UDC 004.056.55:512.6+519.688

Differential Attack on IDEA Block Cipher Based on Its Key-Adding Function

Oleksandr Parshyn[1], Mykola Khmelnytskyi[1]

[1]*National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology*

Abstract

This paper examines a new theoretical differential attack on the IDEA block cipher and several related ciphers from the same design family, such as PES and MESH. We present an analysis of the most probable differentials, which characterise the ciphers' security against the proposed attack. We also propose a design modification targeting the cipher's key-adding function to enhance its security against the attack.

Keywords: symmetric cryptography, block cipher, Lai-Massey scheme, IDEA, differential cryptanalysis

Introduction

One of the most famous ciphers based on the Lai-Massey scheme is IDEA (International Data Encryption Algorithm), which was proposed by X. Lai and J. Massey in 1991 [1]. It is a word-oriented, iterative block cipher that operates on 64-bit blocks, which are divided into 16-bit subwords. The family of IDEA-based ciphers later expanded with the creation of the following block ciphers: FOX [2], which incorporated 8-bit S-boxes and MDS codes; MESH [3], which allowed the block size of IDEA to be enlarged beyond 64 bits; R-IDEA [4], which proposed changing the multiplication-addition box (MA-box) of the original IDEA to improve the non-linearity of the transformation, as well as some others.

Several methods of differential cryptanalysis were developed for IDEA, resulting in successful attacks on reduced numbers of rounds. These methods include standard differential cryptanalysis based on weak-key assumptions [5]; truncated differential cryptanalysis [6]; impossible differential cryptanalysis [7]; slide attacks [8]; and boomerang attacks [9]. J. Hakahara-jr. provides a detailed description of these methods in [8].

As differential cryptoanalysis is the most developed method of cryptoanalysis for block ciphers from the IDEA family, most attacks are based on weak-key assumptions. These assume that some subkeys have a value of 0 or 1. In other words, their fifteen most significant bits are zero. Under these assumptions, attacks can be launched against the full 8.5-round IDEA [10], as well as against MESH [3], R-IDEA [8] and other ciphers from this family. It has been demonstrated that IDEA contains a large number of weak keys (almost 2^{35} out of all possible keys) and enables the identification of cyclic differential characteristics that are certain to pass through the encryption rounds.

The mentioned attacks are built using differential characteristics with XOR as the difference operator. However, IDEA is not a Markov cipher under this difference operator. The authors of IDEA presented a cryptoanalysis of mini versions of IDEA based on modular multiplication [5]. In this paper, we wish to further utilize the concept of non-XOR key-adding operators.

This paper presents a new attack on the IDEA block cipher based on its key-adding function. This attack can be applied to all block ciphers in the IDEA family. We provide the highest probabilities for the differentials, which characterize the complexity of the proposed attack. We also propose a modification to IDEA's key-adding function to improve its security against the aforementioned attack.

The results obtained were partially presented at the 2nd Theoretical and Applied Cybersecurity

(TACS-2024) Scientific and Practical Conference, held in Kyiv, Ukraine on 30 May 2024.

The rest of this paper is organized as follows. Section 1 recalls the main design features and structural elements of the Lai-Massey scheme. Section 2 provides an overview of the IDEA block cipher structure (key schedule, encryption and decryption algorithms). Section 3 provides details of a differential attack on IDEA, along with the corresponding differences for the PES and MESH block ciphers. Section 4 introduces a new modification to the IDEA block cipher's key-addition function to increase its security with regard to the proposed attack.

Preliminaries

Let $V_n = \{0,1\}^n$ be a binary vector space.

Any vector X in V_n, $X = (x_{n-1}, \dots, x_0)$ can be considered a natural representation of an integer:

$$X = x_{n-1}2^{n-1} + \cdots + x_1 2 + x_0.$$

From this representation we can also denote the vector $(0,0,\dots,0)$ as the number 0 and the vector $(1,1,\dots,1)$ (which corresponds to the number $2^n - 1$) as the number -1.

We will also consider the following algebraic operations, as these are the only ones used in the IDEA block cipher family:

1) $\boxplus$ – addition modulo 2^n;
2) $\boxminus$ – subtraction modulo 2^n;
3) $\odot$ – multiplication modulo $2^n + 1$, where 0 (zero vector) denotes a number 2^n;
4) $\oslash$ – division modulo $2^n + 1$ (inverse operation for $\odot$);
5) $\oplus$ – bitwise addition (logical operator XOR).

