Miss in the Middle Attacks on IDEA, Khufu and Khafre

Eli Biham* Alex Biryukov** Adi Shamir***

Abstract. In a recent paper we developed a new cryptanalytic technique based on *impossible differentials*, and used it to attack the Skipjack encryption algorithm reduced from 32 to 31 rounds. In this paper we describe the application of this technique to the block ciphers IDEA, Khufu and Khafre. In the case of IDEA, the new attacks have smaller complexities and cover more rounds than the best currently known attacks. This demonstrates the power of the new cryptanalytic technique, shows that it is applicable to a larger class of cryptosystems, and develops new technical tools for applying it in new situations.

1 Introduction

In [4] we proposed a new cryptanalytic technique based on impossible differentials and described its application to Skipjack [27]. In this paper we apply this technique to the IDEA, Khufu and Khafre cryptosystems. In the case of IDEA our new attacks are much more efficient and cover more rounds than the best previously known attacks on this cipher.

The main idea behind these new attacks is a bit counter-intuitive. Unlike traditional differential and linear cryptanalysis which predict and detect statistical events of highest possible probability, our new approach is to search for events that never happen. Such impossible events are then used to distinguish the cipher from a random permutation, or to perform key elimination (a candidate key is obviously wrong if it leads to an impossible event).

The fact that impossible events can be useful in cryptanalysis is an old idea (for example, some of the attacks on Enigma were based on the observation that letters can not be encrypted to themselves). However these attacks tended to be highly specific, and there was no systematic analysis in the literature of how to identify an impossible behavior in a block cipher and how to exploit it in order to derive the key. In this paper we continue to develop these attacks including the general technique called *miss in the middle* to construct impossible events and a general *sieving attack* which uses such events in order to cryptanalyze the block-cipher. We demonstrate these techniques in the particular cases of

* Computer Science Department, Technion – Israel Institute of Technology, Haifa 32000, Israel, biham@cs.technion.ac.il, http://www.cs.technion.ac.il/~biham/.

** Applied Mathematics Department, Technion – Israel Institute of Technology, Haifa 32000, Israel.

*** Department of Applied Mathematics and Computer Science, Weizmann Institute of Science, Rehovot 76100, Israel, shamir@wisdom.weizmann.ac.il.

Year [Author]	Rounds	Type	Chosen Plaintexts	Time of Analysis
1993 [22]	2	differential	2^{10}	2^{42}
1993 [22]	2.5	differential	2^{10}	2^{106}
1993 [9]	2.5	differential	2^{10}	2^{32}
1997 [8]	3	differential-linear	2^{29}	2^{44}
1997 [8]	3.5	truncated-differential	2^{56}	2^{67}
1998 This paper	3.5	impossible-differential	$2^{38.5}$	2^{53}
	4*	impossible-differential	2^{37}	2^{70}
	4.5	impossible-differential	2^{64}	2^{112}

* From the second to the fifth round.

Table 1 Summary of our attacks on IDEA with reduced number of rounds compared to the best previous results.

IDEA, Khufu and Khafre block ciphers. The main idea is to find two events with probability one, whose conditions cannot be met together. In this case their combination is an impossible event, that we are looking for. Once the existence of impossible events in a cipher is proved, it can be used directly as a distinguisher from a random permutation. Furthermore we can find the keys of a cipher by analyzing the rounds surrounding the impossible event, and guessing the subkeys of these rounds. All the keys that lead to impossibility are obviously wrong. The impossible event in this case plays the role of a *sieve*, methodically rejecting the wrong key guesses and leaving the correct key. We stress that the miss in the middle technique is only one possible way to construct impossible events and the sieving technique is only one possible way to exploit them.

In order to get a sense of the attack, consider a cipher $E(\cdot)$ with n-bit blocks, a set of input differences $\mathcal{P}$ of cardinality 2^p and a corresponding set of output differences $\mathcal{Q}$ of cardinality 2^q. Suppose that no difference from $\mathcal{P}$ can cause an output difference from $\mathcal{Q}$. We ask how many chosen texts should be requested in order to distinguish $E(\cdot)$ from a random permutation? In general about 2^{n-q} pairs with differences from $\mathcal{P}$ are required. This number can be reduced by using structures (a standard technique for saving chosen plaintexts in differential attacks, see [5]). In the optimal case we can use structures of 2^p texts which contain about 2^{2p-1} pairs with differences from $\mathcal{P}$. In this case $2^{n-q}/2^{2p-1}$ structures are required, and the number of chosen texts used by this distinguishing attack is about $2^{n-p-q+1}$ (assuming that $2p < n-q+1$). Thus the higher is $p+q$ the better is the distinguisher based on the impossible event.

This paper is organized as follows: In Section 2 we propose attacks on IDEA [19]. We develop the best known attack on IDEA reduced to 3.5 rounds and the first attacks on 4 and 4.5 rounds, as described in Table 1. In Section 3 we show that this technique can also be applied to Khufu and Khafre [23]. Section 4 concludes the paper with a discussion of provable security of ciphers against differential attacks, and describes several impossible differentials of DES, FEAL, and CAST-256.

2 Cryptanalysis of IDEA

The International Data Encryption Algorithm (IDEA) is a 64-bit, 8.5-round non-Feistel block cipher with 128-bit keys, proposed by Lai and Massey in 1991 [19]. It is a modified version of a previous design by the same authors [18], with added strength against differential attacks [5].

