Journal of Computational and Applied Mathematics 259 (2014) 561–570

Contents lists available at ScienceDirect

Journal of Computational and Applied Mathematics

journal homepage: www.elsevier.com/locate/cam

Differential entropy analysis of the IDEA block cipher

Alex Biryukov[a], Jorge Nakahara Jr.[b], Hamdi Murat Yıldırım[c,*]

[a] University of Luxembourg, Faculté des Sciences, de la Technologie et de la Communication, 6, rue Richard Coudenhove-Kalergi, L-1359, Luxembourg

[b] Department d'Informatique, Université Libre de Bruxelles, Boulevard du Triomphe - CP 212, 1050 Bruxelles, Belgium

[c] Department of Computer Technology and Information Systems, Bilkent University, TR-06800, Bilkent, Ankara, Turkey

ARTICLE INFO

Article history:
Received 12 February 2013
Received in revised form 17 April 2013

Keywords:
Shannon entropy
Differential cryptanalysis
IDEA block cipher

ABSTRACT

This paper describes a new cryptanalytic technique that combines differential cryptanalysis with Shannon entropy. We call it differential entropy (DE). The objective is to exploit the non-uniform distribution of output differences from a given mapping as a distinguishing tool in cryptanalysis. Our preferred target is the IDEA block cipher, since we detected significantly low entropy at the output of its multiplication operation. We looked to further extend this entropy analysis to larger components and for a number of rounds. We present key-recovery attacks on up to 2.5-round IDEA in the single-key model and without weak-key assumptions.

1. Introduction

The original motivation for this paper came from a simple observation: in conventional differential cryptanalysis (DC) [1], an adversary chooses pairs of plaintexts (P, P^*) with a carefully chosen difference $\Delta P = P \oplus P^*$ that lead to a ciphertext pair (C, C^*) with a predictable target difference $\Delta C = C \oplus C^*$, with high probability p (compared to a random permutation). This means that adversaries typically only focus on one or a few high-probability differences ΔP that lead to difference ΔC along a narrow differential trail, which stands out among the other trails which hold with much lower probability.

If the difference ΔC does not satisfy certain criteria (filtering conditions, bit patterns, low Hamming weights), then the pair (P, P^*) is discarded, and another pair is chosen and encrypted. In this way, only the right pairs (P, P^*) that survive the filtering conditions are collected. Due to the probabilistic nature of the attack, only a fraction of $1/p$ of the chosen data is expected to satisfy ΔC. Consequently, most plaintext pairs are discarded.

Thus, if we do not focus only on the highest probability differential trail, but rather study the probability distribution of all output differences, then we would not discard any text pair. To measure the shape of a probability distribution, we use Shannon entropy. We start by analysing a single modular multiplication in IDEA, and then move on to larger components, such as an MA-box. We are particularly interested in low entropy, which means that the probability distribution is biased towards a few output differences, while the remaining output differences hold with negligible probability. In contrast, a random permutation (or mapping over the same domain and range) should have a rather flat probability distribution, which translates into high entropy values.

This paper is organized as follows. Section 2 lists the contributions of this paper; Section 3.1 briefly describes the IDEA cipher and its internal structure; Section 3.2 briefly recalls the definition of Shannon entropy and its application to the probability distribution of output differences; Section 3.3 briefly recalls main aspects of differential cryptanalysis; Section 4 presents a differential entropy (DE) analysis of a single multiplication using xor differences; Section 5 describes attacks on

[*] Corresponding author.
E-mail addresses: alex.biryukov@uni.lu (A. Biryukov), jorge.nakahara@ulb.ac.be (J. Nakahara Jr.), hmurat@bilkent.edu.tr (H.M. Yıldırım).

0377-0427/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cam.2013.08.002

reduced-round IDEA based on results of Section 4; Section 6 presents a differential entropy analysis of a single multiplication using subtraction difference; Section 7 describes attacks on reduced-round IDEA based on results of Section 6; and Section 8 concludes the paper.

2. Contributions

The main contributions of this paper include the following.

- The combination of differential cryptanalysis and Shannon entropy [2] as a new distinguishing tool for the analysis of block ciphers such as IDEA [3]. The new technique is called differential entropy (DE).
- In IDEA, all multiplications are key dependent; that is, one operand is always a round subkey. Therefore, the probability distribution of output differences for every multiplication is key dependent. But this is not a problem, since DE is an appropriate tool to measure the shape of the probability distribution of key-dependent differences.
- Notice that the exact value or even the Hamming weight of the differences are not important for entropy computations, as is often the case in differential cryptanalysis. DE analysis takes into account all possible (output) differences, without ignoring any of them. The more skewed/biased the probability distribution, the lower the entropy. In a sense, our analyses could be interpreted as a kind of *low entropy trail* analysis similar to that based on a *narrow differential trail*.
- We employ both exclusive-or and subtraction as difference operators for measuring the differential entropy.
- We demonstrate significantly low differential entropy after a single multiplication, under input difference 8000_x, for any subkey, both using xor and subtraction differences.

3. Preliminaries

This chapter provides well-known definitions and concepts which are mentioned in this paper.

Definition 1. The *Hamming weight* of a string of bits is the number of 1s in the string.

3.1. IDEA block cipher

The IDEA cipher operates on 64-bit blocks under a 128-bit key and iterates 8.5 rounds (Fig. A.1). IDEA is a design by Lai and Massey [3], and its main design feature is the use of three group operations on 16-bit words: addition in $\mathbb{Z}_{2^{16}}$ (denoted $\boxplus$), bitwise xor (denoted $\oplus$), and multiplication in $GF(2^{16}+1)$ with $0 \equiv 2^{16}$ (denoted $\odot$). Moreover, no operation is applied twice in a row along the encryption framework. The round structure of IDEA is unique in the sense that (i) there are no explicit Substitution boxes (S-boxes); (ii) it is neither a Feistel nor an SPN design; (iii) the round function is an involution which makes the encryption and decryption frameworks very similar except for the reverse order and slightly modified round subkeys.

The key schedule of IDEA consists of a linear transformation that simply permutes the bits of the 128-bit key. We do not exploit weak keys/subkeys [4,5] or related keys, and we refer to [3] for further details.

3.2. Shannon entropy

For completeness purposes, we briefly recall the definition of Shannon entropy.

Definition 2. Let X be a (discrete) random variable over a finite set $\{x_1, \ldots, x_n\}$ with probability distribution $p_i = P(X = x_i)$. The *Shannon entropy* of X is a quantitative measure of the amount of information provided by an observation of X: $H(X) = -\sum_{p_i \neq 0} p_i \cdot \log_2(p_i)$. Note that $0 \leq H(X) \leq \log_2 n$.