We emphasize a general-known fact that

$$\overline{x} = x \oplus (-1) \equiv (-1 - x) \bmod 2^n.$$

The symbol $\overline{\sum\limits_x}$ denotes an average sum $\frac{1}{2^n}\sum\limits_x$, where $x \in \mathbb{Z}_{2^n}$.

We will also require the definitions of differential probabilities and differentials, as these are central to the differential cryptanalysis of block ciphers. *Differential $(\alpha \to \beta)$ of boolean function f w.r.t operation $\circ$* is an arbitrary pair of vectors $\alpha, \beta \in V_n$. For each differential, we identify an event $f(x \circ \alpha) \circ (f(x))^{-1} = \beta$, where x is selected randomly from V_n and z^{-1} denotes the inverse of z w.r.t operation $\circ$.

The probability of the differential (α, β) w.r.t operation $\circ$ is the value:

$$DP^f_\circ(\alpha \to \beta) = \overline{\sum_x}[f(x \circ \alpha) \circ (f(x))^{-1} = \beta],$$

where $[.]$ denotes Iverson's bracket (the indicator function).

For binary operation $\boxtimes$: $V_n \times V_n \to V_n$ the definitions change slightly: the differential becomes a triple of vectors $(\alpha, \beta \to \gamma)$, and the probability of differential becomes

$$DP^{\boxtimes}_\circ(\alpha, \beta \to \gamma) = \\ = \overline{\sum_{x,y}}[(x \circ \alpha) \boxtimes (y \circ \beta) = (x \boxtimes y) \circ \gamma].$$

The algebraic properties of non-XOR differentials have been studied in [11, 12].

1. Lai-Massey Scheme Design and the IDEA Family of Block Ciphers

The design of Lai-Massey ciphers is distinct from that of Feistel Network ciphers, such as DES, and Substitution-Permutation Network (SPN) ciphers, such as AES. Lai-Massey ciphers have unique features, such as:

- complete text diffusion in a single round;
- a rather strong round function with a small number of rounds;
- usage of only three group operations as building blocks, such as bitwise exclusive-or, modular addition and modular multiplication (in a finite field);
- absence of S-boxes or MDS codes.

In the Lai-Massey scheme, encryption is an iterative function, where each iteration takes the form of the following transformation:

$$LM(x,y) = (x + F(x-y),\ y + F(x-y)).$$

Here $F(x,y)$ is a round function, defined for each block cipher separately, as are the adding functions $+, -$, which depend on the algebraic group, built on the vector space V_n of the text entries.

However, it has one problematic property: if $LM(x,y) = (z,t)$ then

$$z - t = x - y.$$

This symmetry significantly decreases the security of Lai-Massey ciphers schemes for common

cryptanalysis methods, so two approaches have been proposed before to eliminate it:

1) use a key-adding function with different algebraic operations, which destroys XOR-differentials between rounds. This approach was utilized in all ciphers from IDEA family;

2) use orthomorphic transformation σ:

$$LM'(x,y) = (\sigma(x + F(x-y)),\ y + F(x-y)),$$

which disrupts the aforementioned internal symmetry [13].

This paper will focus on the first approach, since all block ciphers in the IDEA family are based on it.

2. The Structure of IDEA Block Cipher

Let us begin with the IDEA key schedule of IDEA [14]. It transforms a 128-bit user key K into 52 16-bit subkeys for either the encryption or the decryption processes. In total, 832 bits of subkey material are required across 8.5 rounds.

These are obtained as follows:

1) the 128-bit user key K is stored in a register, which is initially partitioned into eight 16-bit words. These words become the first eight subkeys: $Z_1^{(1)}, Z_1^{(2)}, Z_1^{(3)}, Z_1^{(4)}, Z_1^{(5)}, Z_1^{(6)}, Z_2^{(1)}, Z_2^{(2)}$;
2) the register is then left rotated by 25 bits and is partitioned into eight 16-bit words, which become the next eight round subkeys. The next pack of subkeys will be $Z_2^{(3)}, Z_2^{(4)}, Z_2^{(5)}, Z_2^{(6)}, Z_3^{(1)}, Z_3^{(2)}, Z_3^{(3)}, Z_3^{(4)}$ — and so on;
3) the previous step is repeated until 52 subkeys are obtained.

