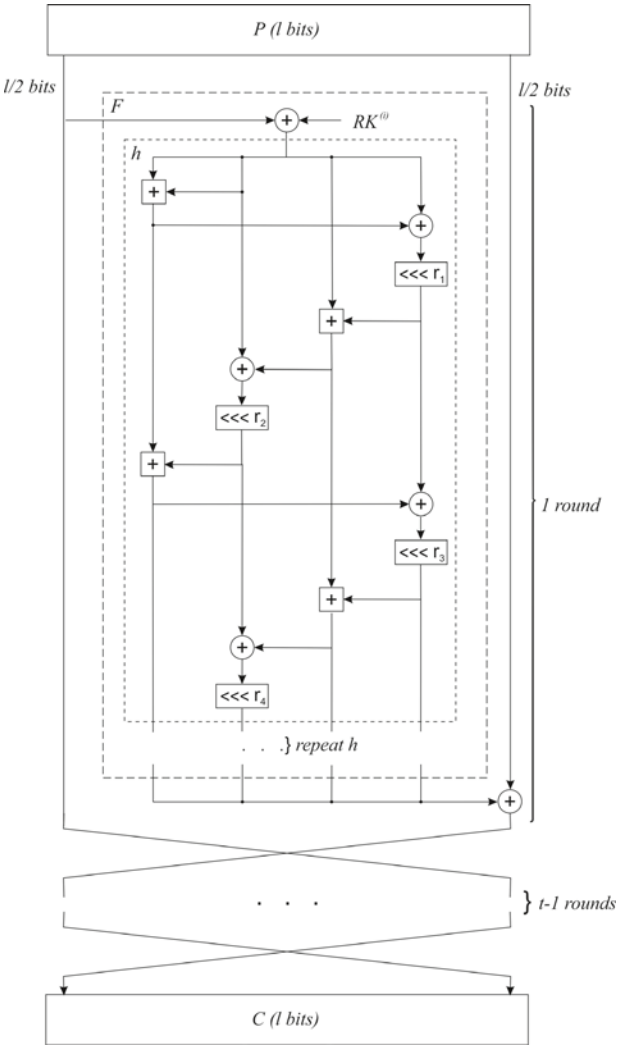

Fig. 1. Cypress block cipher

As can be seen from Fig.1, Cypress round function operates 4 words which pass through the chain of addition, rotation and XOR operations. In case of 256-bit version of the algorithm, the word length is 32 bits.

IV. The Cryptanalysis Model

Differential cryptanalysis operates pairs of input and output differences $(\Delta X, \Delta Y)$ calculated by operation which is used for subkeys insertion (usually, XOR).

The strength to differential cryptanalysis for r-round block cipher is estimated by probability of the best differential characteristic $P(\Delta Y(r-1))$ [18]. A cipher is considered to be resistant to differential attack if $\max P(\Delta Y(r-1)) < 2^{-n}$, where n – a key length [18].

As mentioned in [15], there is no provably secure approach to upper bound evaluation of differential characteristic probability for ARX-ciphers. Based on the up-to-date results [16, 17] devoted to the above problem, the estimation will carried out within the following model.

Let Cypress be an iterated block cipher with round function $Y = f(X, Z)$, where (X, Y) is a pair of plaintext and ciphertext and Z is a round key [18].

Let $\oplus$ be a bitwise operation that defines differences and $\boxplus$ be a modulo addition operation, for which difference propagation probability is less than 1. Then we introduce the following assumptions.

Assumption 1. The Cypress block cipher is a Markov cipher that means probability of r-round differential characteristic equals to product of probabilities of one-round characteristics [18].

Assumption 1 is followed from Cypress design (Feistel network with key addition at the beginning of each round).

Assumption 2. The probability of one-round differential characteristic equals to product of probabilities of differences propagation through modulo addition operation.

It is a usual assumption for ARX-ciphers that simplifies evaluation [16].

Assumption 3. When calculating an output difference after propagation through modulo addition operation, the output difference with the maximum probability is taken.

If for some input difference there are several outputs with the maximum probability, then differential trails for all variants is calculated. If the set of output differences with the maximum probability is too big to calculate all trails in reasonable time, then differential trails are calculated for a random sampling of differences.

Assumption 4. High-probable one-round differential characteristics have input differences with a minimum Hemming weight (≈1-7 active bits).

Assumption 4 follows from the fact that the most probable transitions in difference distribution table for modulo addition operation have a small Hemming weight.

V. Multi-Round Differential Characteristics

In [9] we proposed methods for searching for one-round differential characteristics with high probability for Cypress-256. Application of the proposed optimized method allowed finding the characteristic with probability 1/4. The next goal is to show that maximum probability of r-round differential characteristic $\max P(\Delta Y(r-1)) < 2^{-256.}$

For this purpose, firstly, we propose the method that consists from the following steps:

- Construct a big set of one-round characteristics and then check are there any characteristics that can be combined into at least two-round one. As long as Cypress-256 consists of 10 rounds, according to

Assumption 1 it will be good to include into this set one-round characteristics with probability $P_{thres}(\Delta Y(1)) \geq 2^{-26}$.

- Choose the input differences for building the set according to Assumption 4.
- Search for combinations of one-round differential characteristics from the set into at least two-round ones.

We note that for searching for one-round differential characteristics a partial DDT approach is not used. This is explained by the fact that due to the big number of additions in round function (8 additions) and large input to the round function (128 bits), the partial DDT should contain differential with enough small probability. It will lead to the huge size of the partial DDT, which calculation will take infeasible time.

