UDC 004.056.55
DOI: 10.15587/1729-4061.2017.108413

DEVELOPMENT OF THE APPROACH TO PROVING THE SECURITY OF BLOCK CIPHERS TO IMPOSSIBLE DIFFERENTIAL ATTACK

V. Ruzhentsev
Doctor of Technical Sciences, Associate Professor
Department of information technologies security
Kharkiv National University of Radio Electronics
Nauki ave., 14, Kharkiv, Ukraine, 61166
E-mail: viktor.ruzhentsev@nure.ua

Y. Onishchenko
PhD, Associate Professor
Department of cybersecurity
Kharkiv National University of Internal Affairs
L. Landau ave., 27, Kharkiv, Ukraine, 61080
E-mail: onischenko1980@gmail.com

Пропонується метод, який дозволяє обґрунтувати відсутність нездійснених диференціалів. Складність цього методу, на відміну від відомих, в меншій мірі залежить від розміру блоку. Метод застосовується до Rijndael-подібних SPN шифрів та фейстель-подібних шифрів. Обговорюються результати обчислювальних експериментів з пошуку нездійснених диференціалів для зменшених моделей блокових шифрів. Підтверджується справедливість висновків, отриманих за допомогою запропонованого методу обґрунтування відсутності нездійснених диференціалів

Ключові слова: блоковий шифр, атака нездійснених диференціалів, нездійснений диференціал, Rijndael-подібні перетворення

Предлагается метод, который позволяет обосновать отсутствие невыполнимых дифференциалов. Сложность метода, в отличие от известных, в меньшей степени зависит от размера блока. Метод применяется к Rijndael-подобным SPN шифрам и фейстель-подобным шифрам. Обсуждаются результаты вычислительных экспериментов по поиску невыполнимых дифференциалов для уменьшенных моделей блочных симметричных шифров. Подтверждается справедливость выводов, полученных с помощью предложенного метода обоснования отсутствия невыполнимых дифференциалов

Ключевые слова: блочный шифр, атака невыполнимых дифференциалов, невыполнимый дифференциал, Rijndael-подобные преобразования

1. Introduction

Using of secure data transfer protocols and cryptographic algorithms helps to protect against many threats to information security in the modern information world. One of the main requirements for symmetric cryptographic algorithms is the resistance to known cryptanalytical attacks.

The impossible differential attack (IDA) is one of the most powerful cryptanalytic attacks on many modern block symmetric ciphers (BSC). This cryptanalytic method allows attacking different kinds of block ciphers, including such common ones as SPN [1–3] and Feistel ciphers [4–7]. This attack is one of the most successful for the most popular in the world BSC Rijndael or AES (FIPS-197) with a reduced number of rounds. There are many other popular Rijndael-like SPN ciphers: the "Kalyna" cipher (DSTU 7624: 2014) with all block sizes, 512-bit block ciphers, which are used in the hash functions Whirlpool, Groestl and Kupyna (DSTU 7564: 2014).

The importance of the analysis of BSC resistance to IDA is confirmed by a number of works [1-11]. However, using of the methods proposed in these works would be problematic for 512- or 1024-bit block BSCs which are often used today, for example, in hash algorithms. This indicates the importance of finding ways to prove the resistance of BSC with large block sizes (more than 256 bits) to IDA.

2. Literature review and problem statement

The IDA was proposed at first for BSC SkipJack, IDEA, Khufu in [4, 5]. Then the IDA was applied to other BSCs. The IDA for BSC AES with 5 rounds was proposed in [1].

The IDA on BSCs belongs to the class of attacks on the round function. The adversary must have several plaint text-ciphertext pairs for the attack implementation.

The necessary condition of attack is the existence of impossible differentials (ID), which cover almost all rounds of BSC. An r-round ID is characterized by input difference Δ_{inID} and output difference Δ_{outID}. The transition of Δ_{inID} to Δ_{outID} through r rounds is impossible. If for BSC, there is an r-round ID, then the traditional scheme of IDA on the (r+1)-round BSC can be applied (Fig. 1).

The attack consists of the following main steps. The attacker is looking for a plaintext pair with input difference Δ_{in} and output difference Δ_{outID}. If such right pair is found, he knew that the difference Δ_{inID} cannot be after the first round (according to ID). Thus, all first-round keys K1, which lead to Δ_{inID} after the 1 round, are wrong. By rejecting all wrong keys, the right one can be determined.