Although almost a decade has passed since its introduction, IDEA resisted intensive cryptanalytic efforts [22, 9, 10, 12, 15, 8, 13]. Progress in cryptanalyzing round-reduced variants was very slow, starting with an attack on a two round variant of IDEA in 1993 [22] by Meier and leading to the currently best attack on 3.5 rounds published in 1997 [8] by Borst et.al. In [17, page 79] IDEA reduced to four rounds was claimed to be secure against differential attacks. Table 1 summarizes the history of attacks on IDEA and our new results described in this paper (all attacks in this table are chosen plaintext attacks). In addition to these attacks two relatively large easily detectable classes of weak keys were found: In [10] 2^{51} weak keys out of the 2^{128} keys were found to be detectable with 16 chosen plaintexts and 2^{17} steps using differential membership tests, and in [13] 2^{65} weak keys were found to be detectable given 20 chosen plaintexts with a negligible complexity under differential-linear membership tests. Still the chance of choosing a weak key at random is about 2^{-63} which is extremely low. Related key attacks [6] on 3.5 rounds [15] and on 4 rounds [13] of IDEA were developed but these are mainly of theoretical interest. Due to its strength against cryptanalytic attacks, and due to its inclusion in several popular crypto packages (such as PGP and SSH) IDEA became one of the best known and most widely used ciphers.

Before we describe the attacks we introduce our notation. IDEA is an 8.5-round cipher using two different half-round operations: key mixing (which we denote by T) and M-mixing denoted by $M = s \circ MA$, where MA denotes a multiplication-addition structure and s denotes a swap of two middle words.[4] Both MA and s are involutions. T divides the 64-bit block into four 16-bit words and mixes the key to the data using multiplication modulo $2^{16}+1$ (denoted by $\odot$) with $0 \equiv 2^{16}$ on words one and four, and using addition modulo 2^{16} (denoted by $\boxplus$) on words two and three. The full 8.5-round IDEA can be written as

$$IDEA = T \circ s \circ (s \circ MA \circ T)^8 = T \circ s \circ (M \circ T)^8.$$

We denote the input to the key mixing step T in round i by X^i, and its output (the input to M) by Y^i. The rounds are numbered from one and the plaintext is thus denoted by X^1. We later consider variants of IDEA with a reduced number of rounds which start with M instead of T. In these variants the plaintext is denoted by Y^1 (and the output of M is then X^2). See Figure 1 for a picture of one round of IDEA.

In the rest of this section we describe a 2.5-round impossible differential of IDEA, and a chosen plaintext attacks on IDEA reduced to 4 and 4.5 rounds

[4] As usual the composition of transformations is applied from right to left, e.g. MA is applied first, and the swap s is applied on the result.

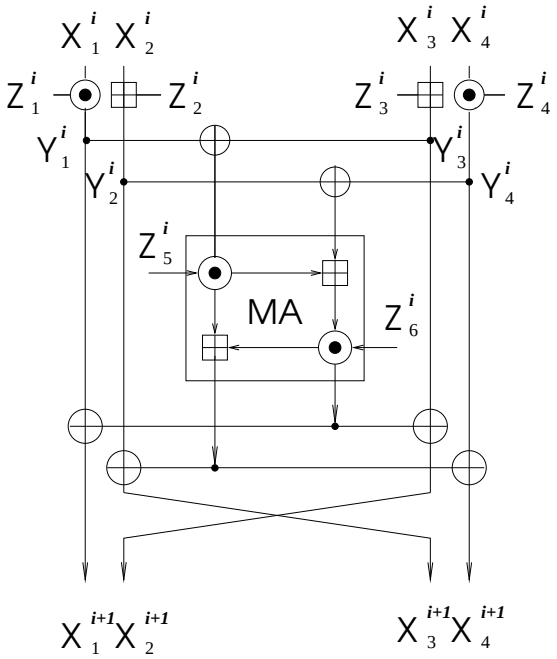

Fig. 1 One round of IDEA.

using this impossible differential, which are faster than exhaustive search. We also describe a similar attack on 3.5-rounds of IDEA, which is more than 2^{14} times faster than the best previously known attack [8] and which uses 2^{17} times less chosen plaintexts. One interesting feature of these attacks is that they are independent of many of the design details of IDEA: They work for any choice of the MA permutation, and for any order of the $\odot$ and $\boxplus$ operations in the key-mixing T. In addition they depend only marginally on the choice of the key-scheduling of IDEA.

