Cryptanalysis of IDEA-X/2

Håvard Raddum

Dep. of Informatics, The University of Bergen, Norway

Abstract. IDEA is a 64-bit block cipher with a 128-bit key designed by J. Massey and X. Lai. At FSE 2002 a slightly modified version called IDEA-X was attacked using multiplicative differentials. In this paper we present a less modified version of IDEA we call IDEA-X/2, and an attack on this cipher. This attack also works on IDEA-X, and improves on the attack presented at FSE 2002.

Keywords: Cryptography, block ciphers, differential cryptanalysis, IDEA.

1 Introduction

The block cipher PES (Proposed Encryption Standard) was introduced at Eurocrypt in 1990 [1]. When differential cryptanalysis [2] became known in 1991, the algorithm was changed, and renamed to IPES (Improved PES). Later the cipher has become known as IDEA (International Data Encryption Algorithm), and is today used in many cryptographic components.

IDEA has been extensively cryptanalysed, but remains unbroken. We briefly mention some of this work. In 1993 2.5 rounds of IDEA was attacked with differential cryptanalysis [3]. At CRYPTO the same year, large classes of weak keys due to the simple key schedule were presented [4]. At EUROCRYPT 1997, 3- and 3.5-round versions of IDEA were broken using a differential-linear attack and a truncated differential attack [5]. Larger classes of weak keys were demonstrated at EUROCRYPT 1998 [6]. At FSE 1999 impossible differentials were used to attack 4.5 rounds of IDEA [7], and at SAC 2002 attacks on IDEA for up to four rounds were improved [8].

At FSE 2002 multiplicative differentials were used to attack a slightly modified version of IDEA called IDEA-X [9]. We show in this paper that there exists a better attack for IDEA-X, and that this attack also works on a less modified version of IDEA we have chosen to call IDEA-X/2 (read as “idea x half”).

The paper is organised as follows. In Section 2 we give a brief description of IDEA and its variants, in Section 3 we build the differential characteristic used to attack IDEA-X/2, in Section 4 we show how to find the subkeys used in the output transformation, and we conclude in Section 5.

2 Description of IDEA

IDEA operates on blocks of 64 bits, using a 128-bit key. The cipher consists of several applications of three group operations $\oplus$, $\boxplus$ and $\odot$. Each operation joins together two words of 16 bits. The operation $\oplus$ is bitwise XOR, $\boxplus$ is addition modulo 2^{16}, and $\odot$ is multiplication modulo $2^{16}+1$, where the all-zero word is treated as the element 2^{16}. IDEA has eight rounds, followed by an output transformation. One round of IDEA and the output transformation is shown in the figure below.