The truncated or byte ID (BID) are used in attacks on many modern BSC [1-3]. Instead of the usual difference, the adversary considers the transition of activity patterns in this type of attack. Each bit of the activity pattern reflects the

© V. Ruzhentsev, Y. Onishchenko, 2017

activity of one byte in usual difference. The bit is 1 if the byte is active, and the bit is 0 if the byte has zero difference. The number of bits in the activity pattern is equal to the number of bytes in the cipher's block.

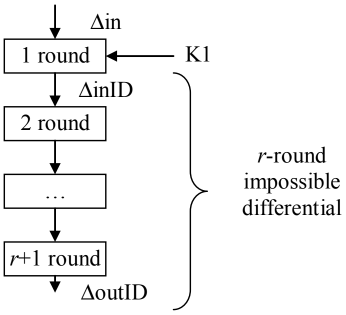

Fig. 1. The scheme of impossible differential attack

The advantage of using BID in IDA is that each found right pair allows rejecting not one or a few wrong first-round keys, but several hundred or thousands of wrong variants of the first-round key.

There are known ID for some most popular general BSC structures. The first example is the 5-round ID $(a, 0)\rightarrow(a, 0)$ for a Feistel cipher with the bijective round function [5], where a is some nonzero difference.

Another example is the 4-round BID for the Rijndael-128. The input difference of this BID has only one active byte and output difference has 4 passive bytes, which are in some column before the last round ShiftRows. This BID is used in many attacks [1–3].

There are a series of works about the ID of generalized Feistel networks [8,11].

The criteria of existence of ID for Rijndael-like BSC with a different number of rounds are presented in [10].

The resume is the following. If the BSC uses the structure with the known ID, then with a high probability there is almost the same ID for this BSC. But there are no guarantees that there is no ID with more rounds for this BSC. For example, the BSC Camellia is the Feistel cipher, so it has 5-round ID. But the 8-round ID were found during the more careful analysis of cipher in [7].

The universal approach to ID building was proposed in [5]. To build the ID, the attacker must find two reliable differentials (each has probability 1). The first one must cover the first n rounds, and another one – in the back way: the last m rounds. If there are such reliable differentials with different final differences, then the $(m+n)$-round ID is found.

Most of the known ID were built or can be built using this method. But there are no known proofs that ID cannot be built in another way, or that ID cannot cover more rounds than two reliable differentials.

The interesting way of ID search was proposed in [5]. The building of the scale model of BSC (with the reduced size of the block and key) is the first step. The exhaustive search of ID for this model is the second step. And transferring the search results from the scale model on original BSC is the last step.

The main disadvantage of this method is that the properties of original and reduced ciphers can be quite different. Therefore, the existence or absence of ID for the scale model cannot guarantee the same for the original BSC.

The algorithms for automatic BID search were proposed in [8, 9]. The algorithms are based on the miss-in-the-middle principle. The attacker tries to find two inconsistent reliable differentials. He uses the exhaustive search of input and output truncated differences (activity patterns) to make it.

The main disadvantage of the methods considered in this section is a significant complexity increasing with the growth of the block size and the number of rounds in BSC. As a result, known methods will not work for many ciphers that are used today in hash functions (block size of 512 or 1024 bits).

3. The aim and objectives of the study

The aim of this work is to develop an approach to proving the absence of ID or BID for ciphers with large block sizes (more than 256 bits).

To achieve this aim, it is necessary to solve the following tasks:

– to formulate a general rule when there are no IDs and BIDs for BSCs;

– to apply this rule to the most common types of BSC;

– to develop reduced models (with a block and key size of up to 16 bits) of the considered types of BSC;

– to check the validity of the theoretical conclusions about the absence of ID and BID for the developed reduced models.

4. The proposed approach to proving the IDs absence for BSCs

Unlike most known approaches [2–12], which were considered earlier and which are aimed at searching the IDs or BIDs, the developed approach will be aimed at proving the IDs absence. The main idea of the proposed approach is to prove the existence of some difference Δ in the intermediate stage of encryption, which can be obtained for any input difference when performing encryption and for any output difference when performing the decryption. Fig. 2 explains this idea.

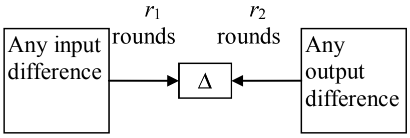

Fig. 2. The proposed approach to proving the ID absence

The proposed approach is based on the following theorem.