2.1 A 2.5-round Impossible Differential of IDEA

Our main observation is that IDEA has a 2.5-round differential with probability zero. Consider the 2.5 rounds $M \circ T \circ M \circ T \circ M$. Then the input difference $(a, 0, a, 0)$ (where 0 and $a \neq 0$ are 16-bit words) cannot cause the output difference $(b, b, 0, 0)$ after 2.5 rounds for any $b \neq 0$. To prove this claim, we make the following observations:

1. Consider a pair with an input difference $(a, 0, a, 0)$ for $a \neq 0$. In such a pair, the inputs to the first MA-structure have difference zero, and the outputs of the first MA have difference zero. Thus, the difference after the first half-round $(s \circ MA)$ is $(a, a, 0, 0)$ (after the swap of the two middle words). After

the next half-round (T) the difference becomes $(c, d, 0, 0)$ for some $c \neq 0$ and $d \neq 0$.
2. Similarly, consider a pair with an output difference $(b, b, 0, 0)$ for $b \neq 0$ after 2.5 rounds. In such a pair the difference before the last half-round (M) is $(b, 0, b, 0)$, and the difference before the last T is of the form $(e, 0, f, 0)$ for some $e \neq 0$ and $f \neq 0$.
3. Therefore, if the input and output differences are both as above, the input difference of the middle half-round (M) is $(c, d, 0, 0)$, and the output difference of the same half-round is $(e, 0, f, 0)$. The difference before the swap of the two middle words is $(e, f, 0, 0)$. From these differences we conclude that the differences of the inputs to the MA-structure in the middle half-round is non-zero $(c, d) = (e, f)$, while the output difference is $(c \oplus e, d \oplus f) = (0, 0)$. This is a contradiction, as the MA-structure is a permutation. Consequently, there are no pairs satisfying both the input and the output differences simultaneously.

Due to symmetry there is another impossible 2.5-round differential, with input difference $(0, a, 0, a)$ and output difference $(0, 0, b, b)$.

2.2 An Attack on 3.5-Round IDEA

Consider the first 3.5 rounds of IDEA $T \circ (M \circ T)^3$. We denote the plaintext by X^1 and the ciphertext by Y^4. The attack is based on the 2.5-round impossible differential with two additional T half-rounds at the beginning and end, and consists of the following steps:

1. Choose a structure of 2^{32} plaintexts X^1 with identical X_2^1, identical X_4^1, and all possibilities of X_1^1 and X_3^1.
2. Collect about 2^{31} pairs from the structure whose ciphertexts satisfy $Y_3^{4\prime} = 0$ and $Y_4^{4\prime} = 0$.
3. For each such pair
   (a) Try all the 2^{32} possible subkeys of the first T half-round that affect X_1^1 and X_3^1, and partially encrypt X_1^1 and X_3^1 into Y_1^1 and Y_3^1 in each of the two plaintexts of the pair. Collect about 2^{16} possible 32-bit subkeys satisfying $Y_1^{1\prime} = Y_3^{1\prime}$. This step can be done efficiently with 2^{16} time and memory complexity.
   (b) Try all the 2^{32} possible subkeys of the last T half-round that affect X_1^4 and X_2^4, and partially decrypt Y_1^4 and Y_2^4 into X_1^4 and X_2^4 in each of the two ciphertexts of the pair. Collect about 2^{16} possible 32-bit subkeys satisfying $X_1^{4\prime} = X_2^{4\prime}$. This step can be done efficiently with 2^{16} time and memory complexity.
   (c) Make a list of all the 2^{32} 64-bit subkeys combining the previous two steps. These subkeys cannot be the real value of the key, as if they do, there is a pair satisfying the differences of the impossible differential.
4. Repeat this analysis for each one of the 2^{31} pairs obtained in each structure and use a total of about 90 structures. Each pair defines a list of about 2^{32}

incorrect keys. Compute the union of the lists of impossible 64-bit subkeys they suggest. It is expected that after about 90 structures, the number of remaining wrong key values is: $2^{64} \cdot (1 - 2^{-32})^{2^{31} \cdot 90} \approx 2^{64} \cdot e^{-45} \approx 0.5$ and thus the correct key can be identified as the only remaining value.

5. Complete the secret key by analyzing the second differential $(0, a, 0, a)$. Similar analysis will give 46 new key bits (16 bits out of 64 are in common with the bits that we already found, and two bits 17 and 18 are common between the 1st and 4th rounds of this differential). Finally guess the 18 bits that are still not found to complete the 128-bit secret key.

This attack requires about $2^{38.5}$ chosen plaintexts and about 2^{53} steps of analysis. This analysis requires only about 2^{48} memory (apart from the memory required to keep the plaintexts and the ciphertexts) when performed in a slightly different order.

2.3 An Attack on a 4-Round IDEA

The attack is also applicable to IDEA reduced to 4 rounds: $(M \circ T)^4$, from second to the fifth round (inclusive). We denote the plaintext by X^2 and the ciphertext by X^6. Depending on the starting round and on the differential being used ($(a, 0, a, 0)$ or $(0, a, 0, a)$), there is a varying amount of overlap between the subkey bits. In the case of our choice (from second to the fifth round, with the first differential), we will work with subkeys:

$$Z_1^2[97 \ldots 112], Z_3^2[26 \ldots 41], Z_1^5[76 \ldots 91], Z_2^5[92 \ldots 107], Z_5^5[12 \ldots 27], Z_6^5[28 \ldots 43],$$

these have 69 distinct key bits out of $6 \cdot 16 = 96$. The attack guesses the two subkeys Z_5^5, Z_6^5 of the last MA structure, and for each guess performs the previous attack on 3.5 round IDEA. More precisely:

1. For each guess of Z_5^5, Z_6^5:
   (a) Decrypt the last half round of all the structures, using the guessed subkeys.
   (b) For each structure find all pairs with zero differences in the third and fourth words, leaving about 2^{31} pairs per structure.
   (c) For each pair:
      i. Notice that at this point we already know Z_3^2 due to the subkey overlap. Thus we calculate the difference of the third words:

$$(Z_3^2 \boxplus X_3^2) \oplus (Z_3^2 \boxplus X_3^{2^*}),$$

      and find the key Z_1^2, which produces the same difference in the first words:

$$(Z_1^2 \odot X_1^2) \oplus (Z_1^2 \odot X_1^{2^*}).$$

      On average only one Z_1^2 is suggested per pair.

ii. Similarly find the pairs of keys Z_1^5 and Z_2^5 which cause equal differences at the 5th round. Since Z_1^2 and Z_2^5 share eleven key bits, we are left with about 2^5 choices of subkey pairs, and thus with about 2^5 choices of newly found 37 subkey bits. These choices are impossible.