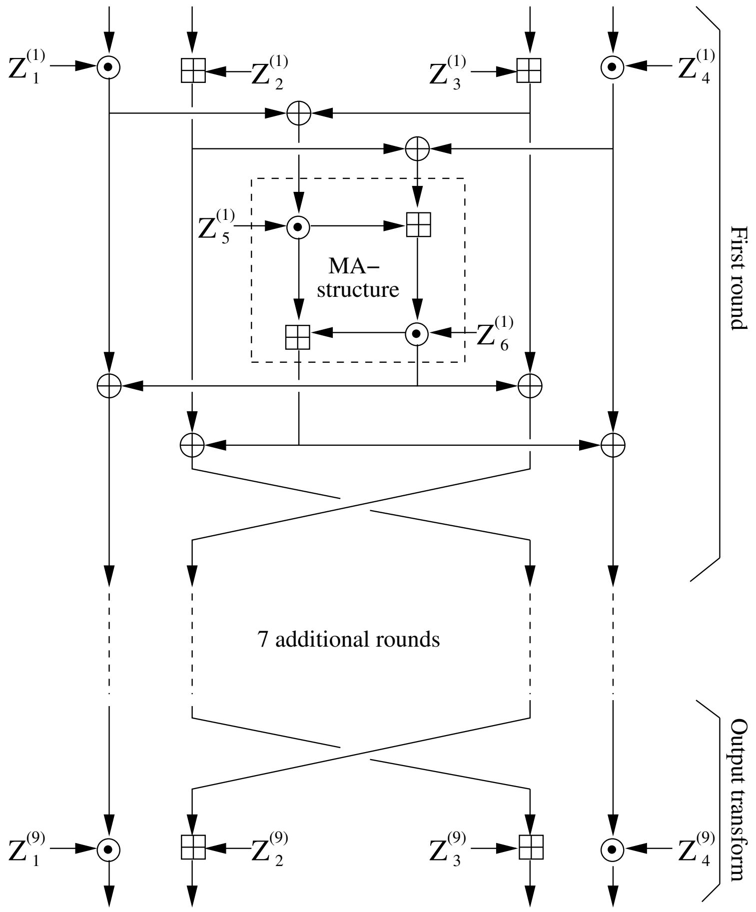

Fig. 1. Structure of IDEA

The security of IDEA lies in the fact that no two of the three group operations are compatible, in the sense that the distributive law does not hold. The designers have also made sure that any two contiguous group operations in IDEA are never the same.

$Z_i^{(r)}$ is subkey i used in round r, where the output transformation counts as the ninth round. Each subkey is a 16-bit word, and a total of 52 subkeys are needed. They are generated as follows. The user selects a 128-bit master key, viewed as eight 16-bit words. The first 8 subkeys are taken as these 8 words, from left to right. Then the master key is cyclically rotated 25 positions to the left, and the resulting eight 16-bit words are taken as the next subkeys, and so on. The order the subkeys are taken in is $Z_1^{(1)}, Z_2^{(1)}, \ldots, Z_6^{(1)}, Z_1^{(2)}, \ldots, Z_6^{(2)}, \ldots, Z_4^{(9)}$.

2.1 IDEA-X and IDEA-X/2

In [9], a variant called IDEA-X is attacked. In IDEA-X, each $\boxplus$ except for the two in the output transformation is changed to an $\oplus$. The authors then show that for 2^{112} of the keys there exists a multiplicative differential characteristic over eight rounds that holds with probability 2^{-32}.

In this paper we consider IDEA-X/2, where we only change half of the $\boxplus$'s in one round to $\oplus$'s. In IDEA-X/2 only the $\boxplus$'s where $Z_2^{(r)}$ and $Z_3^{(r)}$ are inserted are changed to $\oplus$'s, the MA-structure is left unchanged.

3 Building a differential characteristic

3.1 The groups $\mathbb{Z}_{2^{16}}$ and $\mathrm{GF}(2^{16}+1)^*$

The basis of our analysis comes from the fact that both $\mathbb{Z}_{2^{16}}$ and $\mathrm{GF}(2^{16}+1)^*$ are cyclic groups, and therefore isomorphic (see [10]). Here we establish this isomorphism as follows.

Let g_0 be a primitive element of $\mathrm{GF}(2^{16}+1)^*$, and define $g_i = g_{i-1}^2$ for $i = 1, \ldots, 15$. Then each element a in $\mathrm{GF}(2^{16}+1)^*$ can be written uniquely as

$$a = g_{15}^{x_{15}} \odot g_{14}^{x_{14}} \odot \cdots \odot g_0^{x_0},$$

where each $x_i \in \{0, 1\}$. For simpler notation we will write this as $a = \mathbf{g}^{\mathbf{x}}$. Let ϕ be the map from $\mathrm{GF}(2^{16}+1)^*$ to $\mathbb{Z}_{2^{16}}$ defined by $\phi(a) = \mathbf{x}$, where $a = \mathbf{g}^{\mathbf{x}}$. We show that ϕ is an isomorphism.

The identity element of $\mathrm{GF}(2^{16}+1)^*$ is 1, and the identity element of $\mathbb{Z}_{2^{16}}$ is $\mathbf{0}$. Since $1 = \mathbf{g}^{\mathbf{0}}$ we have $\phi(1) = \mathbf{0}$.

Clearly, ϕ is one-to-one.

Let $a = \mathbf{g}^{\mathbf{x}}$ and $b = \mathbf{g}^{\mathbf{y}}$ be two elements of $\mathrm{GF}(2^{16}+1)^*$. Then

$$a \odot b = g_{15}^{x_{15}} \odot g_{15}^{y_{15}} \odot \cdots \odot g_0^{x_0} \odot g_0^{y_0}.$$

If at least one of x_i, y_i is 0 then $g_i^{x_i} \odot g_i^{y_i} = g_i^{x_i+y_i}$, with $x_i + y_i \in \{0,1\}$. If $x_i = y_i = 1$ we get $g_i^1 \odot g_i^1 = g_{i+1}^1 \odot g_i^0$, that is, we get a "carry". Note that $g_{15} = -1$, so if $x_{15} = y_{15} = 1$ we have $g_{15}^1 \odot g_{15}^1 = g_{15}^0$, which means the carry is shifted out of the computation.