Theorem 1. If there is some difference Δ, which can be gained from any input difference in r_1 rounds and from any output difference in r_2 rounds (by going in the back way), then there are no IDs for this BSC with r_1+r_2 or more rounds.

Proof. If there is such intermediate difference Δ, which can be gained from any input and any output differences, then any input difference can be transformed to any output difference through this intermediate difference Δ. Thus, there are no IDs for BSC with r_1+r_2 or more rounds.

Thus, to prove the absence of ID, it is needed to determine the minimal number of rounds r_1 and r_2, then each input and each output difference can be transformed to the intermediate difference Δ.

In case of BID, the intermediate difference Δ usually would have all active bytes or the corresponding activity pattern would have only "1" bits. Theorem 1 can be reformulated as follows for BID.

Theorem 2. If there is some activity pattern Δ, which can be gained from any input activity pattern in r_1 rounds and from any output activity pattern in r_2 rounds (by going in the back way), then there are no BIDs for this BSC with r_1+r_2 or more rounds.

Theorem 2 can be used to estimate the security against IDA for many types of BSC. Rijndael-like SPN ciphers, Feistel ciphers will be considered in this work.

Scaled reduced models of considered BSC will be considered to verify the validity of the gained theoretical results. Scaled models of BSCs have 16-bit blocks and 16-bit keys. The algorithms for computing experiments on searching for ID and BID for reduced models of BSC are presented in Tables 1 and 2.

Table 1

Algorithm for ID searching

	Input data: 16-bit encryption procedure *E*. Empty row of the difference distribution table.
1	Exhaustive search of input difference *d*
1. 1	Reset the row of the difference distribution table
1. 2	Exhaustive search of key *k*
1. 2. 1	Exhaustive search of input value *x*
1. 2. 1. 1	Increment the cell with index $E_k(x)+E_k(x+d)$
1. 3	Check the row of the difference distribution table for zero cells. Each zero cell corresponds to ID
	Output data: Found IDs

Table 2

Algorithm for BID searching

	Input data: 16-bit encryption procedure *E*. Empty row of the difference distribution table.
1	Exhaustive search of input activity patterns
1. 1	Reset the row of the difference distribution table for the current activity pattern
1. 2	Exhaustive search of all input differences *d* corresponding to the activity pattern
1. 2. 1	Exhaustive search of key *k*
1. 2. 1. 1	Exhaustive search of input value *x*
1. 2. 1. 1. 1	Increment the cell with index $E_k(x)+E_k(x+d)$
1. 3	Exhaustive search of zero cells in the row of the difference distribution table
1. 4	Each zero cell corresponds to BID
	Output data: Found IDs.

In the algorithms presented in Table 1, 2, the actions performed inside the loop are indicated by an additional number (for example, the action with the number 1.2.1 will be performed in the loop, which is organized by the action with the number 1.2); E_k () – indicates the operation of encrypting using the key *k*.

4. 1. Scaled reduced models of BSC

The reason for considering scaled reduced models of BSC is that the full exhaustive search of ID or BID can be performed for BSC with a limited size of block and key. Our scaled models of BSC have 16-bit blocks and 16-bit keys. Almost all transformations for reduced models were taken from the known reduced model of cipher AES [13]. Fig. 3, 4 present the schemes of encryption procedure for scaled models of SPN and Feistel ciphers.

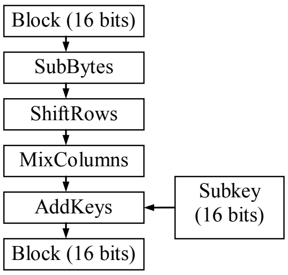

Fig. 3. The scheme of round for SPN ciphers

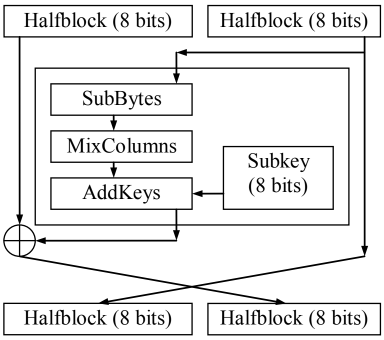

Fig. 4. The scheme of round for Feistel ciphers

The main features of the proposed reduced models of ciphers include:

- block size of 16 bits, key size of 8 or 16 bits;
- block structure for SPN BSC: 2 columns with two 4-bit elements in each;
- structure of a half-block for Feistel BSC: two 4-bit elements;
- multiplication by the 2-by-2 MDS matrix over GF (2^4) is used in the MixColumns transformation;
- substitution 4 to 4 bits is used in the SubBytes transformation;
- branch number of MixColumns transformation is 3.