In the context of differential cryptanalysis, the probability distribution of interest is related to the output difference distribution of a mapping.

Definition 3. The *differential entropy* of a mapping $F : D \to R$, for finite domain D and finite range R, under input difference operator $\otimes$, and output difference operator $\boxdot$, is the entropy of the set of output differences corresponding to a fixed input difference Δ_i. Denote by Δ_o the possible output differences of F. Let $p_{\Delta_o}(\Delta_i) = \frac{|\{X \in D | F(X) \boxdot F(X \otimes \Delta_i) = \Delta_o\}|}{|D|}$. Then, for a given Δ_i,

$$H(F, \Delta_i) = - \sum_{\Delta_o | p_{\Delta_o}(\Delta_i) \neq 0} p_{\Delta_o}(\Delta_i) \cdot \log_2(p_{\Delta_o}(\Delta_i)). \tag{1}$$

This concept of *differential entropy* is not the same *differential entropy* as used in a well-known book on Information Theory by Cover and Joy [6], since it does not concern *continuous random variables*.

In Sections 4 and 5, we set $\otimes = \boxdot = \oplus$ as the difference operator. In Section 6, we exploit modular subtraction as the difference operator. We drop the subscripts Δ_o when it is clear from the context.

3.3. Differential cryptanalysis

Differential cryptanalysis (DC) is a chosen plaintext technique developed by Biham and Shamir formerly to attack the DES cipher [1]. The intuition is that for carefully chosen plaintext pairs, (P, P^*), with a given difference $\Delta P = P \oplus P^*$, the ciphertext pairs, (C, C^*), are expected to have a predictable difference $\Delta C = C \oplus C^*$ with high probability p. This is a statistical attack requiring $O(p^{-1})$ chosen plaintexts.

DC has become a general type of attack, and it has been adapted to stream ciphers [7], hash functions [8], and MAC algorithms [9].

In [10], Albrecht and Leander proposed a model to distinguish between the probability distribution of the right key and the one for the wrong key. Considering one fixed input difference and all associated differences for block ciphers in which the subkey gets mixed with the internal state via an xor operation, their model considers multinomial distributions and suggests better success probabilities against combinations of standard DC and its variants. However, it also comes with increased time and memory complexities, for instance, exhausting the codebook.

Note that the subkeys of IDEA are involved as operands of the multiplication or the modular addition. In this paper, we use a new technique, the differential entropy analysis of a single multiplication using xor differences.

For our attacks on IDEA, we exploit whenever possible some well-known difference values, such as 8000_x, that can bypass modular addition and exclusive-or for free:

$$(X \boxplus Z) \oplus ((X \oplus 8000_x) \boxplus Z) = 8000_x, \quad \forall Z \in \mathrm{GF}(2^{16}+1),$$

where the subscript x denotes hexadecimal notation. Therefore, 8000_x is a fixed point difference for modular addition and for xor. This way, we can focus only on the multiplications.

Definition 4 (*[1]*). An i-round *differential trail* is a sequence of differences $(\Delta x_1, \Delta x_2, \ldots, \Delta x_{i+1})$, where Δx_1 is the initial input difference to the first round; Δx_j is both the output difference observed after the round $j-1$ and the input difference to the round j for $j \in \{2, \ldots, i\}$.

Definition 5 (*[1]*). The probability of a i-round differential trail or a differential characteristic $(\Delta x_1, \Delta x_2, \ldots, \Delta x_{i+1})$ corresponds to the fraction of text pairs that satisfy all differences Δx_j for $i \le j \le i+1$, among all possible such pairs.

DC is also a very flexible technique in the sense that there are many variants based on it or combined with other methods, such as truncated differentials, impossible differentials, differential-linear [5], boomerang [11], and rectangle attacks. In a sense, DE is yet another differential-based attack.

4. Differential entropy of a single multiplication

We start by studying a single $\odot$. We use whenever possible the wordwise difference 8000_x, and make no assumptions about the subkey value, which we denote simply as Z, when its position is implicit from the context or not relevant. Using the terminology in (1), the probability distributions of output differences $\Delta_o = (X \odot Z) \oplus ((X \oplus 8000_x) \odot Z)$ for some subkey Z are listed in Table 1. Note that, in this table, not only are very few output differences possible, but the ones that show up are not uniformly distributed. Some differences are much more probable than others, and this distribution depends on the subkey value. Plotting a graph of the entropy distribution for all possible 16-bit subkeys in the horizontal axis and the entropy in the vertical axis, one obtains Fig. A.2. Since the multiplication is over 16-bit inputs, entropy values were computed taking into account all possible input pairs with difference 8000_x, exhaustively.

The mirror symmetry in Fig. A.2 provides a lot of information about the entropy behaviour in $\odot$, such as the following.

- The minimum entropy is zero for the well-known weak subkeys $Z \in \{0000_x, 0001_x\}$ [4], while the maximum entropy is 10.444, for $Z \in \{5557_x, AAAA_x\}$. Overall, the entropy is significantly low, because only a few output differences are suggested, and even those that are possible are not uniformly distributed. This observation is valid for any 16-bit subkey value. The meaning of low is made clear when we compare the entropy with $-\sum_{2^{16}-1} 1/(2^{16}-1) * \log_2 1/(2^{16}-1) = \log_2(2^{16}-1) \approx 15.99$, which is expected from a random 16-bit permutation. The lower the entropy, the better the (entropy-based) distinguisher compared to the expected behaviour for an ideal 16-bit permutation. Apart from IDEA, we have also examined the xor difference entropy of the AES S-box [12]. The result is that, for any nonzero input xor difference, the output xor difference entropy is 6.9843. This is a consequence of the fact that the AES S-box is based on a differentially uniform mapping [13], which makes the probability distribution of output differences flatter and closer to uniform. Moreover, for the Skipjack S-box [14], the entropy is variable, but is on average 6.557. Both values are close to the maximum $\log_2 255 \approx 7.9943$ expected from an ideal 8-bit permutation.
- The existence of equivalent subkeys from the point of view of differential entropy, that is, subkeys with the same entropy and the same probability distribution. For instance, the subkeys 8000_x and 8001_x both have the second lowest entropy, 0.00094254. In general, subkeys Z and $2^{16}+1-Z$ share the same probability distribution, which explains the mirror-symmetric curve in Fig. A.2. The proof is as follows. Notice that $2^{16}+1-Z = -Z = 0 \odot Z$ in $\mathrm{GF}(2^{16}+1)$, since $0 \equiv 2^{16}$.

Table 1
Probability distribution of output differences of a single multiplication with input difference 8000_x.