From this we see that $a \odot b = \mathbf{g}^{\mathbf{x} \boxplus \mathbf{y}}$, showing that $\phi(a \odot b) = \phi(a) \boxplus \phi(b)$, and that ϕ respects the group operations. This shows that ϕ is an isomorphism.

3.2 Differential properties of ϕ

In a cryptographic setting, we may regard ϕ as a 16-bit S-box. The above analysis shows that $a \odot b = \phi^{-1}(\phi(a) \boxplus \phi(b))$. In other words, the two diagrams below may be used interchangeably.

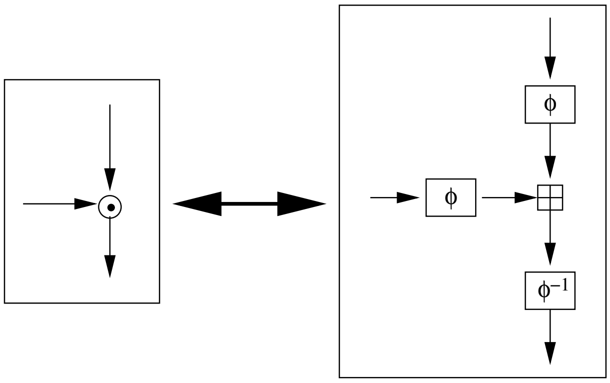

Fig. 2. Isomorphic diagrams

We have computed the S-box ϕ explicitly using $g_0 = 3$ as a primitive element, and checked its differential properties. In the first key-mixing layer in each round, $Z_1^{(r)}$ and $Z_4^{(r)}$ are mixed with two of the words using $\odot$. Using the isomorphic diagram above, we may first send the keys and the two words through ϕ, and then combine using $\boxplus$. In the analysis of the differential properties we should therefore let the output differences of ϕ be $\boxminus$, subtraction modulo 2^{16}.

We found that if we let the input differences to ϕ be differences with respect to $\oplus$, then the following differential holds with probability 1/2:

$$\delta_{\oplus} = FFFD_x \xrightarrow{\phi} \delta_{\boxminus} = 2^{15}.$$

The difference $\delta_{\boxminus}$ is preserved through the key-addition. Through ϕ^{-1} we get the reversed differential with probability 1/2: $\delta_{\boxminus} \xrightarrow{\phi^{-1}} \delta_{\oplus}$. These may be combined into the differential

$\delta_{\oplus} \xrightarrow{Z_j^{(r)} \odot} \delta_{\oplus}$ that, on the average over all keys $Z_j^{(r)}$, holds with probability 1/4 ($j \in \{1,4\}$). For each key $Z_j^{(r)}$, we have checked the exact probability of this differential. The keys 1 and -1 are known to be weak under $\odot$, the differential holds with probability 1 and 0.5, respectively. The smallest probability that occurs (for the keys 3 and -3 with $g_0 = 3$) is greater than 0.166.., and the probability lies in the range $0.23 - 0.27$ for $2^{16} - 22$ of the possible values for $Z_j^{(r)}$.

3.3 Differential characteristic of IDEA-X/2

Let the 64-bit cipher block be denoted by (w_1, w_2, w_3, w_4), where each w_i is a 16-bit word referred to as word i.

All differences in the characteristic are with respect to $\oplus$, and we denote $\delta = FFFD_x$. Let a pair of texts at the beginning of one round have difference $(\delta, \delta, \delta, \delta)$. Words 2 and 3 will have difference δ after XOR with $Z_2^{(r)}$ and $Z_3^{(r)}$. Each of the words 1 and 4 will have difference δ after multiplication with $Z_1^{(r)}$ and $Z_4^{(r)}$ with probability 1/4. Thus the difference after the key-mixing layer in the beginning of the round is $(\delta, \delta, \delta, \delta)$ with probability 2^{-4}.