5. Analysis of Rijndael-like SPN ciphers

By Rijndael-like ciphers with *n* columns and *m* rows in the block (state), we mean a cipher which consists of four main transformations of Rijndael in each round. These transformations are BS, SR, MC and AddKey. The first transformation BS (analogue of ByteSub in Rijndael) performs substitution for each byte of the state of the cipher. The second transformation SR (analogue of ShiftRow in Rijndael) performs the byte permutation in the state. The third transformation MC (analogue of MixColumn in Rijndael) performs the multiplication of each of *n* *m*-byte columns on a fixed MDS-matrix with the size of *m***m* bytes. The fourth transformation AddKey makes XOR-ing of round keys to the state.

The variants of Rijndael-like ciphers with *m*<=*n* were used in BSC Rijndael. The variants of Rijndael-like ciphers with $m>=n$ were used in BSC Kalyna [13]. The scheme of SR-transformation in this case is presented in Fig. 5.

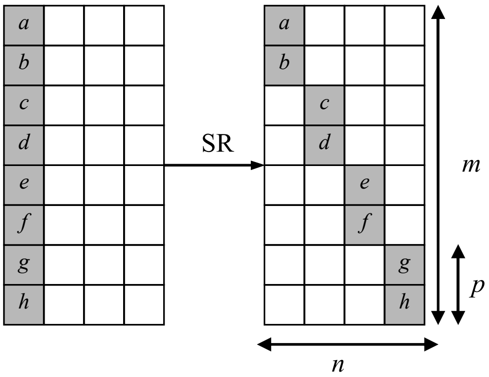

Fig. 5. The scheme of ShiftRows (SR) transformation

The BS and AddKey do not change the activity patterns. The SR change only the positions of active and passive bits in the activity patterns. The MC is the transformation which made the maximum influence on activity patterns. The rules of probability estimation for different size of MC were presented in [14]. Tables 3 and 4 give the probabilities for the activity patterns transformations when they pass through MC of Rijndael and MC of Kalyna, respectively.

Table 3

The probabilities of transformations of the activity patterns through MC of Rijndael, Log_2(Probability)

Output	0	1	2	3	4
Input					
0	0	–	–	–	–
1	–	–	–	–	0
2	–	–	–	–7.99	–0.023
3	–	–	–15.99	–8.017	–0.0226
4	–	–23.983	–16.0115	–8.0171	–0.0226

Table 4

The probabilities of transformations of the activity patterns through MC of Kalyna, Log_2(Probability)

Output	0	1	2	3	4	5	6	7	8
Input									
0	0	–	–	–	–	–	–	–	–
1	–	–	–	–	–	–	–	–	0
2	–	–	–	–	–	–	–	–7.99	–0.046
3	–	–	–	–	–	–	–15.9	–8.04	–0.045
4	–	–	–	–	–	–23.9	–16.0	–8.04	–0.045
5	–	–	–	–	–31.9	–24.0	–16.0	–8.04	–0.045
6	–	–	–	–39.9	–32.0	–24.0	–16.0	–8.04	–0.045
7	–	–	–47.9	–40.0	–32.0	–24.0	–16.0	–8.04	–0.045
8	–	–55.9	–48.0	–40.0	–32.0	–24.0	–16.0	–8.04	–0.045

In Table 3, 4, the number of active bytes at the input of MC is changed by columns and the number of active bytes at the output is changed by rows. Zero probability of the activity pattern's transformation corresponds to symbol "–" in Table 3 and 4. It is important for the further research that any non-zero input difference always can be transformed into the all-active bytes output difference.

Now statement 1 about the absence of IDs for Rijndael-like ciphers can be proved.

Statement 1. There are no BIDs for Rijndael-like BSC with 4 or more full rounds and with the block, which has more rows than columns (the necessary condition is that during ShiftRows-transformation each output column gets at least 1 byte from each input column).