Z	Δ_o	$p_{\Delta_o}(8000_x)$	$H(\odot, 8000_x)$
4000_x	2000_x	$65528/2^{16} = 2^{-0.000176}$	0.00188
	6000_x	2^{-14}	
	$e000_x$	2^{-14}	
2000_x	1000_x	$65520/2^{16} = 2^{-0.000352}$	0.00364
	3000_x	2^{-13}	
	7000_x	2^{-14}	
	$f000_x$	2^{-14}	
1000_x	0800_x	$65504/2^{16} = 2^{-0.000705}$	0.00692
	1800_x	2^{-12}	
	3800_x	2^{-13}	
	7800_x	2^{-14}	
	$f800_x$	2^{-14}	

$(X\odot -Z)\oplus((X\oplus 8000_x)\odot -Z) = (X\odot 0\odot Z)\oplus((X\oplus 8000_x)\odot 0\odot Z) = ((X\odot 0)\odot Z)\oplus(((X\oplus 8000_x)\odot 0)\odot Z) = ((-X)\odot Z)\oplus((-(X\oplus 8000_x))\odot Z) = ((10001_x - X)\odot Z)\oplus((10001_x - X - 8000_x)\odot Z) = ((10001_x - X)\odot Z)\oplus((8001_x - X)\odot Z)$.

Let $Y = 8001_x - X$. We have

$(X \odot -Z) \oplus ((X \oplus 8000_x) \odot -Z) = ((Y \oplus 8000_x) \odot Z) \oplus (Y \odot Z)$.

This implies that, under the input difference 8000_x, we have the same set of output differences for both Z and $-Z$. □

In the next section, we use the differential entropy analysis of a single multiplication as an effective DE attack on reduced-round versions of IDEA.

5. DE attacks on IDEA using xor differences

We first attack 1.5-round IDEA starting from an MA half-round with input difference either of the form $(8000_x, 0000_x, 8000_x, 0000_x)$ or $(0000_x, 8000_x, 0000_x, 8000_x)$. Differences are depicted in red in Fig. A.3. Due to the chosen differences, the MA-box is bypassed by these differences; that is, the input difference to the first MA-box is $(0000_x, 0000_x)$ in both cases. The difference after the next half-round is either $(\Delta, 8000_x, 0000_x, 0000_x)$ or $(0000_x, 0000_x, 8000_x, \Delta)$, where Δ stands for an unknown set of differences depending on $Z_1^{(2)}$ or $Z_4^{(2)}$. Let us focus on the case $(\Delta, 8000_x, 0000_x, 0000_x)$, the leftmost scheme in Fig. A.3. The other case is similar. Whatever Δ is, we know from Section 4 that the output difference entropy of Δ is low (Fig. A.2).

We describe two ways to attack 1.5-round IDEA. One can exploit $A \oplus B$, which means the rightmost input to the (second) MA-box. Note that $A \oplus B$ has zero entropy, since the difference is fixed: 8000_x. For a random permutation, one would expect the entropy to be much higher than zero. Therefore, we can distinguish 1.5-round IDEA from a random permutation by just comparing the entropy at $A \oplus B$. Alternatively, one can use $C \oplus D$ and exploit the entropy in Δ after $Z_1^{(2)}$, which is not zero but still low (compared to that of a random permutation).

Based on these 1.5-round distinguishers, we can further perform key-recovery attacks on 2-round IDEA, recovering $(Z_3^{(3)}, Z_4^{(3)})$ if we use (A, B) or $(Z_1^{(3)}, Z_2^{(3)})$ if we use (C, D).

Suppose the case of $A \oplus B$, whose entropy is zero. This means that there is only a single output difference in $A \oplus B$. If we partially decrypt a half-round by guessing values for $(Z_3^{(3)}, Z_4^{(3)})$ and further observe two (or more) distinct differences coming out of $A \oplus B$, then we will be sure that we are not dealing with 2-round IDEA, but rather with a random permutation (and the guessed subkey values are wrong), because the entropy should be zero. In general, if we expect differential entropy H at some point, but observe 2^{H+1} differences, then we get a contradiction of the expected entropy. Notice that, according to Shannon's formula, $H \leq \log_2 n$, where n is the number of possible output differences. To guarantee that we got differences from enough pairs at $A \oplus B$, we try all 2^{15} possible pairs of 16-bit words with difference 8000_x at the input. The data complexity becomes 2^{16} chosen plaintexts. The memory complexity is constant. We guess 32 key bits, and partially decrypt one $\boxplus$, one $\odot$, and perform one $\oplus$. This costs approximately one fourth of a round. Thus, there are $2^{32} \cdot 2^{16}/4 \cdot 1/2 = 2^{45}$ 2-round computations.

If we use $C \oplus D$ instead, then we use a structure composed of 2^{15} text pairs of the form $\{(a, b, c, d), (a \oplus 8000_x, b, c \oplus 8000_x, d)\}$, and encrypt them across 2-round IDEA, as in the rightmost scheme in Fig. A.3. This means 2^{16} chosen plaintexts. We guess $(Z_1^{(3)}, Z_2^{(3)})$, and check the entropy after a half-round partial decryption, obtaining a difference $C \oplus D$. If the entropy of the differences in $C \oplus D$ is low, then we have potential candidate values for $(Z_1^{(3)}, Z_2^{(3)})$. Otherwise, the subkeys guessed were wrong. The effort is $2^{32} \cdot 2^{16}$ computations of an $\boxplus$, an $\oplus$, and a $\odot$. This is about the cost of a quarter of a round. Thus, there are 2^{45} 2-round computations.

We can further extend the attack to 2.5-round IDEA. Consider two pools of plaintexts of the form (a, b, c, d) and (a, b, c', d), where $c \oplus c' = 8000_x$, and $a \in \{0, \ldots, 2^{16} - 1\}$; b and d are arbitrary fixed values. Each pool contains 2^{16} chosen plaintexts. One can form 2^{32} pairs using these pools, and about 2^{16} of these pairs will have difference $(8000_x, 0000_x, 8000_x,$

0000_x) after the first half-round. This is the input difference and the number of pairs we needed in our previous attack on 2-round IDEA. We recover $Z_1^{(3)}, Z_2^{(3)}, Z_3^{(3)}$ and $Z_4^{(3)}$, with $2 \cdot 2^{16}$ chosen plaintexts (CP) and equivalent memory, but there are 64 key bits left to recover. This last step can be performed by exhaustive key search.

6. Differential entropy using subtraction differences

An alternative difference operator for DC is modular subtraction, which, on the one hand, makes differences non-commutative but, on the other hand, such differences propagate across modular addition for free (i.e. with probability 1). The differential entropy is computed according to (1) with $\otimes = \boxminus = -$.