Since the differences in words 1 and 3 are the same and the differences in words 2 and 4 are the same, the two input differences to the MA-structure are both 0. Then the output differences of the MA-structure will be 0, so the difference of the blocks after the XOR with the outputs from the MA-structure will be $(\delta, \delta, \delta, \delta)$. Since words 2 and 3 have equal differences the difference of the blocks after the swap at the end of the round will also be $(\delta, \delta, \delta, \delta)$.

This one-round characteristic may be concatenated with itself 8 times to form the 8-round differential characteristic

$$(\delta, \delta, \delta, \delta) \overset{8 \text{ rounds}}{\longrightarrow} (\delta, \delta, \delta, \delta)$$

that holds with probability $(2^{-4})^8 = 2^{-32}$.

The probability of this characteristic may be increased by a factor four as follows. In the first round $Z_1^{(1)}$ and $Z_4^{(1)}$ are inserted using $\odot$. We look at the alternative diagram for this operation, containing the S-boxes ϕ. Then we see that the first application of ϕ is done to words 1 and 4 of the plaintext block, before any key-material has been inserted. This means we can select the plaintext pairs such that the words 1 and 4 will have difference $\delta_{\boxminus}$ before $\phi(Z_1^{(1)})$ and $\phi(Z_4^{(1)})$ are inserted, with probability 1. Then the probability of the characteristic of the first round will be 2^{-2} instead of 2^{-4}, and the overall probability of the 8-round characteristic will be 2^{-30}.

4 Key recovery

We select 2^{32} pairs of plaintext with difference $(\delta, \delta, \delta, \delta)$, and ask for the corresponding ciphertexts. A pair of plaintexts that has followed the characteristic is called a *right* pair, and a pair that has not followed the characteristic is called a *wrong* pair. We expect to have 4 right pairs among the 2^{32} pairs.

4.1 Filtering out wrong pairs

Let c_i and c'_i be the i'th words of the ciphertexts in one pair. We compute what values (if any) $Z_2^{(9)}$ and $Z_3^{(9)}$ may have to make this pair a right pair. If this pair is a right pair we have $(c_2 \boxminus Z_2^{(9)}) \oplus (c'_2 \boxminus Z_2^{(9)}) = \delta$. Two cases arise.

Case 1: The second least significant bits of $(c_2 \boxminus Z_2^{(9)})$ and $(c'_2 \boxminus Z_2^{(9)})$ are both 0. Since $(c_2 \boxminus Z_2^{(9)})$ and $(c'_2 \boxminus Z_2^{(9)})$ are otherwise bitwise complementary to each other, we have $(c_2 \boxminus Z_2^{(9)}) \boxplus (c'_2 \boxminus Z_2^{(9)}) = 2^{16} - 3$. This yields $2Z_2^{(9)} = 3 \boxplus c_2 \boxplus c'_2$, which is possible only if exactly one of c_2 and c'_2 is odd. In that case we get $Z_2^{(9)} = (3 \boxplus c_2 \boxplus c'_2) >> 1$ or $Z_2^{(9)} = ((3 \boxplus c_2 \boxplus c'_2) >> 1) \boxplus 2^{15}$.

Case 2: The second least significant bits of $(c_2 \boxminus Z_2^{(9)})$ and $(c'_2 \boxminus Z_2^{(9)})$ are both 1. In this case we have $(c_2 \boxminus Z_2^{(9)}) \boxplus (c'_2 \boxminus Z_2^{(9)}) = 1$. This gives $2Z_2^{(9)} = 2^{16} - 1 \boxplus c_2 \boxplus c'_2$, again only possible when exactly one of c_2 and c'_2 is odd. In that case we get $Z_2^{(9)} = (2^{16} - 1 \boxplus c_2 \boxplus c'_2) >> 1$ or $Z_2^{(9)} = ((2^{16} - 1 \boxplus c_2 \boxplus c'_2) >> 1) \boxplus 2^{15}$.

When exactly one of c_2 and c'_2 is odd, we don't know if we are in case 1 or 2, so four values of $Z_2^{(9)}$ will be suggested.

The reasoning above also applies to c_3 and c'_3, so when exactly one of c_3 and c'_3 is odd, we will get four values of $Z_3^{(9)}$ suggested.

