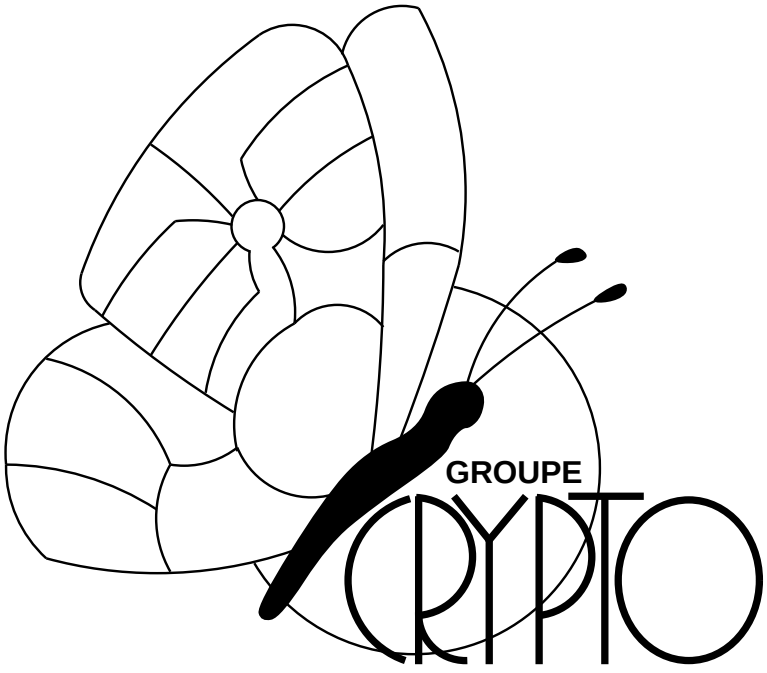
UCL
Université
catholique
de Louvain

REGARDS

UCL Crypto Group Technical Report Series

Impossible differential and square attacks: Cryptanalytic link and application to Skipjack

Gilles Piret · Jean-Jacques Quisquater



http://www.dice.ucl.ac.be/crypto/

Technical Report
CG–2001/4

Place du Levant 3
B-1348 Louvain-la-Neuve, Belgium

Phone: (+32) 10 472541
Fax: (+32) 10 472598

Impossible differential and square attacks: Cryptanalytic link and application to Skipjack

Gilles Piret Jean-Jacques Quisquater

November 2001

Département d'Électricité (DICE), Université catholique de Louvain
Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium
E-mail: {piret, jjq}@dice.ucl.ac.be

Abstract. This paper shows a surprising similarity between the construction of, respectively, impossible differentials and square distinguishers. This observation is illustrated by comparing two attacks on IDEA (Biham & al., FSE'99 [2], Nakahara & al., 2001 [7]). Using this similarity, we also derive a 16-round square distinguisher on Skipjack, directly based on the impossible differential attack presented in (Biham & al., Eurocrypt'99 [1]). However it is not the best square distinguisher we can find for Skipjack; this one is 19 rounds long. We use it to attack up to 24 rounds of Skipjack. Although this result is clearly not as good as those obtained by impossible differential on Skipjack, it must be pointed out that it is the first time that so big a part (24 rounds out of 32) of a non-square-like cipher is attacked using the square attack.
Finally, we discuss the strong and weak points of respectively impossible differential and square attacks.

1 Introduction

The square attack was introduced by J. Daemen, L. Knudsen, and V. Rijmen when they published the algorithm of the same name (see [5]). It was presented as a dedicated attack. Square attacks were then applied to reduced-round Rijndael and Crypton, which is not surprising, as their structure is very close to the one of Square. Four years later however, S. Lucks applied the square technique to a non-square-like cipher, namely Twofish [9]. This way he managed to break up to eight rounds of Twofish, which is at present the best known attack on it. Another example of application of the square attack to a cipher whose structure is not related to Square was recently given

CG–2001/4

by Nakahara & al. in [7]. Their attack was however less efficient than the best one known on IDEA (which is based on impossible differentials) (see [2]).

The impossible differential technique was developed by Biham & al. and presented in two papers, namely [1] and [2]. Since then, it was applied to several other block ciphers: for example Twofish ([6], [4]) and Mars [3].

We were intrigued by the fact that IDEA as well as Twofish were attacked both by square and impossible differential techniques. In the present paper we propose an explanation to this fact. The side effect of our observations is that impossible differential and square "characteristics" can frequently be converted one into the other. We illustrate this point by showing how the impossible differential distinguisher on Skipjack presented in [1] can be converted into a 16-round square distinguisher. However it is not the best square distinguisher existing for Skipjack. This one is 19 rounds long; we use it to attack up to 24 rounds of Skipjack.