Let us first consider a single multiplication. We have output difference $\Delta_o = (X \odot Z) - ((X - \Delta_i) \odot Z)$, for an input difference Δ_i and subkey Z.

Fig. A.4 is a similar graph to that of Section 4, but this time using modular subtraction as the difference, for arbitrary fixed subkeys Z. In Fig. A.4, we observe a minimum entropy of zero for $Z \in \{0000_x, 0001_x\}$ and maximum entropy 1.99996 for $Z \in \{00D9_x, FF28_x\}$, which means there are at most four differences coming out of a single multiplication, whatever the subkey value. This entropy range is even lower than that observed for xor differences in Fig. A.2.

For the AES *s*-box, subtraction differences give a maximum entropy of 7.2981, which is higher than the xor entropy in Section 4.

Moreover, we observe in Fig. A.4 a mirror symmetry just like in Fig. A.2. The reason is the following: the output difference we measure now is $\Delta_o = (X \odot Z) - ((X - 8000_x) \odot Z)$. Notice that for the subkey $2^{16} + 1 - Z = -Z = 0 \odot Z$ in $\mathrm{GF}(2^{16}+1)$ we have $(X \odot -Z) - ((X - 8000_x) \odot -Z) = (X \odot 0 \odot Z) - ((X - 8000_x) \odot 0 \odot Z) = (X \odot Z) \odot 0 - ((X - 8000_x) \odot Z) \odot 0 = -(X \odot Z) \boxplus ((X - 8000_x) \odot Z) = -\Delta_o$. Therefore, the subkeys Z and $2^{16} + 1 - Z$ lead to the same probability distribution, but the difference values are additive complements: Δ_o and $-\Delta_o$, respectively. Notice that, for instance, $00D9_x$ and $FF28_x$ are equivalent subkeys, since $00D9_x \boxplus FF28_x = 2^{16} + 1$.

Note that the difference value $\Delta_i = 8000_x$ is very special, because, if a pair of 16-bit words (X, X^*) satisfy $X - X^* = 8000_x$, then $X = X^* \boxplus 8000_x$, and, since the difference affects only the most significant bit, we have $X = X^* \oplus 8000_x$. Thus, $X^* = X \oplus 8000_x$ or $X^* = X \boxplus 8000_x$; that is, $X^* - X = 8000_x$. In summary, in the special case $\Delta_i = 8000_x$, the subtraction difference becomes commutative. In general, if $X - X^* = \Delta$, then $X = X^* \boxplus \Delta$; that is, $X^* - X = -\Delta = 2^{16} - \Delta$. The only way $2^{16} - \Delta = \Delta$ in $\mathbb{Z}_{2^{16}}$ is if $\Delta = 8000_x$.

Apart from the duality $X \boxplus 8000_x = X \oplus 8000_x$ that connects operations in $\mathbb{Z}_{2^{16}}$ and $\mathbb{Z}_2^{16}$, another motivation to invest in the subtraction difference for entropy analysis is that the modular multiplication can be viewed simply as repeated addition. This is made clearer by Lai's Low–High algorithm [15] for multiplication in $GF(2^{16}+1)$.

Let $a, b \in \mathbb{Z}_{2^{16}+1}$, $R = ab \bmod 2^{16}$, and $Q = ab \operatorname{div} 2^{16}$. Then

$$a \odot b = \begin{cases} R - Q & \text{if } R \geq Q \\ R - Q + 2^{16} + 1 & \text{if } R < Q, \end{cases}$$

where R denotes the remainder ('Low' part) and Q denotes the quotient ('High' part) when ab is divided by 2^{16}.

The following theorem upper bounds the entropy of a single multiplication using subtraction differences and the input difference $\Delta X = 8000_x$.

Theorem 1. *Let $\Delta X = X - X' = 8000_x$, for $X, X', Z \in \mathbb{Z}_2^{16}$. Then, there are at most four possible output differences $\Delta Y = X \odot Z - (X - \Delta X) \odot Z$. Consequently, the output difference entropy $H(\Delta Y) \leq 2$, $\forall Z \in \mathbb{Z}_{2^{16}}$.*

The proof of this theorem is in the Appendix.

7. DE attacks on IDEA using subtraction differences

Distinguish-from-random attacks using subtraction difference can be performed just like the attack on 1.5-round IDEA starting from an MA half-round in Section 5. Let us use, for instance, an input difference of the form $(0000_x, 8000_x, 0000_x, 8000_x)$. We refer again to Fig. A.3. Due to the fact that $X - X^* = 8000_x$ is the same as $X \oplus X^* = 8000_x$, the input difference to the first MA-box is $(0000_x, 0000_x)$. The difference after the next half-round is $(0000_x, 0000_x, 8000_x, \Delta)$, where Δ stands for an unknown set of up to four differences whose specific values depend on $Z_4^{(2)}$ according to Fig. A.4. Whatever the difference values in Δ, we know that the difference entropy of Δ is lower than 2.

As in Section 5, one can exploit $A \oplus B$, which means the leftmost input to the (second) MA-box. Note that $A \oplus B$ has zero entropy, since the (subtraction) difference is always 8000_x. For a random permutation, one would expect the entropy to be much higher than zero. Therefore, we can distinguish 1.5-round IDEA from a random permutation by just comparing the entropy of $A \oplus B$. Alternatively, one can use $C \oplus D$ and exploit the entropy in Δ after $Z_4^{(2)}$, which is not zero but still quite low (less than 2).

Based on these 1.5-round distinguishers, we can further perform key-recovery attacks on 2-round IDEA, recovering $(Z_1^{(3)}, Z_2^{(3)})$ if we use (A, B) or $(Z_3^{(3)}, Z_4^{(3)})$ if we use (C, D).

Table 2
The complexity of attacks on from 2-round to 6-round IDEA.

Rounds	Attack	Reference	Data	Time[a]
2	Differential	[16]	2^{10} CP	2^{40}
2.5	Differential	[4]	2^{10} CP	2^{32}
2.5	Diff. entropy	Section 5	2^{17} CP	2^{64}
2.5	Differential	[16]	2^{10} CP	2^{106}
3	Differential-linear	[17]	2^{29} CP	2^{44}
3.5	Differential	[17]	2^{56} CP	2^{67}
3.5	Linear	[18]	103 KP	2^{97}
4	Impossible differential	[19]	$2^{36.6}$ CP	$2^{66.6}$
4	Linear	[20]	114 KP	2^{114}
4.5	Impossible differential	[19]	2^{64} KP	$2^{110.4}$
5	Demirci–Selçuk–Türe	[21]	2^{24} CP	2^{126}
5	Demirci–Selçuk–Türe	[22]	$2^{24.6}$ CP	2^{124}
5.5	Key-dependent linear	[23]	2^{21} CP	$2^{112.1}$
6	Key-dependent linear	[23]	2^{49} CP	$2^{112.1}$

CP: chosen plaintext; KP: known plaintext.