Next comes the encryption phase, as shown on Fig.1.

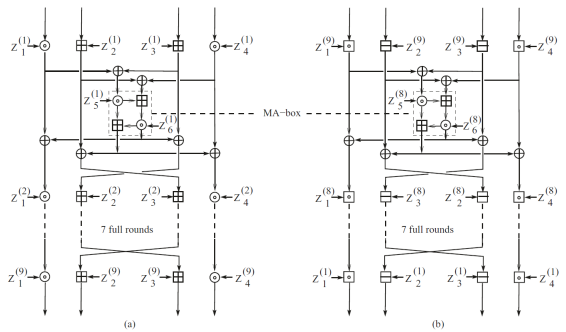

Figure 1: Computational graph of the IDEA cipher: (a) encryption and (b) decryption

Let $X^{(i)} = (X_1^{(i)}, X_2^{(i)}, X_3^{(i)}, X_4^{(i)})$ be the input word of the i-th round, where $X_j^{(i)} \in \mathbb{Z}_2^{16}, 1 \le j \le 4$. Here $X^{(1)}$ is the open text.

One round of encryption can be divided into three stages: a key-addition function, a multiplication-addition box (MA), and an output block.

The key-adding function looks like this:

$$Y^{(i)} = (X_1^{(i)} \odot Z_1^{(i)}, X_2^{(i)} \boxplus Z_2^{(i)}, X_3^{(i)} \boxplus Z_3^{(i)}, X_4^{(i)} \odot Z_4^{(i)}).$$

The result of key-adding function is a pair of values $(n_i, q_i) = (Y_1^{(i)} \oplus Y_3^{(i)}, Y_2^{(i)} \oplus Y_4^{(i)})$, which is sent to MA-box.

Result of MA-box is a pair (r_i, s_i):

$$s_i = ((Z_5^{(i)} \odot n_i) \boxplus q_i) \odot Z_6^{(i)},$$
$$r_i = s_i \boxplus (Z_5^{(i)} \odot n_i).$$

The output block combines the result of the multiplication and addition block and rearranges the words as follows:

$$X^{(i+1)} =$$
$$= (Y_1^{(i)} \oplus s_i, Y_3^{(i)} \oplus s_i, Y_2^{(i)} \oplus r_i, Y_4^{(i)} \oplus r_i).$$

$X^{(i+1)}$ is the input block for the next encryption round. This procedure is repeated eight times.

After the final round, the modified final transformation is applied:

$$X^{(9)} = (Y_1^{(8)} \oplus s_8, Y_2^{(8)} \oplus r_8, Y_3^{(8)} \oplus s_8, Y_4^{(8)} \oplus r_8).$$

The final ciphertext is acquired as follows:

$$C = (X_1^{(9)} \odot Z_1^{(9)},\ X_2^{(9)} \boxplus Z_2^{(9)},$$
$$X_3^{(9)} \boxplus Z_3^{(9)}, X_4^{(9)} \odot Z_4^{(9)}).$$

We will also illustrate the similarities in the key-adding functions and MA-boxes of the PES and MESH-64 block ciphers using computational graphs (see Fig. 2, 3). They share the same design structure, consisting of a key-adding function and an MA-box, with the result XOR'ed. The differences lie in the operations used in the key-adding function and the MA-box itself.

Note that the same parts of the results of the key-adding functions are being XOR-ed in all these block ciphers:

$$(n_i, q_i) = (Y_1^{(i)} \oplus Y_3^{(i)}, Y_2^{(i)} \oplus Y_4^{(i)}), \quad (1)$$

even though $Y^{(i)}$ are different by design. This is the basic of the proposed attack.

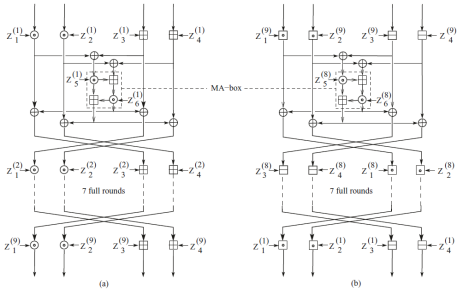

Figure 2: Computational graph of the PES cipher: (a) encryption and (b) decryption