Proof. To prove the statement, we must prove that intermediate difference with all active bytes can be gained from any input difference after the 2-round enciphering and from any output difference after the 2-round deciphering. The conditions of statement 1 will be fulfilled in this case.

The 2-round enciphering contains the sequence of transformations: MC, SR, MC. The 2-round deciphering contains the same sequence of reverse transformations: MC^{-1}, SR^{-1}, MC^{-1}. Each of these two sequences can make all-active bytes difference from any input difference.

Consider the sequence MC, SR, MC. Each non-zero input difference has at least 1 active column. According to Tables 1 and 2, we always can get the difference with all active bytes in this column after the first MC transformation. The following operation SR distributes the active bytes to all over the columns and makes all columns active. So, the last MC always can make the difference with all active bytes. The same arguments work for the sequence of reverse transformations. Thus, according with theorem $2r1+r2=2+2=4$. The statement is proved.

This result completely agrees with the known results, because the longest known ID for 128-bit Rijndael covers 3 full and 1 reduced rounds [3].

In cases when the condition of statement 1 about the number of rows and columns in the block is not true ($m<n$) (for example, Rijndael with block 192 or 256 bits), $r1$ and $r2$ must be increased by at least one round each. Thus, the absence of IDs can be proved for 6 or more rounds.

Using the algorithms from Tables 1, 2, the search of ID and BID for scaled reduced models of AES was performed. The results are shown in Tables 5, 6.

Table 5

Results of ID search for scaled reduced models of AES

Number of rounds	Number of found ID	Comments
4	510	For each input difference with only one active S-box
5	0	–

Table 6

Results of BID search for scaled reduced models of AES

Number of rounds	Number of found BID	Comments
4 reduced (without MC in the last round)	24	6 BIDs for each activs ity pattern with only one active S-box
4	0	–

5. 1. Discussion of the results for Rijndael-like ciphers

The results of the computational experiments from Table 6 confirm the validity of the previously proved statement 1.

The results from Table 5 show that conventional IDs can cover more rounds of BSC than BID. For example, in case of

4 complete rounds of a reduced AES, no BID was found, but several IDs. The input difference of the detected IDs can be described by the activity pattern with only one active bit, but the output difference cannot be described by the activity pattern, because the values in each of the active bytes of difference are important. Similar 4-round IDs were found and for original full-size AES, but information about these IDs in the available literature was not found. Perhaps using of these IDs can make known IDA on AES more efficient. However, this issue requires additional research.

BSC Kalyna (DSTU 7624:2014) with all block sizes, 512-bit BSCs used in hash algorithms Whirlpool, Groestl and Kupyna (DSTU 7564:2014) meet the conditions of statement 1, thus, there is no BID for these ciphers with 4 or more rounds.

6. Analysis of Feistel ciphers with optimal diffusion

Feistel network is one of the most popular schemes of modern ciphers. But it is known that potentially one round of the SPN scheme provides better diffusion than one round of the Feistel scheme. Thus, it seems a good idea to use the optimal (maximal) diffusion in the round function of the Feistel scheme. Such construction was used, for example, in BSC Tornado [15] and Labyrinth [16]. The scheme of the round function for such cipher is presented in Fig. 6.

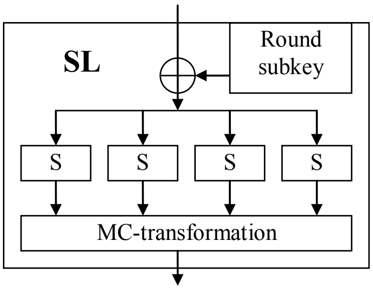

Fig. 6. SL-transformation

The important thing is that the whole half-block is used as one column during the MC-transformation. Thus, the linear transformation provides a maximal (optimal) diffusion. It is important for the further research that any non-zero input activity pattern always can be transformed into the all-active bits output activity pattern (Table 3, 4).

The scheme of the 3-round enciphering procedure and a variant of the activity pattern's transformation are presented in Fig. 7.

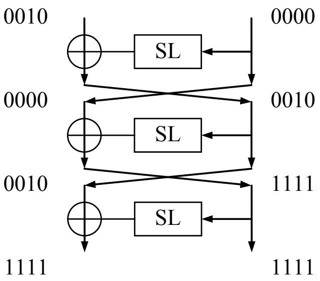

Fig. 7. The scheme of the 3-round transformation and a variant of the activity pattern's transformation

Theorem 2 allows proving the following statement for such BSC.