The probability that, in a random pair, exactly one of c_2 and c'_2 is odd, and exactly one of c_3 and c'_3 is odd is $1/4$. When we filter on this condition about 2^{30} of the pairs will remain.

Next we focus on the words c_1 and c'_1 in a pair. For the multiplication with $Z_1^{(9)}$ we use the alternative diagram containing the S-boxes ϕ and ϕ^{-1}. We have examined how the 2^{16} pairs with input difference δ behave through ϕ. It turns out that 2^{15} pairs get output difference 2^{15} (with respect to $\boxminus$), and that there are 2^{15} other possible output differences, each with a unique pair producing it. Now we go backwards through the last ϕ^{-1} and look at the difference $\phi(c_1) \boxminus \phi(c'_1)$. If this difference is not one of the possible output differences of ϕ receiving input difference δ, we can throw away this pair as a wrong pair. When ϕ receives input difference δ there are $2^{15} + 1$ possible output differences, so this happens with probability $1/2$.

The same reasoning applies for c_4 and c'_4, so the probability of both words 1 and 4 surviving this test is $1/4$. After performing this test we expect to be left with 2^{28} pairs, each one with the possibility of being a right pair.

4.2 Finding the subkey $(Z_1^{(9)}, Z_2^{(9)}, Z_3^{(9)}, Z_4^{(9)})$

Each of the remaining pairs has at least one subkey that would make it a possible right pair. For each pair, these subkeys are suggested as the right subkeys. The correct subkey is suggested for each right pair, and all wrong keys are suggested more or less at random. We proceed to count how many keys each pair suggests.

Each pair suggests 4 values of $Z_2^{(9)}$ and 4 values of $Z_3^{(9)}$. These values can be combined in 16 different ways to produce a possible $(Z_2^{(9)}, Z_3^{(9)})$-value for the subkey. By examining the key schedule, we find that $Z_2^{(9)}$ and $Z_3^{(9)}$ completely determine $Z_4^{(1)}$. Letting p_4 and p'_4 be the fourth words of the plaintexts in one pair, we check for each of the 16 values of $Z_4^{(1)}$ if $(p_4 \odot Z_4^{(1)}) \oplus (p'_4 \odot Z_4^{(1)}) = \delta$. If this doesn't hold, and the pair we are examining is a right pair, then the value of $Z_4^{(1)}$ (and hence $(Z_2^{(9)}, Z_3^{(9)})$) must be wrong and can be discarded. Because of the special way we have chosen p_4 and p'_4 (we have $\phi(p_4) \boxminus \phi(p'_4) = 2^{15}$ with probability 1), the probability of passing this test is 1/2, so we expect that 8 of the initial 16 possible $(Z_2^{(9)}, Z_3^{(9)})$-values remain.

The number of $(Z_1^{(9)}, Z_4^{(9)})$-values suggested for one pair depends on whether $\phi(c_1) \boxminus \phi(c'_1)$ or $\phi(c_4) \boxminus \phi(c'_4)$ is 2^{15}. Whenever $\phi(c_1) \boxminus \phi(c'_1) = 2^{15}$, this pair will suggest 2^{15} values of $Z_1^{(9)}$.

When $\phi(c_1) \boxminus \phi(c'_1) \neq 2^{15}$ we will get exactly one value of $Z_1^{(9)}$ suggested, likewise for $Z_4^{(9)}$. We expect to have four right pairs, each with difference δ in words 1 and 4 just before ϕ in the output transformation. The probability of getting difference 2^{15} after ϕ is 1/2 for each word, so we expect that one of the right pairs will suggest 2^{15} values for both $Z_1^{(9)}$ and $Z_4^{(9)}$, a total of 2^{30} values for $(Z_1^{(9)}, Z_4^{(9)})$. The probability that a random pair after filtering has $\phi(c_1) \boxminus \phi(c'_1) = \phi(c_4) \boxminus \phi(c'_4) = 2^{15}$ is 2^{-30}, so we don't expect any other pairs to have this property, since we are left with only 2^{28} pairs.

The probability that a random pair after filtering has $\phi(c_1) \boxminus \phi(c'_1) = 2^{15}$ is 2^{-15}, so we expect to find 2^{13} pairs with this property. These pairs will suggest 2^{15} values for $Z_1^{(9)}$ and one value for $Z_4^{(9)}$ each. The same goes for the fourth word, we expect 2^{13} pairs suggesting one value for $Z_1^{(9)}$ and 2^{15} values for $Z_4^{(9)}$.