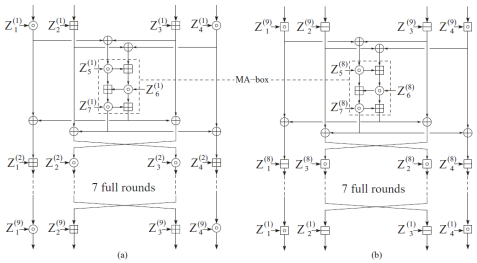

Figure 3: Computational graph of the MESH-64 cipher: (a) encryption and (b) decryption

3. Attack on IDEA Block Cipher Based on Key-Adding Function

Our attack on IDEA is based on the following observation: consider differentials in the form $(\alpha, \beta, \alpha, \beta)$. These differentials transform to $(0, 0)$ on the input of MA-box according to (1), so the output of MA-box gives also $(0, 0)$, regardless of the round subkeys. This result is XORed back with each part of the round message, resulting in the same differential, which is then propagated further. Therefore, the only structural element that introduces changes during the round is the key-adding function.

Our attention will be drawn to the two messages whose bitwise difference is (α, α, α, α). As will be demonstrated later, these differences result in higher probability differentials, so our subsequent research will focus solely on differentials of this form. As mentioned previously, they pass through the MA-box unchanged; therefore, we can only consider the probability of the difference being preserved when passing through the key-adding function without change:

$$\mathbb{P}_1(\alpha) = DP^{\boxplus}_{\oplus}(\alpha, 0 \to \alpha),$$
$$\mathbb{P}_2(\alpha) = DP^{\odot}_{\oplus}(\alpha, 0 \to \alpha),$$
$$\mathbb{P}(\alpha) = \mathbb{P}_1^2(\alpha) \cdot \mathbb{P}_2^2(\alpha).$$

The probability $\mathbb{P}$ characterizes the complexity of a differential attack on the IDEA cipher for one round of encryption.

Similar attacks based on the same principle can be performed not only on the IDEA cipher, but also on the PES (IDEA's predecessor) and the MESH-64, MESH-96 and MESH-128 ciphers, since they have a similar structure and also ensure the stability of the Lay-Massey scheme using a key-addition function. [3]

The attack on the PES and MESH-64 ciphers is carried out in exactly the same way as the attack on the IDEA cipher. Given the same structures of the key-addition function and the operations involved, all the differential strength estimates will also be the same.

The MESH-96 and MESH-128 ciphers use three and four parallel Lay-Massey schemes, respectively, as opposed to two schemes in the PES, IDEA and MESH-64 ciphers. However, the operations used in the key-addition function and the method of combining the results remain the same:

$$\mathbb{P}_{MESH96} = \mathbb{P}_1^3 \cdot \mathbb{P}_2^3;$$
$$\mathbb{P}_{MESH128} = \mathbb{P}_1^4 \cdot \mathbb{P}_2^4.$$

The probabilities, $\mathbb{P}_1$ and $\mathbb{P}_2$, were obtained through an extensive search of all possible differences α. Highest probabilities are shown in the table 1. It can be seen that such attacks are possible for no more than two rounds of encryption. For 64-bit secure text blocks, we expect differential probabilities to approach 2^{-64}, and the proposed attack achieves this with two rounds of encryption.

Table 1
Probabilities of differentials with the highest probability of attack

α_{hex}	$\mathbb{P}_1(\alpha)$	$\mathbb{P}_2(\alpha)$	$\log(\mathbb{P}(\alpha))$
8080	0.5	0.000045	-30.880
8888	0.125	0.000124	-31.956
FFFD	0.000061	0.25	-31.998
8000	1	0.000015	-32.049
8001	0.5	0.000025	-32.577
8008	0.5	0.000025	-32.577
8010	0.5	0.000025	-32.577
8020	0.5	0.000025	-32.577
8040	0.5	0.000025	-32.577
8100	0.5	0.000025	-32.577

4. Modifications to the Key-Adding Function

In this section, we propose an alternative operation that could enhance the security of the IDEA block cipher, as well as block ciphers based on the Lai-Massey scheme, against the proposed attack and other forms of differential cryptanalysis.