Statement 2. There are no BIDs for the 6- or more-round Feistel BSC with the Rijndael-like round function and MixColumns-transformation which cover the whole half-block.

Proof. To prove the statement, we must prove that the intermediate difference with all active bytes can be gained from any input difference after the 3-round enciphering and from any output difference after the 3-round deciphering.

The simple passage of zero-difference to zero-difference can be used in the first round (Fig. 7).

We shall call such 1-round zero to zero passage of the difference as trivial round. Other variants of the 1-st round can make the possibility of getting the all-active bytes difference even faster than 3 rounds.

There is at least 1 active byte in the left half of the input difference. In any case, some non-zero difference will be at the input of the 2-round function. According to Tables 3 and 4, the difference at the output of the 2-round function can have all active bytes. So, after the 2-nd round we always can get the all-active bytes difference in the right half-block and, in case of the trivial 1-st round, the left half of the input difference in the left half-block (Fig. 7).

The all-active bytes input to the 3-round function can be transformed (Tables 3 and 4) to the all-active bytes output. Thus, we'll get the all-active bytes difference after the 3-rd round.

Using the same arguments, we can show that three deciphering rounds also can transform any difference to the all-active bytes intermediate difference. Thus, according with theorem $2r1+r2=3+3=6$. The statement is proved.

As in the previous part of the work, the search of ID and BID with using the algorithms from Tables 1 and 2 for scaled reduced models of the considered Feistel cipher was performed. The results are shown in Table 7, 8.

Table 7

Results of ID search for scaled reduced models of Feistel ciphers

Number of rounds	Number of found ID	Comments
7 (S-block max_dif=10)	12	Example: 0x0100-0x0001
7 (S-block max_dif=4)	8	Example: 0x0100-0x0001
8	0	–

Table 8

Results of BID search for scaled reduced models of Feistel ciphers

Number of rounds	Number of found BID	Comments
5	4	Two BIDs for each of the activie ty patterns 1000 and 0100
6	0	–

6. 1. Discussion of the results for Feistel BSC

The results from Table 8 confirm the validity of statement 2.

Computational experiments on ID search were performed for reduced models of Feistel ciphers with different parameters of substitutions. The maximum value in the difference distribution table was used as the variable parameter. This value is indicated in the first column in Table 7. In the first case (the first row of Table 7), the maximum value in the difference table for substitution 4 to 4 bits is 10 (S-block max_dif=10), and in the second case (the second row of Table 7), the value is 4 (S-block max_dif=4). The presented results show that the differential properties of nonlinear substitutions do not have an essential influence on the resistance of the BSC to the IDA. At the same time, it is quite expected that the higher maximum value in the difference table leads to a greater amount of IDs.

As in case of SPN ciphers, the results of computational experiments show that the absence of BID does not mean the absence of ID for the Feistel cipher. Unlike SPN ciphers, where the difference in the required amount of rounds for the absence of BID and ID was 1 (Tables 5 and 6), in case of Feistel ciphers this difference is 2 rounds.

BSCs Tornado and Labyrinth with a block size of 128 bits meet the conditions of statement 2, thus, there is no BID for these ciphers with 6 or more rounds.

7. Conclusions

1. Theorems about the absence of impossible differentials (ID) (Theorem 1) and the absence of byte impossible differentials (BID) (Theorem 2) are formulated and proved for block symmetric ciphers (BSC) in general. These theorems can be used to prove the ID and BID absence for some types of BSC even with large block sizes (256 and more bits).

2. Two common types of BSCs are analyzed: Rijndael-like SPN ciphers and Feistel ciphers. Statement 1 about the absence of BID for the Rijndael-like ciphers with 4 or more rounds was proved. Statement 2 about the absence of BID for Feistel ciphers with optimal diffusion and with 6 or more rounds was proved. Statement 1 allowed proving the absence of BIDs for the following BSCs with 4 or more rounds: for Kalyna (DSTU 7624: 2014) with all block sizes; for 512-bit block ciphers that are used in the hash functions Whirlpool, Groestl and Kupyna (DSTU 7564: 2014). Statement 2 made possible proving the absence of BIDs for 6 or more rounds of Tornado and Labyrinth ciphers with a block size of 128 bits.