(d) We need about 50 structures to filter out all the wrong keys (this is because we fix many key bits at the outer-most loop):

$$2^{37} \cdot \left(1 - \frac{2^5}{2^{37}}\right)^{2^{31} \cdot 50} \approx 2^{37} \cdot e^{-37} \approx 2^{-16}$$

2. After analyzing all the structures only a few possible subkey values remain. These values are verified using auxiliary techniques.

This attack requires about $50 \cdot 2^{32} \approx 2^{38}$ chosen plaintexts packed into structures as in the previous section. The total complexity of this attack consists of about $2^{32} \cdot 2^{38}$ half-round decryption (MA) steps which are equivalent to about 2^{67} 4-round encryptions plus about $2^{32} \cdot 2^{37} \cdot 2^5 \approx 2^{74}$ simple steps. When these steps are performed efficiently, they are equivalent to about 2^{70} 4-round encryption steps, and thus the total time complexity is about 2^{70} encryptions.

2.4 An Attack on a 4.5-Round IDEA

In this section we describe our strongest attack which can be applied to the 4.5 rounds of IDEA described by: $M \circ (T \circ M)^4$ which start after the first T half-round. We denote the plaintext by Y^1 and the ciphertext by X^6. In addition to the 64 key bits considered in the previous section we now need to find the subkeys of the two additional M half-rounds. We observe however, that only 16 of these key bits are new, and the other 48 bits are either shared with the set we found in the previous section, or are shared between the first and the last half-rounds. Therefore, it suffices to guess 80 key bits in order to verify whether the impossible differential occurs. These key bits are 12–43, 65–112, covering the subkeys:

$$Z_5^1[65 \ldots 80], Z_6^1[81 \ldots 96], Z_1^2[97 \ldots 112], Z_3^2[26 \ldots 41],$$

$$Z_1^5[76 \ldots 91], Z_2^5[92 \ldots 107], Z_5^5[12 \ldots 27], Z_6^5[28 \ldots 43].$$

The attack consists of the following steps:

1. Get the ciphertexts of all the 2^{64} possible plaintexts.
2. Define a structure to be the set of all 2^{32} encryptions in which X_2^2 and X_4^2 are fixed to some arbitrary values, and X_1^2 and X_3^2 range over all the possible values. Unlike the previous attacks, these structures are based on the intermediate values rather than on the plaintexts.
3. Try all the 2^{80} possible values of the 80 bits of the subkeys. For each such subkey
   (a) Prepare a structure, and use the trial key to partially decrypt it by one half-round with the keys Z_5^1 and Z_6^1 to get the 2^{32} plaintexts.

(b) For each plaintext find the corresponding ciphertext and partially decrypt the last two half-rounds by the trial subkeys (Z_5^5, Z_6^5 and Z_1^5, Z_2^5). Partially encrypt all pairs in the structure with the subkeys Z_1^2 and Z_3^2.
(c) Check whether there is some pair in the structure which satisfies the 64-bit condition $Y_1^{2\prime} = Y_3^{2\prime}$, $X_1^{5\prime} = X_2^{5\prime}$, $Y_3^{5\prime} = 0$, and $Y_4^{5\prime} = 0$.
(d) If there is such an impossible pair, the trial 80-bit value of the subkeys cannot be the right value.
(e) If there is no such pair in the structure, try again with another structure.
(f) If no pairs are found after trying 100 structures, the trial 80-bit value is the real value of the 80 bits of the key.

4. Assuming that a unique 80 bit value survives the previous steps, the remaining 48 bits of the key can be found by exhaustive search.

This attack requires 2^{64} plaintexts, and finds the key within 2^{112} steps using about 2^{32} memory. This is about 2^{16} times faster than exhaustive search. See Table 1 for a summary of our attacks on IDEA compared to the best previous attacks.

3 Attacks on Khufu and Khafre

Khufu and Khafre are two 64-bit block 512-bit key ciphers designed by Merkle [23] with a fast software implementation in mind. Khufu is faster than Khafre due to a smaller number of rounds but has a much slower key-setup. The strength of Khufu is based on key-dependent 8x32-bit S-boxes. These are unknown to an attacker and thus defy analysis based on specific properties of the S-boxes. The only additional way in which the key is used is at the beginning and at the end of the cipher, where 64-bit subkeys are XORed to the plaintext and to the ciphertext. The cipher is a Feistel cipher, so the input to a round is split into two 32-bit halves L and R. Each round consists of the following simple steps:

1. Use the least significant byte of L as an input to the S-box: $S[LSB(L)]$.
2. XOR the output of the S-box with R: $R = R \oplus S[LSB(L)]$.
3. Rotate L by several bytes according to the rotation schedule.
4. Swap L and R.