Consider the following operation:

$$f(x,y) = x \otimes y = (x+1)\cdot(y+1) - 1, \quad (2)$$

where operation $\cdot$ represents usual multiplication modulo $2^{16}+1$. Considering:

$$x,\ y \in \{0,\dots,2^n-1\},$$
$$x+1,\ y+1 \in \{1,\dots,2^n\} = \mathbb{Z}^*_{2^{16}},$$
$$(x+1)\cdot(y+1) \in \{1,\dots,2^n\},$$

then, respectively:

$$x \otimes y \in \{0,\dots,2^n-1\},$$

so this operation, unlike modular multiplication in the original IDEA cipher, is performed on naturally represented numbers by binary vectors without additional refinements. In particular, the neutral element w.r.t. the operation $\otimes$ is zero vector 0, as in bitwise or modular addition. However, the introduced operation is slightly more computationally complex.

Differentials $DP^{\otimes}_{\oplus}$ under the $\oplus$ operation possess the following properties.

Lemma 1. *For every $n \in \mathbb{N}$ it holds*

$$DP^{\otimes}_{\oplus}(-\mathbf{1}, -\mathbf{1} \to 0) = 1.$$

Proof. By definition we have

$$DP^{\otimes}_{\oplus}(-\mathbf{1}, -\mathbf{1} \to 0) =$$
$$= \overline{\sum_{x,y}} [f(x\oplus(-\mathbf{1}), y\oplus(-\mathbf{1})) \oplus f(x,y) = 0].$$

Here $f(x,y) = (x+1)\cdot(y+1)-1 = x\cdot y + x + y$. Meanwhile,

$$f(x\oplus(-\mathbf{1}), y\oplus(-\mathbf{1})) =$$
$$= (x\oplus(-\mathbf{1})+1)\cdot(y\oplus(-\mathbf{1})+1) - 1.$$

Here equation $x\oplus(-\mathbf{1}) = -\mathbf{1} - x$ holds as this operation means invertion of all bits of a number. Also $(2^n - x) \bmod 2^n = (2^n - x) \bmod (2^n+1)$, because $x \in [0, 2^n-1]$; thus,

$$f(x\oplus(-\mathbf{1}), y\oplus(-\mathbf{1})) = (2^n - x)\cdot(2^n - y) - 1 =$$
$$= 2^{2n} - x\cdot 2^n - y\cdot 2^n + x\cdot y - 1.$$

Considering each element, we obtain

$$2^{2n} \equiv (-1)^2 \bmod (2^n+1) \equiv 1 \bmod (2^n+1);$$
$$-x\cdot 2^n \equiv x \bmod (2^n+1);$$
$$-y\cdot 2^n \equiv y \bmod (2^n+1).$$

Then it follows that

$$f(x\oplus(-\mathbf{1}), y\oplus(-\mathbf{1})) = f(x,y),$$

and $\overline{\sum_{x,y}} [f(x,y)\oplus f(x,y) = 0] = 1$, which concludes the proof. □

Lemma 2. *For every $n \in \mathbb{N}$ it holds*

$$DP^{\otimes}_{\oplus}(0, -\mathbf{1} \to -\mathbf{1}) = DP^{\otimes}_{\oplus}(-\mathbf{1}, 0 \to -\mathbf{1}) = 1$$

Proof. Since the operation $\otimes$ is symmetrical by definition, it is sufficient to consider only one of differentials:

$$DP^{\otimes}_{\oplus}(0, -\mathbf{1} \to -\mathbf{1}) =$$
$$= \overline{\sum_{x,y}} [f(x, y\oplus(-\mathbf{1})) \oplus f(x,y) = -\mathbf{1}]$$

Let us consider the left part of this equation:

$$f(x,y) = x\cdot y + x + y,$$

by definition. Then:

$$f(x, y\oplus(-\mathbf{1})) = (x+1)\cdot(2^n - y) - 1 =$$
$$= 2^n\cdot x + 2^n - x\cdot y - y - 1 =$$
$$= -\mathbf{1} - (x\cdot y + x + y) =$$
$$= -\mathbf{1} \oplus (x\cdot y + x + y)$$

Therefore,

$$DP^{\otimes}_{\oplus}(0, -\mathbf{1} \to -\mathbf{1}) = \overline{\sum_{x,y}} [-\mathbf{1} = -\mathbf{1}] = 1,$$

which concludes the proof. □

The properties from Lemmas 1 and 2 highlight that there are special differentials for the $\otimes$ operation, which must be considered when analyzing the security of the next proposed modifications. These special differentials can be seen as an analogy of those for modular addition, which have similar property:

$$DP^{\boxplus}_{\oplus}(2^{n-1}, 2^{n-1} \to 0) = 1,$$
$$DP^{\boxplus}_{\oplus}(2^{n-1}, 0 \to 2^{n-1}) = 1.$$

Lets us consider two key-adding functions:

$$Y' =$$
$$= (X_1 \otimes Z_1, X_2 \boxplus Z_2, X \boxplus Z_3, X_4 \otimes Z_4), \quad (3)$$

$$Y'' =$$
$$= (X_1 \odot Z_1, X_2 \otimes Z_2, X_3 \otimes Z_3, X_4 \odot Z_4). \quad (4)$$

As they have the same structure as the original key-adding function, the specified differential attack would work in the same way on the cipher with the replaced key-adding function.