[a] The *Time* measurement unit is the number of associated round computations.

Suppose the case of $A \oplus B$, whose entropy is zero. This means that there is only a single output difference in $A \oplus B$. If we partially decrypt a half-round by guessing values for $(Z_1^{(3)}, Z_2^{(3)})$, and further observe two (or more) distinct differences in $A \oplus B$, then we will be sure we are not dealing with 2-round IDEA, but rather with a random permutation (and the guessed subkey values are wrong), because the entropy should be zero. In general, if we expect differential entropy H at some point, but observe 2^{H+1} or more differences, then we get a contradiction of the expected entropy. Notice that, according to Shannon's formula, $H \leq \log_2 n$, where n is the number of possible output differences. To guarantee we got all differences at $A \oplus B$, we try all 2^{15} possible pairs of 16-bit words with difference 8000_x. The data complexity becomes 2^{16} chosen plaintexts. The memory complexity is constant. We guess 32 key bits, and partially decrypt one $\boxplus$, one $\odot$, and perform one $\oplus$. This costs approximately one fourth of a round. Thus, there are $2^{32} \cdot 2^{16}/4 \cdot 1/2 = 2^{45}$ 2-round computations.

If we use $C \oplus D$ instead, then we use a structure composed of 2^{15} text pairs of the form $\{(a, b, c, d), (a, b \oplus 8000_x, c, d \oplus 8000_x)\}$, and encrypt them across 2-round IDEA as in the rightmost scheme in Fig. A.3. This means 2^{16} chosen plaintexts. We guess $(Z_3^{(3)}, Z_4^{(3)})$, and check the entropy after a half-round partial decryption, obtaining a difference $\nabla = C \oplus D$. If the entropy of the differences in ∇ is less than 2, then we have potential candidate values for $(Z_3^{(3)}, Z_4^{(3)})$. Otherwise, the subkeys guessed were wrong. The effort is $2^{32} \cdot 2^{16}$ computations of an $\boxplus$, an $\oplus$, and a $\odot$. This is about the cost of a quarter of a round. Thus, there are 2^{45} 2-round computations.

A similar strategy to that of Section 5 for attacking 2.5-round IDEA can also be used with subtraction differences. Just notice that for the subtraction difference the entropy after multiplication is at most 2 (lower than for the xor difference).

8. Conclusion

This paper has described a new attack technique called differential entropy, combining differential cryptanalysis with Shannon entropy. Our target was the IDEA block cipher, due to the heavy use of key-dependent modular multiplication in $GF(2^{16} + 1)$, which makes the difference distribution of output differences also key dependent. Furthermore, we observed and sometimes even proved that the entropy can be low for some components, such as $\odot$, for most of the subkey values.

Our analyses, using xor and subtraction differences, were applied to 2.5-round IDEA.

Table 2 can be used to compare the complexity of attacks on 2.5-round IDEA.

In summary, we exploit the biased probability distribution of output differences in (reduced-round) IDEA cipher, in a novel way.

Experiments in IDEA-32, a mini version of IDEA operating on 32-bit blocks, exhausting the codebook (2^{32} plaintexts) and using a difference of the form $(00_x, 80_x, 00_x, 80_x)$, for both xor and subtraction differences, indicated that the entropy increases steadily after 1.5 rounds because of the interaction between the $\oplus$ operation and the subtraction differences after the MA-box. That means that, although the MA-box output has low entropy, it is not preserved after the $\oplus$ operations mixing the MA-box outputs to the four words in a cipher state at the end of a round. The measured entropy reached values close to 8 for all four words in the state, which is the maximum for 8-bit words. Thus, we could no longer distinguish reduced-round IDEA-32 from a random permutation beyond two rounds using DE. We expect the same behaviour in the original IDEA cipher.

9. Future work and open problems

There are alternative research directions to try.

- One could try to combine entropy with other techniques to detect nonrandom behaviour such as χ^2 tests.
- One could attack other ciphers based on IDEA, such as MESH [24] and RIDEA [25].

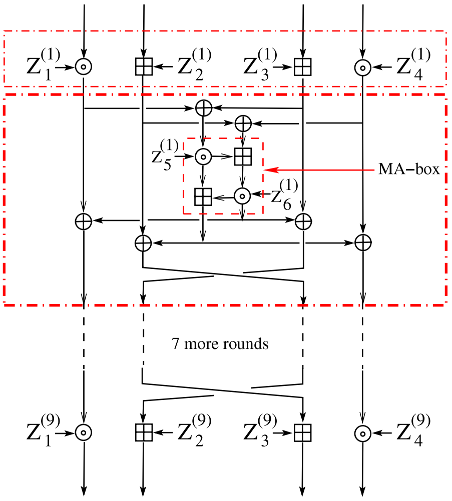

Fig. A.1. Computational graph of half-rounds, a full round, and an MA-box of the IDEA cipher.

- We have consistently worked with differences based on xor and subtraction as difference operators. Another possibility is to use multiplicative differentials [26], or mixed differences [15] such as $(-, \oplus, \oplus, -)$, that is, a modular subtraction difference for $\odot$ and xor differences for $\boxplus$.

Acknowledgement

The second author was funded by INNOVIRIS, the Brussels Institute for Research and Innovation, under the ICT Impulse program CRYPTASC.

Appendix. Proof of Theorem 1

Let $A \cdot 2^{16} + B = X * Z$ and $A' \cdot 2^{16} + B' = (X - \Delta X) * Z = (X - 8000_x) * Z = (X + 8000_x) * Z$, where $*$ denotes multiplication in $\mathbb{Z}_{2^{16}}$. The conversion between multiplication in $\mathbb{Z}_{2^{16}}$ and multiplication in $GF(2^{16}+1)$ is Lai's Low–High algorithm

$$X \odot Z = \begin{cases} B - A & \text{if } B \geq A \\ 2^{16} + 1 + B - A & \text{if } B < A. \end{cases}$$

The representation of $X \odot Z$ in terms of the extended 32-bit value $A \cdot 2^{16} + B$ allows us to distinguish the influence of the input difference ΔX and subkey Z on the distribution of output differences. Let $Z = (z_{15}, z_{14}, \ldots, z_0)$ and $X = (x_{15}, x_{14}, \ldots, x_0)$, with $x_i, z_i \in \mathbb{Z}_2$, $0 \leq i \leq 15$. The distribution of output differences ΔY will be analysed in terms of the 16-bit quantities A, A', B, and B'. Consider the following cases.