The S-box is changed every eight rounds in order to avoid attacks based on guessing a single S-box entry. The rotation schedule of Khufu for every eight rounds is: $2, 2, 1, 1, 2, 2, 3, 3$ (byte rotations to the right). Since our attack works equally well for any rotation schedule we simplify the description of the attack by assuming that all the rotations are by a single byte to the left. A description of this simplified version of Khufu can be found in Figure 2. Khafre differs from Khufu only in two aspects: its S-boxes are known, and it XORs additional 64-bit subkeys to the data every eight rounds. The best currently known attack on Khafre is by Biham and Shamir [5], which requires about 1500 chosen plaintexts for attacking 16 rounds, and about 2^{53} chosen plaintexts for attacking 24 rounds. The best attack on Khufu is by Gilbert and Chauvaud [11]. It requires about 2^{43}

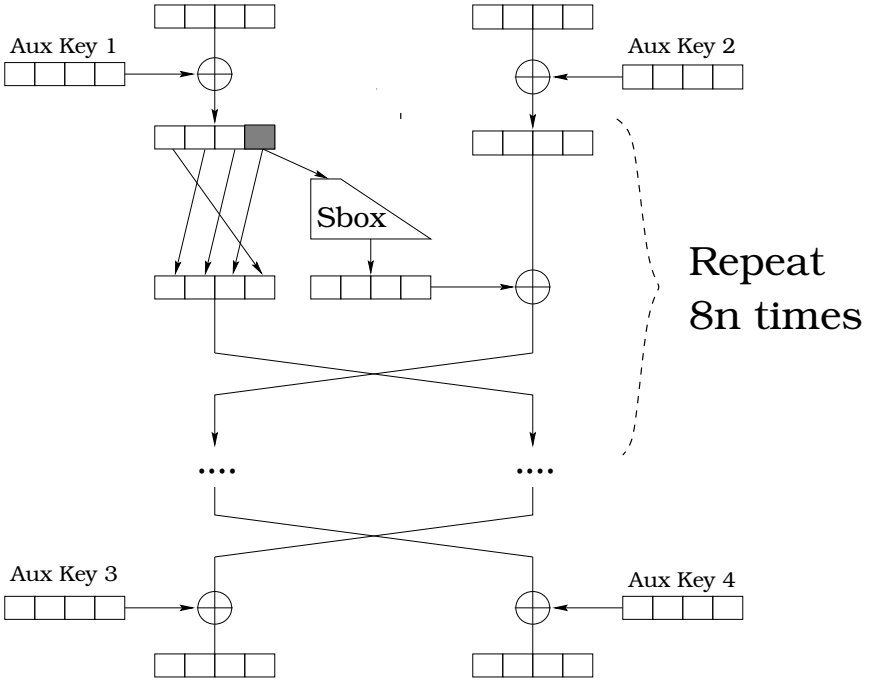

Fig. 2 Description of Khufu.

chosen plaintexts and 2^{43} operations (preliminary information on the secret key can be derived with about 2^{31} chosen plaintexts in 2^{31} steps). It is believed that Khufu is stronger than Khafre, since Khufu has secret key-dependent S-boxes, which prohibit attacks based on analysis of specific S-boxes.

Interestingly the approach described in this section is not very sensitive to the differences between these two ciphers, and works well for both of them since it is independent of the concrete choice of the S-boxes and (surprisingly) does not assume their knowledge by an attacker. We describe our attack on Khufu, and unless explicitly stated otherwise all the results hold for Khafre as well, usually with smaller complexities.

3.1 Impossible Differentials of Khufu

In this section we describe long impossible differentials for Khufu. The impossibilities in Khufu stem mainly from the fact that the avalanche effect of the difference can be postponed by eight rounds. This leads to many eight round differentials with probability one, whose concatenation is contradictory. Due to the byte-oriented structure of Khufu, these differentials come in sets of 256 or

larger, and allow tight packing into structures. We study mainly the differentials with an eight byte input difference 000000*0, where 0 denotes a byte with zero difference and * denotes a byte with arbitrary non-zero difference. However two byte and three byte input differences are possible as long as $p + q$ remains constant (see the relevant discussion in the Introduction). Notice that a XOR of two different S-box entries necessarily looks like ****, since the S-boxes of Khufu are built from four permutations. Let us study one of these differentials in some more detail.

The differential that we describe below spans 14 rounds of Khufu, and covers the set of 256 input differences and the corresponding set of impossible 2^{32} output differences. An 18-round differential can be obtained similarly, and will appear in the final version of this paper.

1. Consider a pair of inputs with difference 000000*0. After eight rounds of Khufu this difference turns into the difference ****00*0.
2. Similarly consider a pair with the output difference *00**00* after the 14th rounds. This output difference can only be derived from a difference 0**00**0 at the output of the 10th round. Thus in order for an input difference 000000*0 to cause output difference *00**00*, the necessary condition is that the difference ****00*0 at the input to the 9th round causes the difference 0**00**0 at the output of the 10th round. This may happen only if 00*0⊕****=00**, which is clearly impossible, since * is a non-zero difference.