Introduce additional value:

$$\mathbb{P}_3(\alpha) = DP^{\otimes}_{\oplus}(\alpha, 0 \to \alpha).$$

Then, for the modifications (3), (4) the differential probabilities, which are parameters of the proposed attack, are obtained as

$$\mathbb{P}_{Y'}(\alpha) = (\mathbb{P}_1)^2 \cdot (\mathbb{P}_3)^2;$$
$$\mathbb{P}_{Y''}(\alpha) = (\mathbb{P}_2)^2 \cdot (\mathbb{P}_3)^2.$$

Tables 2 and 3 were obtained through an exhaustive search of all possible differences α. As can be seen, differentials for the difference $FFFF$ hold the biggest value because of the properties mentioned in Lemmas 1 and 2. Modification Y' did not improve security level of IDEA cipher against the proposed attack; however, modification Y'' showed better results. The mean differentials probabilities are as follows for the original IDEA and modifications Y' and Y'' respectively:

$$\overline{\mathbb{P}} = 2^{-40.47};$$
$$\overline{\mathbb{P}}_{Y'} = 2^{-39.17};$$
$$\overline{\mathbb{P}}_{Y''} = 2^{-47.67}.$$

It can be seen that the structural change of modification (3) slightly decreased the cipher's strength, whereas modification (4), on the contrary, slightly increased it against the proposed attack:

$$\overline{\mathbb{P}}_{Y''} \approx (\overline{\mathbb{P}})^{1.18}.$$

Table 2
Probabilities of differentials with highest probability of the attack for modification (3)

α_{hex}	$\mathbb{P}_1$	$\mathbb{P}_3$	$\log(\mathbb{P}_{Y'})$
FFFF	0.000031	1	-29.954
8000	1	0.000031	-29.954
8080	0.5	0.000061	-30.002
8888	0.125	0.000164	-31.148
8001	0.5	0.000041	-31.148
8008	0.5	0.000041	-31.148
8010	0.5	0.000041	-31.148
8020	0.5	0.000041	-31.148
8040	0.5	0.000041	-31.148
8100	0.5	0.000041	-31.148

Table 3
Probabilities of differentials with highest probability of the attack for modification (4)

α_{hex}	$\mathbb{P}_2$	$\mathbb{P}_3$	$log(\mathbb{P}_{Y''})$
FFFF	0.000015	1	-32.049
FFFD	0.25	0.000031	-33.953
FFF9	0.062508	0.000041	-37.147
FFF1	0.015642	0.000048	-40.689
FFE1	0.003931	0.000059	-44.079
AAAA	0.00016	0.000549	-46.880
FFC1	0.001011	0.000065	-47.717
CCCC	0.000186	0.00031	-48.097
6666	0.000098	0.00031	-49.944
FF81	0.000286	0.000075	-50.949

These results are achieved by increasing the number of operations performed. For eight rounds of encryption, the original IDEA cipher performed 16 modular additions and multiplications in the key-adding function. The key-adding function (3) requires 48 modular additions, 16 modular multiplications and 16 modular subtractions for eight rounds, while key-adding function (4) requires 32 modular additions, 32 modular multiplications and 16 modular subtractions.

Conclusions

In this work, a new theoretical differential attack on the IDEA block cipher has been proposed and analyzed. The attack is based on specific properties of the key-adding function within the round transformations, particularly its interaction with the modular addition and multiplication operations that define the cipher's structure. By exploiting these properties, the proposed attack enables the construction of differential characteristics with non-negligible probabilities.

Based on the derived differential characteristics, quantitative estimates of the cipher's security level with respect to the proposed attack have been obtained. These estimates provide an analytical assessment of the computational complexity of the attack. Although the attack remains theoretical in nature, the results indicate that the security of IDEA is sensitive to the precise algebraic design of its key-adding component.