(i) $z_0 = 1, x_{15} = 0, x'_{15} = 1$.
(ii) $z_0 = 1, x_{15} = 1, x'_{15} = 0$.
(iii) $z_0 = 0, x_{15} = 0, x'_{15} = 1$.
(iv) $z_0 = 0, x_{15} = 1, x'_{15} = 0$.

The only difference between B and B' is in the most significant bit, namely, $B \oplus B' = \Delta X = 8000_x$. In (i), if $z_{15} = 0$, then $B = B' + \Delta X$, and $A' = A + 1 + Z \gg 1$, where $Z \gg 1$ means right shift of Z by one bit (the least significant bit of Z is discarded). If $z_{15} = 1$, then $B' = B + \Delta X$, and $A' = A + Z \gg 1$.

For $z_{15} = 0$ the following output differences can result.

- The case $B' \geq A'$ and $B \geq A$ gives $\Delta Y_1 = B' - A' - (B - A) = B + \Delta X - A - 1 - Z \gg 1 - B + A = \Delta X - 1 - Z \gg 1$.
- The case $B' \geq A'$ and $B < A$ gives $\Delta Y_2 = B' - A' - (2^{16} + 1 + B - A) = B + \Delta X - A - 1 - Z \gg 1 - 2^{16} - 1 - B + A = \Delta X - Z \gg 1$.
- The case $B' < A'$ and $B < A$ gives $\Delta Y = 2^{16} + 1 + B' - A' - (2^{16} + 1 + B - A) = \Delta Y_1$.
- The case $B' < A'$ and $B \geq A$ cannot happen, because $B' < A' \Rightarrow B + \Delta X < A + Z \gg 1 \Rightarrow B < A - \Delta X + Z \gg 1 < A$. The last inequality holds because $\Delta X > Z \gg 1, \forall Z \in \mathbb{Z}_2^{16}$. This contradicts the assumption that $B \geq A$.

For $z_{15} = 1$, the possible output differences are identical to ΔY_1 (for $B' \geq A'$ and $B \geq A$) and ΔY_2 (for $B' \geq A'$ and $B < A$). The case $B' < A'$ and $B < A$ gives $\Delta Y = \Delta Y_1$, and, finally, $B' < A'$ and $B \geq A$ cannot happen, because $B' < A' \Rightarrow B + \Delta X < A + Z \gg 1 \Rightarrow B < A - \Delta X + Z \gg 1 < A$. The last inequality holds because $\Delta X > Z \gg 1$, $\forall Z \in \mathbb{Z}_2^{16}$. This contradicts the assumption that $B < A$.

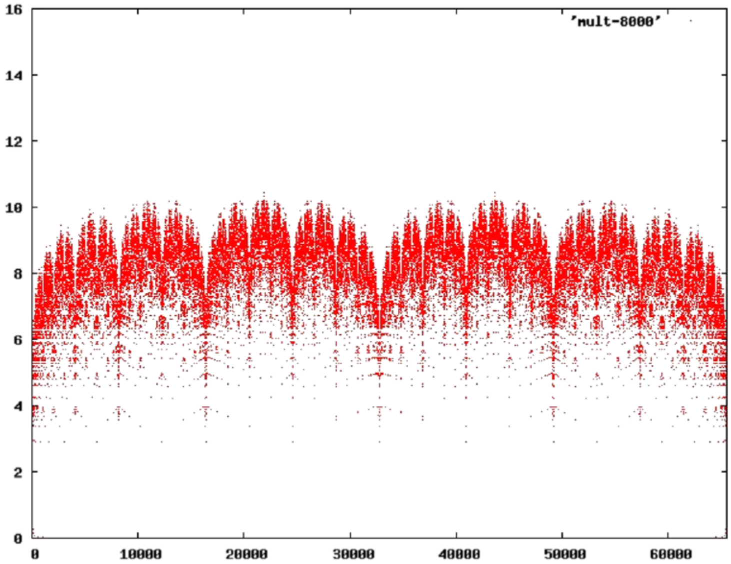

Fig. A.2. Differential entropy distribution for $\odot$ with input difference 8000_x.

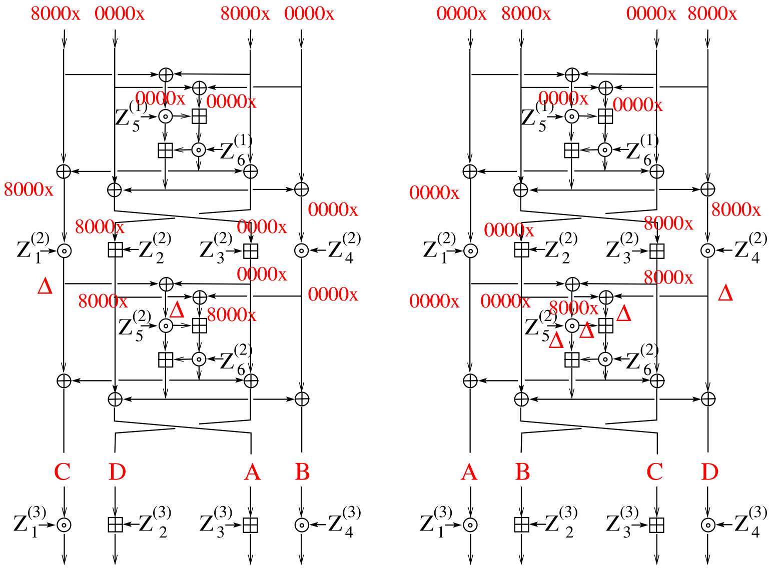

Fig. A.3. Attack on reduced-round IDEA using differential entropy of a single multiplication.

The remaining possible output differences are the additive complements of ΔY_1 and ΔY_2: $\Delta Y_3 = 2^{16} - \Delta Y_1 = \Delta X + Z \gg 1$, and $\Delta Y_4 = 2^{16} - \Delta Y_2 = \Delta X + 1 + Z \gg 1$. This result comes from the fact that both $B' - A' \geq B - A$ and $B' - A' < B - A$ can occur in the computation of ΔY.

In (ii), similarly, changing the roles of A and A', and of B and B', if $z_{15} = 0$, then $B' = B + \Delta X$ and $A = A' + 1 + Z \gg 1$; if $z_{15} = 1$, then $B = B' + \Delta X$ and $A = A' + Z \gg 1$.

For $z_{15} = 0$ the possible output differences are as follows.