All other pairs will suggest exactly one value for $(Z_1^{(9)}, Z_4^{(9)})$.

Each of the values suggested from one pair for $(Z_1^{(9)}, Z_4^{(9)})$ must be coupled with the eight values for $(Z_2^{(9)}, Z_3^{(9)})$, so the total number of subkeys suggested is expected to be

$$8(1 \cdot 2^{30} + 2^{13} \cdot 2^{15} + 2^{13} \cdot 2^{15} + (2^{28} - 2^{14}) \cdot 1) \approx 2^{34}.$$

The correct subkey is expected to be suggested 4 times, and the other keys are expected to be distributed more or less at random over the other 2^{64} possible values. It is highly unlikely that a wrong key should be suggested four times, so we take the most suggested key as the correct subkey.

4.3 Finding the rest of the key

By keeping track of which pairs suggest which keys, the right pairs will be revealed. The remaining 64 bits of the master key may be found by further analysis using the right pairs. Since we know the differences in these pairs at any stage of the encryption, we may start at the plaintext or ciphertext side and let these pairs suggest values for the (partially) unknown subkeys. We will not go into details here, but this strategy should work faster than searching exhaustively for the remaining 64 bits.

5 Conclusion

We have shown how to use the isomorphism between the groups $\mathbb{Z}_{2^{16}}$ and $\mathrm{GF}(2^{16}+1)^*$ as a basis for a differential attack on IDEA-X/2 that works without any conditions on the subkeys. This attack also works on IDEA-X, and gives an improvement over the attack found in [9]. This shows that the security of IDEA depends on the fact that $\boxplus$ and not $\oplus$ is used when inserting the subkeys $Z_2^{(r)}$ and $Z_3^{(r)}$.

A 4-round characteristic has been implemented, to check that theory and practice are consistent when the round keys are not independent, but generated by the key schedule. The implementation also incorporated the first round trick, bringing the probability of the differential to 2^{-14}. One thousand keys were generated at random, and for each key 2^{20} pairs of plaintext were encrypted, and the number of right pairs recorded. The expected number of right pairs is 64, the actual number of right pairs produced by the keys ranged from 33 to 131. Thus the analysis (assuming independent round keys) seems to be consistent with the key schedule of IDEA.

References

1. X. Lai and J. Massey. *A Proposal for a New Block Encryption Standard.* Advances in Cryptology - EUROCRYPT '90, LNCS 0473, pp. 389 - 404, Springer-Verlag 1991
2. E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer Verlag, 1993.
3. W. Meier. *On the security of the IDEA block cipher.* Advances in Cryptology - EUROCRYPT '93, LNCS 0765, pp. 371 - 385, Springer-Verlag 1994.
4. J. Daemen, R. Govaerts and J. Vandewalle. *Weak Keys for IDEA.* Advances in Cryptology - CRYPTO '93, LNCS 0773, pp. 224 - 231, Springer-Verlag 1994.
5. J. Borst, L. Knudsen and V. Rijmen. *Two Attacks on Reduced IDEA.* Advances in Cryptology - EUROCRYPT '97, LNCS 1233, pp. 1 - 13, Springer-Verlag 1997.
6. P. Hawkes. *Differential-Linear Weak Key Classes of IDEA.* Advances in Cryptology - EUROCRYPT '98, LNCS 1403, pp. 112 - 126, Springer-Verlag 1998
7. E. Biham, A. Biryukov and A. Shamir. *Miss in the Middle Attacks on IDEA and Khufu.* Fast Software Encryption '99, LNCS 1636, pp. 124 - 138, Springer-Verlag 1999.
8. H. Demirci. *Cryptanalysis of IDEA using Exact Distributions.* Selected Areas in Cryptography, pre-proceedings.

9. N. Borisov, M. Chew, R. Johnson and D. Wagner. *Multiplicative Differentials.* Fast Software Encryption 2002, LNCS 2365, pp. 17 - 33, Springer-Verlag 2002.
10. D. R. Stinson. *Cryptography Theory and Practice.* CRC Press 1995, p. 179.