Finally, a modification of the design of the key-adding function is proposed with the objec-

tive of strengthening the cipher against the presented attack. The suggested change aims to increase security level against the proposed attack by the cost of slightly increasing the number of algebraic computations during the round transformation.

Acknowledgments

The authors would like to thank Serhii Yakovliev for his valuable guidance and insightful discussions throughout this research project, as well as for his continuous support.

References

[1] X. Lai and J. L. Massey, "A Proposal for a New Block Encryption Standard," in Advances in Cryptology – EUROCRYPT'90, pp. 389–404, 1991. DOI: 10.1007/3-540-46877-3_35.

[2] P. Junod and S. Vaudenay, "FOX: A new family of block ciphers," in Selected Areas in Cryptography, vol. 3357, 08 2004. DOI: 10.1007/978-3-540-30564-4_8.

[3] J. Nakahara, V. Rijmen, B. Preneel, and J. Vandewalle, "The MESH Block Ciphers," in Information Security Applications (K.-J. Chae and M. Yung, eds.), pp. 458–473, Springer Berlin Heidelberg, 2004. DOI: 10.1007/978-3-540-24591-9_34.

[4] H. M. Yıldırım, Some Linear Relations for Block Cipher IDEA. Ph.d. thesis, Middle East Technical University, Turkey, 2002. URL: https://etd.lib.metu.edu.tr/upload/3/12608289/index.pdf.

[5] X. Lai, On the Design and Security of Block Ciphers. Ph.d. thesis, Swiss Federal Institute of Technology, Zurich, 1992. DOI: 10.3929/ethz-a-00064671.

[6] J. Borst, L. R. Knudsen, and V. Rijmen, "Two Attacks on Reduced IDEA," in Advances in Cryptology – EUROCRYPT'97 (W. Fumy, ed.), vol. 1233 of Lecture Notes in Computer Science, pp. 1–13, Springer, 1997. DOI: 10.1007/3-540-69053-0_1.

[7] E. Biham, A. Biryukov, and A. Shamir, "Miss-in-the-Middle Attacks on IDEA, Khufu and Khafre," in Fast Software Encryption, FSE '99 (L. R. Knudsen, ed.), vol. 1636 of Lecture Notes in Computer Science, pp. 124–138, Springer, 1999. DOI: 10.1007/3-540-48519-8_10.

[8] J. Nakahara-Jr., Lai-Massey Cipher Designs. History, Design Criteria and Cryptanalysis. Springer Cham, 2018. DOI: 10.1007/978-3-319-68273-0.

[9] A. Biryukov, J. J. Nakahara, B. Preneel, and J. Vandewalle, "New Weak-Key Classes of IDEA," in Information and Communications Security – ICICS 2002 (R. H. Deng, S. Qing, F. Bao, and J. Zhou, eds.), vol. 2513 of Lecture Notes in Computer Science, pp. 315–326, Springer, 2002. DOI: 10.1007/3-540-36159-6_27.

[10] J. Daemen, R. Govaerts, and J. Vandewalle, "Weak Keys for IDEA," in Advances in Cryptology – CRYPTO'93 (D. R. Stinson, ed.), vol. 773 of Lecture Notes in Computer Science, pp. 224–231, Springer, 1993. DOI: 10.1007/3-540-48329-2_20.

[11] P. Hawkes and L. O'Connor, "XOR and Non-XOR Differential Probabilities," in Advances in Cryptology – EUROCRYPT '99, vol. 1592 of Lecture Notes in Computer Science, pp. 272–285, Springer, 1999. DOI: 10.1007/3-540-48910-X_19.

[12] S. Yakovliev and V. Bakhtigozin, "Asymptotic Distributions for S-Box Heterogeneous Differential Probabilities," Theoretical and Applied Cybersecurity, vol. 1, no. 1, pp. 37–41, 2019. DOI: 10.20535/tacs.2664-29132019.1.169029.

[13] S. Vaudenay, "On the Lai-Massey Scheme," in Advances in Cryptology – ASIACRYPT'99, pp. 8–19, Springer Berlin Heidelberg, 1999. DOI: 10.1007/978-3-540-48000-6_2.

[14] X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," in Advances in Cryptology – EUROCRYPT'91, pp. 1–12, 1991. DOI: 10.1007/3-540-46416-6_2.