- The case $B' \geq A'$ and $B \geq A$ gives $\Delta Y_1 = B' - A' - (B - A) = B + \Delta X - A + 1 + Z \gg 1 - B + A = \Delta X + 1 + Z \gg 1$.
- The case $B' \geq A'$ and $B < A$ gives $\Delta Y_2 = B' - A' - (2^{16} + 1 + B - A) = B + \Delta X - A + 1 + Z \gg 1 - 2^{16} - 1 - B + A = \Delta X + Z \gg 1$.
- The case $B' < A'$ and $B < A$ gives $\Delta Y = \Delta Y_1$.
- The case $B' < A'$ and $B \geq A$ cannot happen, because $B' < A' \Rightarrow B - \Delta X < A - 1 - Z \gg 1 \Rightarrow B < A + \Delta X - 1 - Z \gg 1 < A$. The last inequality holds because $\Delta X > Z \gg 1$, $\forall Z \in \mathbb{Z}_2^{16}$. This contradicts the assumption that $B \geq A$.

In (iii), there is no difference between B and B', because $z_0 = 0$, and the input difference ΔX which affects only the most significant bits of X and $X + \Delta X$ is not present in the 16 least significant bits of the 32-bit result of conventional multiplication. Two cases are distinguished: $(x_{15} = 0 \Leftrightarrow x'_{15} = 1) \Rightarrow A' = A + Z \gg 1$ or $(x_{15} = 1 \Leftrightarrow x'_{15} = 0) \Rightarrow A = A' + Z \gg 1$.

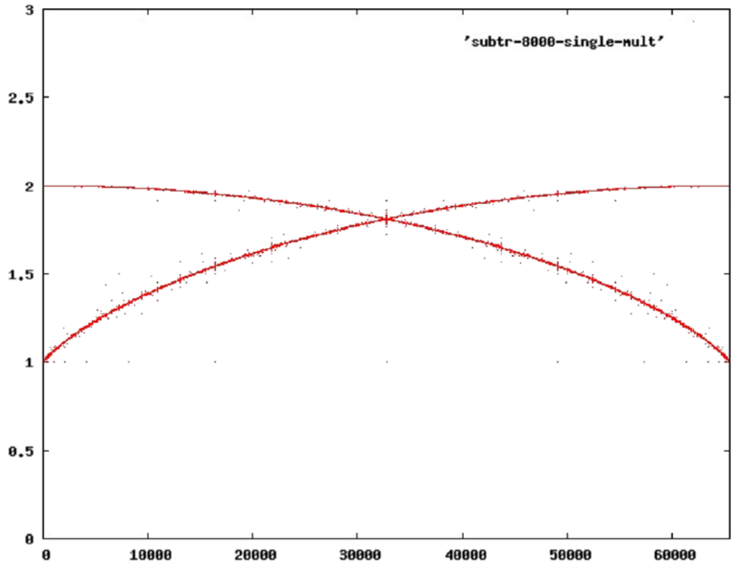

Fig. A.4. Subtraction entropy distribution of a single $\odot$ with input difference 8000_x.

If $A' = A + Z \gg 1$, then the output differences are as follows.

- The case $B' \geq A'$ and $B \geq A$ gives $\Delta Y_1 = B' - A' - (B - A) = B - A - Z \gg 1 - B + A = -Z \gg 1 = 2^{16} - Z \gg 1$.
- The case $B' \geq A'$ and $B < A$ gives $\Delta Y_2 = B' - A' - (2^{16} + 1 + B - A) = B - A + Z \gg 1 - 2^{16} + 1 - B + A = Z \gg 1 - 1$.
- The case $B' < A'$ and $B < A$ gives the difference ΔY_1.
- The case $B' < A'$ and $B \geq A$ cannot happen, because $B' < A' \Rightarrow B < A - Z \gg 1 < A$ for $Z \notin \{0, 1\}$. This contradicts the assumption that $B \geq A$.

In (iv), similarly to (iii), changing the roles of A and A', and of B and B', the same results follow. □

For some subkeys, there are fewer than four possible output differences. These keys are $0, 1, 2^i, 2^{16} + 1 - 2^i, 1 \leq i \leq 15$.

For the subkey $Z = 1$, there is only the output difference $\Delta X = 8000_x$, which corresponds to ΔY_1 and ΔY_3. The difference ΔY_2 (and ΔY_4) cannot occur, because $A = A'$. Thus, the entropy $H_Z(\Delta Y) = 0$ for $Z = 1$.

For $Z = 0 = 2^{16}$, the extended multiplication can be viewed with one extra layer corresponding to the 17th bit of Z. This will imply that only A and A' will differ ($B = B'$), namely $A - A' = \Delta X$. Therefore, $A > B$ and $A' > B'$, always, and $\Delta Y = 2^{16} + 1 + B' - A' - (2^{16} + 1 + B - A) = B' - A' - B + A = A - A' = \Delta X$. Therefore, the entropy $H_Z(\Delta Y) = 1$ for $Z = 0$.

For $Z = 2^i$, $1 \leq i \leq 15$, there can be only two possible output differences. Notice that $z_0 = 0$; that is, all these subkeys are even valued. The differences ΔY_2 (and consequently ΔY_4) cannot happen, because $B' \geq A', B < A$, and $B' = B$ imply that $A > B = B' \geq A'$, but, since $A' = A + Z \gg 1$, it follows that $A' < A$, which contradicts the assumption that $A' = A + Z \gg 1$, for $Z > 1$. The possible differences are $\Delta Y_1 = 2^{16} - Z \gg 1 = 2^{16} - 2^{i-1}$ and $\Delta Y_3 = Z \gg 1 = 2^{i-1}$. Similarly, the additive complements of subkeys that are powers of 2 also generate only two output differences. They correspond to $Z = 2^{16} - 2^i$, $1 \leq i \leq 15$. Notice that all of these subkeys are odd valued ($z_0 = 1$). The differences ΔY_2 (and ΔY_4) cannot happen, because $B' \geq A', B < A$, and $B' = B + \Delta X$ imply that $A + \Delta X > B + \Delta X = B' \geq A'$, but, on the other hand $A = A' + 1 + Z \gg 1 \leq A' + \Delta X$. This is a contradiction. The possible differences are $\Delta Y_1 = \Delta X - Z \gg 1$ and its additive complement $\Delta Y_3 = \Delta X + Z \gg 1$.

Therefore, except for $Z \in \{0, 2^i, 2^{16} - 2^i\}, 0 \leq i \leq 15$, there are exactly four output differences $\Delta Y = X \odot Z - (X - \Delta X) \odot Z$ for $\Delta X = 8000_x$. It follows that the output entropy $H_Z(\Delta Y) = 2$. These output differences and their distribution can be denoted as $(\Delta Y_1, 2^{16}p_1)$, $(\Delta Y_2, 2^{16}p_2)$, $(\Delta Y_3, 2^{16}p_3)$, $(\Delta Y_4, 2^{16}p_4)$, where p_i is the probability of occurrence of the ith difference, and $\sum_{i=1}^{4} p_i = 1$. The value p_i are key dependent. Moreover, $\Delta Y_3 = 2^{16} - \Delta Y_1$, which implies that ΔY_3 and ΔY_1 occur equally often ($p_3 = p_1$), and similarly $p_2 = p_4$.