3. The scaled reduced 16-bit encryption transformations for Rijndael-like SPN and Feistel ciphers were implemented. Computational experiments on the ID and BID search for these reduced models confirmed the validity of the theoretical conclusions obtained using statements 1 and 2. It is shown that the absence of BID does not mean the ID absence. For the considered reduced SPN and Feistel ciphers, IDs cover, respectively, 1 and 2 rounds more than BIDs. Thus, one of the possible directions of future research is the study of using of the found IDs in attacks on the BSCs.

References

1. Biham, E. Cryptanalysis of Reduced Variant of Rijndael [Text] / E. Biham, N. Keller // The Third Advanced Encryption Standard Candidate Conference. – New York, 2000.
2. Cheon, J. H. Improved Impossible Differential Cryptanalysis of Rijndael and Crypton [Text] / J. H. Cheon, M. Kim, K. Kim, L. Jung-Yeun, S. Kang // Lecture Notes in Computer Science. – 2002. – P. 39–49. doi: 10.1007/3-540-45861-1_4
3. Lu, J. New Impossible Differential Attacks on AES [Text] / J. Lu, O. Dunkelman, N. Keller, J. Kim // Lecture Notes in Computer Science. – 2008. – P. 279–293. doi: 10.1007/978-3-540-89754-5_22
4. Biham, E. Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials [Text] / E. Biham, A. Biryukov, A. Shamir // Technion, CS Dept, Tech Report CS0947. – 1998.
5. Biham, E. Miss in the Middle Attacks on IDEA and Khufu [Text] / E. Biham, A. Biryukov, A. Shamir // Lecture Notes in Computer Science. – 1999. – P. 124–138. doi: 10.1007/3-540-48519-8_10
6. Lu, J. Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1 [Text] / J. Lu, J. Kim, N. Keller, O. Dunkelman // Lecture Notes in Computer Science. – 2008. – P. 370–386. doi: 10.1007/978-3-540-79263-5_24
7. Wu, W.-L. Impossible Differential Cryptanalysis of Reduced-Round ARIA and Camellia [Text] / W.-L. Wu, W.-T. Zhang, D.-G. Feng // Journal of Computer Science and Technology. – 2007. – Vol. 22, Issue 3. – P. 449–456. doi: 10.1007/s11390-007-9056-0
8. Kim, J. Impossible Differential Cryptanalysis for Block Cipher Structures [Text] / J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, S. Sung // Lecture Notes in Computer Science. – 2003. – P. 82–96. doi: 10.1007/978-3-540-24582-7_6
9. Luo, Y. A Unified Method for Finding Impossible Differentials of Block Cipher Structures [Text] / Y. Luo, Z. Wu, X. Lai, G. Gong // IACR Cryptology ePrint Archive. – 2009.
10. Li, R. Impossible Differential Cryptanalysis of SPN Ciphers [Text] / R. Li, B. Sun, C. Li // IACR Cryptology ePrint Archive. – 2010.
11. Yap, H. Impossible Differential Characteristics of Extended Feistel Networks with Provable Security against Differential Cryptanalysis [Text] / H. Yap // Communications in Computer and Information Science. – 2009. – P. 103–121. doi: 10.1007/978-3-642-10240-0_9
12. Daemen, J. AES proposal: Rijndael [Text] / J. Daemen, V. Rijmen // First Advanced Encryption Standard (AES) Conference. – Ventura, CA, 1998.
13. Gorbenko, I. D. The perspective block symmetrical cipher “Kalyna” – a main positions and specification [Text] / I. D. Gorbenko, V. I. Dolgov, R. V. Oliynykov, V. I. Ruzhentsev et. al. // Applied radioelektroniks. – 2007. – Vol. 6, Issue 2. – P. 195–208.
14. Ruzhentsev, V. I. About method of the security estimation to truncated differential attack [Text] / V. I. Ruzhentsev // Radioelectroniks and informatics. – 2003. – Issue 4. – P. 130–133.
15. Gorbenko, I. D. The Algorithm of the block symmetrical enciphering “Tornado”. The specification of the transformation [Text] / I. D. Gorbenko, S. A. Golovashich // Radiotechnics. – 2003. – Issue 134. – P. 60–80.
16. Golovashich, S. A. Specification of the algorithm of the block symmetrical enciphering “Labyrinth” [Text] / S. A. Golovashich // Applied Radioelectroniks. – 2007. – Vol. 6, Issue 2. – P. 230–240.