For additional impossible differentials of Khufu with up to 20 rounds see Table 3 (these were observed experimentally on a small model of Khufu with 24-bit block and 3x12-bit S-boxes using 100 different keys). If these differentials hold for full 64-bit Khufu, then using the 20-round impossible differential from Table 3 it is possible to distinguish Khufu from a random cipher, with only about 2^{48} chosen plaintexts. This is the first cryptanalytic result for Khufu with more than 16 rounds.

By experimentally analyzing reduced models of Khufu we noticed that some differentials are impossible for fractions of the key-space, and not for all the keys. Below we describe some of the *key-dependent impossible differentials*[5] found on a 24-bit Khufu. Key-dependent differentials cover more rounds of Khufu, since they come from corresponding impossible differentials (with the same input/output conditions) by adding few rounds in the middle of Khufu. This way the contradiction in the middle becomes key-dependent. See Table 2 for examples of such differentials. In order to get the results for 24 rounds we tested 100 different keys, with 2^{21} structures of eight 24-bit plaintexts (each structure contains $8 \cdot 7/2 = 28$ pairs). In a random mapping one would expect to get about 30 pairs with difference in a single byte and about 180 pairs with differences in two bytes. If the key fraction for the full 64-bit Khufu is the same, then we can use the impossible differential for 16 rounds of Khufu (third line of Table 2) as

[5] Conditional (key-dependent) characteristics were studied in the case of conventional differential cryptanalysis in [3].

Rounds	Input	Output	Type	Key Fraction
14	000000*0	**0**00*	Impossible	14%
14	000000*0	*00***00	Impossible	10%
16	000000*0	*00**00*	Impossible	48%
18	000000*0	*00*000*	Impossible	64%
23	000000*0	0000000*	Impossible	58%
23	000000*0	000*0000	Impossible	86%
23	000000*0	*0000000	Impossible	19%
23	000000*0	000*000*	Impossible	2%
24	000000*0	000*0000	Impossible	19%

Table 2 Some Impossible Key-Dependent differentials of Khufu (derived from 24-bit model).

an efficient distinguisher of Khufu from a random cipher. We need about 2^{34} pairs with input difference 000000*0. Thus we can use 2^{27} chosen plaintexts packed into 2^{19} structures of 2^8 chosen plaintexts, each containing 2^{15} pairs. This data can be used to distinguish 16-round Khufu from a random permutation with 2^{27} chosen plaintexts and in 2^{27} steps using an array of 2^{16} of words with $1-(1-2^{-32})^{2^{34}} \approx 1-(\frac{1}{e})^4 \approx 0.98$ success probability for half of the keys.

3.2 Attacks on Khufu

We are aware of attacks on Khufu with more than 20 rounds that find the full description of the unknown S-boxes faster than via exhaustive search. However, the description of these attacks is too long for this submission, and will appear in the final version of this paper. Below we show an attack on a 16-round version of Khufu using the 15-round impossible differential shown in Table 3 (000000*0$\not\longrightarrow$*00**00*) from the 1st to the 15th round). Since the S-boxes are unknown, we can always assume that the bytes of the last subkey can be arbitrarily set to zero, yielding an equivalent (but modified) description of the corresponding S-boxes (and using a modified first subkey).

1. Encrypt structures of 256 plaintexts differing only in the 7th byte (we count the bytes of the block from left to right).
2. Check all the 2^{15} pairs contained in the structure and retain only those with zero difference in ciphertext bytes 5 and 6 (2^{-16} of all pairs are left). In addition we can discard a small number of pairs that have zero difference in byte 2 or 3.
3. Denote the inputs to the S-box used in the last round in a particular pair by i and j. Denote the ciphertext difference by $C' = C'_1, C'_2, \ldots, C'_8$. For each remaining pair we get the impossible condition on the two middle bytes of $S[i] \oplus S[j]$:

$$S[i]_2 \oplus S[j]_2 \neq C'_2 \quad \text{and} \quad S[i]_3 \oplus S[j]_3 \neq C'_3$$

Rounds	Input		Output	Type
14	000000*0	$\not\longrightarrow$	*00**00*	Impossible
14	00*000*0	$\not\longrightarrow$	*00*000*	Impossible
15	000000*0	$\not\longrightarrow$	*00**00*	Impossible
15	000000*0	$\not\longrightarrow$	*00*000*	Impossible
15	000000*0	$\not\longrightarrow$	*00**000	Impossible
15	000000*0	$\not\longrightarrow$	000**00*	Impossible
15	000000*0	$\not\longrightarrow$	*000*00*	Impossible
16	000000*0	$\not\longrightarrow$	000*000*	Impossible
16	000000*0	$\not\longrightarrow$	*000000*	Impossible
16	000000*0	$\not\longrightarrow$	000**000	Impossible
18	000000*0	$\not\longrightarrow$	000*0000	Impossible
18	000000*0	$\not\longrightarrow$	*0000000	Impossible
18	000000*0	$\not\longrightarrow$	0000000*	Impossible
20	000000*0	$\not\longrightarrow$	000*0000	Impossible

Table 3 Some Impossible differentials of Khufu (derived from 24-bit model).

About two structures (2^9 chosen plaintexts) are sufficient in order to find the first such constraint. However in order to actually derive an S-box from such constraints it seems that at least 2^{32} constraints are required. Thus the total data requirements of this attack rises to 2^{41} chosen plaintexts.