Another symmetry in the distribution is that $p_1 + p_2 = \frac{1}{2}$. The output entropy $H_Z(\Delta Y)$ can, therefore, be considerably simplified:

$$H_Z(\Delta Y) = -\sum_{i=1}^{4} p_i \cdot \log p_i = -2 \cdot p_1 \cdot \log_2 p_1 - 2 \cdot (1/2 - p_1) \cdot \log_2(1/2 - p_1).$$

As noticed before, for subkeys Z that are powers of 2, the following equality holds:

$$H_Z(\Delta Y) = H_{2^{16}+1-Z}(\Delta Y),$$

where $\Delta X = 8000_x$.

References

[1] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, in: Adv. in Cryptology, CRYPTO'90, in: LNCS, vol. 537, Springer, 1990, pp. 2–21.

[2] C.E. Shannon, A mathematical theory of communication, Bell System Technical Journal 27 (1948) 379–423 and 623–656.

[3] X. Lai, J.L. Massey, S. Murphy, Markov ciphers and differential cryptanalysis, in: Adv. in Cryptology, Eurocrypt'91, in: LNCS, vol. 547, Springer, 1991, pp. 17–38.

[4] J. Daemen, R. Govaerts, J. Vandewalle, Weak keys for IDEA, in: Adv. in Cryptology, CRYPTO'93, in: LNCS, vol. 773, Springer, 1993, pp. 224–231.

[5] P. Hawkes, Differential-linear weak key classes of IDEA, in: Adv. in Cryptology, EUROCRYPT'98, in: LNCS, vol. 1403, Springer, 1998, pp. 112–126.

[6] T.M. Cover, J.A. Thomas, Elements of Information Theory, Wiley-Interscience, New York, NY, USA, 1991.

[7] E. Biham, O. Dunkelman, Differential cryptanalysis in stream ciphers, IACR ePrint Archive, 2007/218.

[8] X. Wang, H. Yu, Y. Lisa Yin, Efficient collision search attacks on SHA-0, in: Adv. in Cryptology, CRYPTO 2005, in: LNCS, vol. 3621, Springer, 2005, pp. 1–16.

[9] J. Kim, A. Biryukov, B. Preneel, S. Hong, On the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1, in: Security and Cryptography for Networks, 5th International Conference, SCN 2006, in: LNCS, vol. 4116, Springer, 2006, pp. 242–256.

[10] M.R. Albrecht, G. Leander, An all-in-one approach to differential cryptanalysis for small block ciphers, in: L.R. Knudsen, H. Wu (Eds.), Selected Areas in Cryptography (SAC), in: LNCS, vol. 7707, Springer, 2013, pp. 1–15.

[11] D. Wagner, The boomerang attack, in: Workshop on Fast Software Encryption, FSE'99, in: LNCS, vol. 1636, Springer, 1999, pp. 156–170.

[12] FIPS197: Advanced Encryption Standard (AES), FIPS PUB 197 Federal Information Processing Standard Publication, vol. 197, US Department of Commerce, 2001.

[13] K. Nyberg, Differentially uniform mappings for cryptography, in: Adv. in Cryptology, EUROCRYPT 1993, in: LNCS, vol. 765, Springer, 1993, pp. 55–64.

[14] NSA: Skipjack and KEA Algorithm Specifications, Version 2.0, May 29, 1998.

[15] X. Lai, On the Design and Security of Block Ciphers, Ph.D. Dissertation ETH no. 9752, Swiss Federal Institute of Technology, Zurich, Hartung-Gorre Verlag Konstanz, 1992.

[16] W. Meier, On the security of the IDEA block cipher, in: T. Helleseth (Ed.), Adv. in Cryptology, Eurocrypt'93, in: LNCS, vol. 765, Springer, 1994, pp. 371–385.

[17] J. Borst, L.R. Knudsen, V. Rijmen, Two Attacks on Reduced Round IDEA, Advances in Cryptology, Proceedings of EUROCRYPT 1997, in: Lecture Notes in Computer Science, vol. 1233, Springer-Verlag, 1997, pp. 1–13.

[18] P. Junod, New Attacks Against Reduced-Round Versions of IDEA, Proceedings of Fast Software Encryption 2005, in: Lecture Notes in Computer Science, vol. 3557, Springer-Verlag, 2005, pp. 384–397.

[19] E. Biham, A. Biryukov, A. Shamir, Miss in the Middle Attacks on IDEA and Khufu, Proceedings of Fast Software Encryption 1999, in: Lecture Notes in Computer Science, vol. 1636, Springer-Verlag, 1999, pp. 124–138.

[20] J. Nakahara Jr., B. Preneel, J. Vandewalle, The Biryukov–Demirci Attack on Reduced-Round Versions of IDEA and MESH Ciphers, Proceedings of Australasian Conference on Information Security and Privacy 2004, in: Lecture Notes in Computer Science, vol. 3108, Springer-Verlag, 2004, pp. 98–109.

[21] H. Demirci, A.A. Selçuk, Erkan Türe, A New Meet-in-the-Middle Attack on the IDEA Block Cipher, Proceedings of Selected Areas in Cryptography 2003, in: Lecture Notes in Computer Science, vol. 3006, Springer-Verlag, 2004, pp. 117–129.

[22] E.S. Ayaz, A.A. Selçuk, Improved DST Cryptanalysis of IDEA, Proceedings of Selected Areas in Cryptography 2006, in: Lecture Notes in Computer Science, vol. 4356, Springer-Verlag, 2007, pp. 1–14.

[23] X. Sun, X. Lai, The Key-Dependent Attack on Block Ciphers, Advances in Cryptology, Proceedings of ASIACRYPT 2009, in: Lecture Notes in Computer Science, vol. 5912, 2009, pp. 19–36.

[24] J. Nakahara Jr., V. Rijmen, B. Preneel, J. Vandewalle, The MESH block ciphers, in: Information Security Applications (WISA'03), in: LNCS, vol. 2908, Springer, 2003, pp. 458–473.

[25] H.M. Yıldırım, Nonlinearity properties of the mixing operations of the block cipher IDEA, in: Progress in Cryptology, INDOCRYPT, 4th International Conference on Cryptology in India, in: LNCS, vol. 2904, Springer, 2003, pp. 68–81.

[26] N. Borisov, M. Chew, R. Johnson, D. Wagner, Multiplicative differentials, in: Fast Software Encryption, FSE'02, in: LNCS, vol. 2365, Springer, 2002, pp. 17–33.