Thus, we calculate a probability of difference propagation through the addition operation on the fly using the fast algorithm presented in [17]. Due to the fact that the smaller the probability, the bigger the number of transitions with maximum probability for addition operation, some random number of differentials can be chosen for each addition in order to minimize calculation time (random sampling).

Because of limitation of computational resources, for input differences with 1-4 active bits we found and added to the set all characteristics with $P_{thres}(\Delta Y(1)) \geq 2^{-26}$; for inputs with 5 active bits – with $P_{thres}(\Delta Y(1)) \geq 2^{-18}$ and for inputs with 6 active bits – with $P_{thres}(\Delta Y(1)) \geq 2^{-10}$. We did not search through input differences with more than 6 active bits because of very large number of possible variants, but we suppose it is enough to obtain reliable estimates.

Some statistic devoted to the obtained set is presented in Table 1.

TABLE I. STATISTIC ON ONE-ROUND DIFFERENTIAL CHARACTERISTICS

Input's Hemming Weight, bits	$P_{thres}(\Delta Y(1))$, $\log_2 n$	$\max P(\Delta Y(1))$, $\log_2 n$	Number of Trails
1	-26	> -26	0
2	-26	-14	2986
3	-26	-12	10357
4	-26	-6	28392
5	-18	-2	1446
6	-10	-3	343

As can be seen from the table, despite the fact that the most probable transitions in the difference distribution table for modulo addition have 1-3 active bits, the most probable characteristics were obtained for input differences with 4-6 active bits. This is due to the fact that before passing modulo addition, differences are also pass through linear operations which modifies bits' positions.

The most probable one-round characteristics are presented in Table 2. As can be seen from the table, outputs of the most probable characteristics also have small Hemming weight, but does it helps to build multi-round characteristics with high probability.

We combined one-round differential characteristics from the set into at least two-round ones, but no input and output did not coincide with each other. Despite output differences of one-round characteristics have a small Hemming weight, they cannot be further extended into high-probable characteristics. Because the combination of one-round characteristics did not reveal any match, the next step is to extend one-round characteristics into multi-round step by step. This point is under research now.

VI. CONCLUSIONS

In this work we introduce a cryptanalysis model for the lightweight block cipher Cypress that was recently developed in Ukraine. Then we propose a method for searching for multi-round differential characteristics for Cypress-256. The method includes the construction of a big set of one-round characteristics with further combination of them. Using this method, no match within the set was found. It is good for Cypress-256 from the point of view of its strength to differential cryptanalysis.

Also the analysis of constructed set revealed that inputs with the minimal Hemming weight are not always leads to high probable characteristics (especially, multi-round ones). Actually, the most popular characteristics with a high probability have inputs with 5-6 active bits. The goal of future research is the estimation of $\max P(\Delta Y(r-1))$.

REFERENCES

[1] R. Oliynykov *et al*., "A New Encryption Standard of Ukraine: The Kalyna Block Cipher," *IACR Cryptology ePrint Archive*, 2015, 650.

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

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

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

[5] I.D. Gorbenko, A.A. Zamula, and Ye.A. Semenko. "Ensemble and Correlation Properties of Cryptographic Signals for Telecommunication System and Network Applications", *Telecommunications and Radio Engineering*, vol. 75, No 2, pp.169-178, 2016.

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

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

[8] M.Yu. Rodinko and R.V. Oliynykov. "Postkvantovyy maloresursnyy blokovyy shyfr "Kyparys" [A post quantum lightweight blick cipher Cypress]," *Radiotekhnika*, issue 189, pp. 100-107, 2017. (in Ukrainian).

TABLE II. SOME MOST PROBABLE ONE-ROUND DIFFERENTIAL CHARACTERISTICS

Input difference, hex	Output difference, hex	$P(\Delta Y(1))$, $\log_2 n$
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 2000 20 20202000	2000 10000000 200000 200000	-8
0 4000 40 40404000	4000 20000000 400000 400000	-8
0 8000 80 80808000	8000 40000000 800000 800000	-8
180 80 80000080 8000	8 40040440 80800800 80000800	-8
80 80 80000180 8000	8 40040440 80800800 80000800	-8
100 80 80000000 808080	80 400000 8000 8000	-8
80001000 80000800 800 800	800000 40040040 80000800 80000000	-8
8000 8000 8180 800000	800 4044040 80080080 80080	-8
80000000 40000000 400000 40004040	40000000 2000 40 40	-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

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

[10] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystem", *Journal of Cryptology*, vol. 4, pp. 3-72, 1991.

[11] J. Daemen and V. Rijmen, "The wide trail design strategy," *IMA International Conference on Cryptography and Coding,* Springer, Berlin, Heidelberg, 2001, pp. 222-238.

[12] Pub, NIST FIPS. "197: Advanced encryption standard (AES)," *Federal information processing standards publication* 197.441: 0311, 2001.

[13] K. Aoki *et al*, "Camellia: A 128-bit block cipher suitable for multiple platforms—design andanalysis," *International Workshop on Selected Areas in Cryptography*, Springer, Berlin, Heidelberg, 2000, pp. 39-56.

[14] D. Dinu *et al,* "Design strategies for arx with provable bounds: Sparx and lax," *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Berlin, Heidelberg, 2016, pp. 484-513.

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

[16] A. Biryukov and V. Velichkov, "Automatic Search for Differential Trails in ARX Ciphers," *Cryptographers' Track at the RSA Conference,* Springer, Cham, 2014, pp. 227-250.

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

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