It is interesting to note that these attacks are particularly sensitive to redundancy in the plaintexts. If the distribution of the plaintexts is not uniform, then in some cases we can efficiently convert these chosen message attacks into known-plaintext and even ciphertext-only attacks, similarly to [7].

4 Concluding Remarks

Since the introduction of differential cryptanalysis in 1990 various approaches to the design of ciphers with provable security against this attack were suggested (see for example [2, 26, 21]). One way of proving a cipher to be secure against differential attack is to show an upper bound on the probability of the best differential. For example in [26] for a Feistel cipher with a bijective round function the probability of a three (or more) round differential was proved to be less than $2p^2$, where p is the highest probability for a non-trivial one-round differential.[6] This result makes it possible to construct Feistel ciphers with few rounds which are provably resistant against conventional differential cryptanalysis (for example, four rounds with best differential probability $\leq 2^{61}$). Examples of such ciphers are $\mathcal{KN}$ [26][7] and MISTY [20].

Notice however that any four and five round Feistel cipher has lots of impossible differentials, which are independent of the exact properties of the round

[6] A better bound of p^2 was proved later by Aoki and Ohta.

[7] Recently broken by high-order differential techniques [28, 14].

function (this was already observed in [16] in the case of DEAL cipher). For example, if the round function is bijective then for any value of $a \neq 0$, we have an impossible five-round differential $(a, 0) \not\to (a, 0)$, since it causes a zero output difference at the third round, but the round function is bijective and the input difference of this round is non-zero.

Using the properties of the round function one can usually extend the impossible differentials to cover even more rounds of a cipher. For example, for DES we can devise many 7-round impossible differentials: Denote by Θ the set of all the 24 one-bit and two-bit differences, that activate only one S-box after the expansion E. Let $\mu \in \Theta$ be one such difference. Consider 64-bit input difference $(\mu, 0)$. After the second round only four bits may differ. At the third round these four bits make at most six S-boxes active[8] and thus at the input to the fourth round specific 14-15 bits have difference zero and either one or two bits differ with probability one. On the other hand we may consider 64-bit output difference after the seventh round (without the final swap): $(\eta, 0)$, where $\eta \in \Theta$. Due to symmetry it also leads to 14-15 bits with difference of zero, at the input to the fourth round and either one or two bits with a difference of one. If for example μ and η activate the same S-box but $\mu \neq \eta$ then the differential $(\mu, 0) \to (\eta, 0)$ is impossible. Also if the bits of $(\mu, 0)$ which differ with probability one have an intersection with zero difference bits of $(\eta, 0)$ at the fourth round, then a such differential is also impossible.

FEAL [24, 25] has three 3-round characteristics with probability one. Using two such characteristics, with additional three rounds in between results in the following impossible differential (here $_x$ denotes a hexadecimal number):

$$(02000000_x, 8080000_x) \not\longrightarrow (02000000_x, 8080000_x).$$

In this case the characteristics with probability one ensure that the data after round three and before round seven has the same difference: $(02000000_x, 8080000_x)$. Therefore, the output difference of the F-function in round five is zero, and thus the input difference of F in this round is zero as well (since F in FEAL is a permutation). The input difference of F in round four is 02000000_x and the output difference must be 80800000_x which is impossible in the F function of FEAL (for example bit 19 of the output always differs for the specified input difference).

CAST-256 [1] has 20-round impossible differential (17 rounds forward and 3 rounds backwards, or vice versa) with inputs and outputs which differ only by one word.

Another general belief is that large expanding S-boxes (n bits of input, m bits of output, $n \ll m$) offer increased security against differential attacks. In particular 8x32 bit S-boxes are very popular, and can be found in Khufu, Khafre, CAST, Blowfish, Twofish and other ciphers. However, difference distribution tables of such S-boxes contain very few possible entries – at most 2^{16}, and all the other $2^{32} - 2^{16}$ pairs of input/output differences are impossible. This facilitates

[8] Due to the design principles of DES, the four output bits of an S-box influence two expanding and two non-expanding bits of S-boxes in the next rounds. Thus at most six S-boxes are activated at the next round.

the construction of impossible differentials and can thus make such schemes more vulnerable to the new type of attacks described in this paper.

References

1. C. M. Adams, *The CAST-256 Encryption Algorithm*, AES submission, available at `http://www.entrust.com/resources/pdf/cast-256.pdf`.
2. C. M. Adams, S. E. Tavares, *Designing S-boxes for Ciphers Resistant to Differential Cryptanalysis*, Proceedings of the 3rd symposium on State and Progress of Research in Cryptography, pp.181–190, 1993.
3. I. Ben-Aroya, E. Biham, *Differential Cryptanalysis of Lucifer*, Journal of Cryptology, Vol. 9, No. 1, pp. 21–34, 1996.
4. E. Biham, A. Biryukov, A.Shamir, *Cryptanalysis of Skipjack Reduced to 31 Rounds, Using Impossible Differentials*, Technion Technical Report CS0947, submitted to EUROCRYPT'99, 1998.
5. E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
6. E. Biham, *New Types of Cryptanalytic Attacks Using Related Keys*, J. of Cryptology, Vol.7, pp.229–246, 1994.
7. A. Biryukov, E. Kushilevitz, *From Differential Cryptanalysis to Ciphertext-Only Attacks*, Lecture Notes in Computer Science 1462, Advances in Cryptology – Proceedings of CRYPTO'98, pp.72–88, Springer-Verlag, 1998.
8. J. Borst, L. R. Knudsen, V. Rijmen, *Two Attacks on Reduced IDEA (extended abstract)*, Lecture Notes in Computer Science 1223, Advances in Cryptology – Proceedings of EUROCRYPT'97, pp.1–13, Springer-Verlag, 1997.
9. J. Daemen, R. Govaerts, J. Vandewalle, *Cryptanalysis of 2,5 Rounds of IDEA (extended abstract)*, Technical Report ESAT-COSIC Technical Report 93/1, Department of Electrical Engineering, Katholieke Universiteit Leuven, March 1993.
10. J. Daemen, R. Govaerts, J. Vandewalle, *Weak Keys of IDEA*, Lecture Notes in Computer Science 773, Advances in Cryptology – Proceedings of CRYPTO'93, pp.224–231, Springer-Verlag, 1994.
11. H. Gilbert, P. Chauvaud, *A chosen plaintext attack of the 16-round Khufu cryptosystem*, Lecture Notes in Computer Science 839, Advances in Cryptology – Proceedings of CRYPTO'94, pp.359–368, Springer-Verlag, 1994.
12. P. Hawkes, L. O'Connor, *On Applying Linear Cryptanalysis to IDEA*, Lecture Notes in Computer Science 1163, Advances in Cryptology – Proceedings of ASIACRYPT'96, pp.105–115, Springer-Verlag, 1996.
13. P. Hawkes, *Differential-Linear Weak Key Classes of IDEA*, Lecture Notes in Computer Science 1403, Advances in Cryptology – Proceedings of EUROCRYPT'98, pp.112–126, Springer-Verlag, 1998.
14. T. Jakobsen, *Cryptanalysis of Block ciphers with probabilistic Non-linear relations of Low Degree*, Lecture Notes in Computer Science 1462, Advances in Cryptology – Proceedings of CRYPTO'98, pp.212–222, Springer-Verlag 1998.
15. J. Kelsey, B. Schneier, D. Wagner, *Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES*, Lecture Notes in Computer Science 1109, Advances in Cryptology – Proceedings of CRYPTO'96, pp.237–251, Springer-Verlag, 1996.
16. L. R. Knudsen, *DEAL - A 128-bit Block Cipher*, AES submission, available at `http://www.ii.uib.no/~larsr/papers/deal.ps`, 1998.

17. X. Lai, *On the Design and Security of Block Ciphers*, Ph.D. thesis, Swiss Federal Institute of Technology, Zurich 1992.
18. X. Lai, J. L. Massey, *A Proposal for a New Block Encryption Standard*, Lecture Notes in Computer Science 473, Advances in Cryptology – Proceedings of EUROCRYPT'90, pp.389–404, Springer-Verlag, 1991.
19. X. Lai, J. L. Massey, S. Murphy, *Markov Ciphers and Differential Cryptanalysis*, Lecture Notes in Computer Science 547, Advances in Cryptology – Proceedings of EUROCRYPT'91, pp.17–38, Springer-Verlag, 1992.
20. M. Matsui, *New Block Encryption Algorithm MISTY*, Lecture Notes in Computer Science 1267, Fast Software Encryption - 4th International Workshop (FSE'97), pp.54–68, Springer-Verlag, 1997.
21. M. Matsui, *New Structure of Block Ciphers with Provable Security Against Differential and Linear Cryptanalysis*, Lecture Notes in Computer Science 1039, Fast Software Encryption - 3rd International Workshop (FSE'96), pp.205–218, Springer Verlag, 1996,
22. W. Meier, *On the Security of the IDEA Block Cipher*, Lecture Notes in Computer Science 765, Advances in Cryptology – Proceedings of EUROCRYPT'93, pp.371–385, Springer-Verlag, 1994.
23. R. C. Merkle, *Fast Software Encryption Functions*, Lecture Notes in Computer Science 537, Advances in Cryptology – Proceedings of CRYPTO'90, pp. 476 – 501, Springer-Verlag, 1990.
24. S. Miyaguchi, A. Shiraishi, A. Shimizu, *Fast Data Encryption Algorithm FEAL-8*, Review of Electrical Communications Laboratories, Vol. 36, N. 4, pp.433-437, 1988.
25. S. Miyaguchi, *FEAL-N specifications*, NTT, 1989.
26. K. Nyberg and L. R. Knudsen, *Provable Security Against a Differential Attack*, Journal of Cryptology, Vol.8, No.1, pp. 27-37, 1995.
27. *Skipjack and KEA Algorithm Specifications*, Version 2.0, 1998. Available at the National Institute of Standards and Technology's web-page, `http://csrc.nist.gov/encryption/skipjack-kea.htm`.
28. T. Shimoyama, S. Moriai, T. Kaneko, *Improving the High Order Differential Attack and Cryptanalysis of the KN Cipher*, Lecture Notes in Computer Science 1396, Proceedings of the First International Workshop on Information Security (ISW'97) (Japan), pp.32–42, Springer-Verlag 1997.