This paper is organized as follows: In section 2 we recall the square attack principle and give some definitions. In section 3 we show the link existing between square attacks and impossible differentials. Section 4 illustrates these observations on IDEA, and derives a new distinguisher based on one of the square distinguishers given in [7]. Section 5 analyzes the impossible differential and square attacks on Skipjack. We present a 19-round square distinguisher on Skipjack, and apply it to attack up to 24 rounds. Section 6 is the conclusion.

2 The square attack

We will use the notion of "multiset" to describe an n-bit data channel (roughly speaking, a multiset is a set whose elements may appear several times). A **n-bit multiset** is a multiset whose elements belong to the set $\{0,1\}^n$. The following definitions are fundamental regarding to the square attack:

Definition 1. A n-bit multiset with $k \cdot 2^n$ entries is said **active** if any value in $\{0,1\}^n$ is found exactly k times.
A multiset is said **passive** if it contains only one fixed value.
A multiset is said **garbled** if it is neither active nor passive.

Note that we will allow us to write also "active/passive word" to designate an active/passive multiset. The basic principle of a square attack is, beginning with a set of plaintexts whose words are either active or passive, to trace active and passive words along the encryption process (the rules of

propagation for active and passive words will be detailed in the next section). More formally, we define the following terms:

Definition 2. The **state** of a word is whether it is active, active, or garbled. The **state** of the data at a certain point of an encryption is the description of the state of each word that is relevant for the attack.
A **square-like characteristic** is the description of the state of the data after each round.

The following notion is not necessary to attack IDEA or Skipjack, it is nevertheless very useful for attacks on other algorithms (S. Lucks uses it to attack Twofish for example [9]):

Definition 3. A multiset $\{x_i\}_{i=0..k\cdot 2^n-1}$ is said to be **balanced** whenever

$$\bigoplus_{i=0}^{k\cdot 2^n-1} x_i = 0$$

Balanced multisets have the following properties:

Theorem 4. *An active multiset is balanced. A passive multiset is balanced. The sum of two balanced multisets is a balanced multiset.*

3 Square characteristics versus impossible differential characteristics

Building an impossible-differential characteristic is most of the time all about tracing the zero and non-zero differences. Square attacks, as for them, are about tracing active and passive words. We observed that the rules of propagation are very similar for square attacks and impossible cryptanalysis attacks. More precisely, it appears that active words behave the same way as non-zero differences, while passive words behave just like zero differences. We summarize these observations in table 1, where:

- δ_0 (resp. $\Delta_{\neq 0}$) stands for a zero (resp. non-zero) difference.
- *Act*, *Pas*, *Bal* respectively denote an active, passive, and balanced multiset.
- $\oplus$ denotes the group operation of the cipher (which is often exclusive or, but it can also be addition *mod* 2^{32} for example).

Square attacks	Impossible differential attacks
$Pas \oplus Pas \rightarrow Pas$	$\delta_0 \oplus \delta_0 \rightarrow \delta_0$
$Act \oplus Pas \rightarrow Act$	$\Delta_{\neq 0} \oplus \delta_0 \rightarrow \Delta_{\neq 0}$
$Act \oplus Act \rightarrow Bal$	$\Delta_{\neq 0} \oplus \Delta_{\neq 0} \rightarrow ?$
$Act \xrightarrow{F} Act$	$\Delta_{\neq 0} \xrightarrow{F} \Delta_{\neq 0}$
$Pas \xrightarrow{F} Pas$	$\delta_0 \xrightarrow{F} \delta_0$
$Act \xrightarrow{f} ?$	$\Delta_{\neq 0} \xrightarrow{f} ?$
$Pas \xrightarrow{f} Pas$	$\delta_0 \xrightarrow{f} \delta_0$

Table 1: Parallelism between square and impossible differential characteristics

- F (resp. f) denotes a bijective (resp. non-bijective) function.

The interesting point with these observations is that it is often possible, given an impossible-differential characteristic, to build a corresponding square-like characteristic. And reciprocally, given a square-like characteristic, one can build an impossible-differential characteristic. In the next section, we will illustrate this technique by showing how two known characteristics on IDEA can be converted one into the other. Then in section 5 we will apply our technique to build a square-distinguisher for Skipjack, based on the impossible-differential distinguisher given in [1].

4 IDEA

The International Data Encryption Algorithm (IDEA) is a 64-bit block cipher using a 128-bit key, developed in 1991 by Lai and Massey. It is 8,5-rounds long. 2,5 rounds of IDEA are pictured in figure 1, where $\circledcirc$ represents multiplication modulo $2^{16}+1$ (with 2^{16} being interpreted as 0), $\boxplus$ represents addition modulo 2^{16} and $\oplus$ represents exclusive or. The $Z_i^{(j)}$ represent key material. We do not detail the key schedule, as it does not have any importance for our comments. We observe that one round is basically made out of two operations: key-mixing denoted by T, and M-mixing denoted by $M = s \circ MA$, where MA denotes a multiplication-addition structure and s denotes the swap of the two middle words.

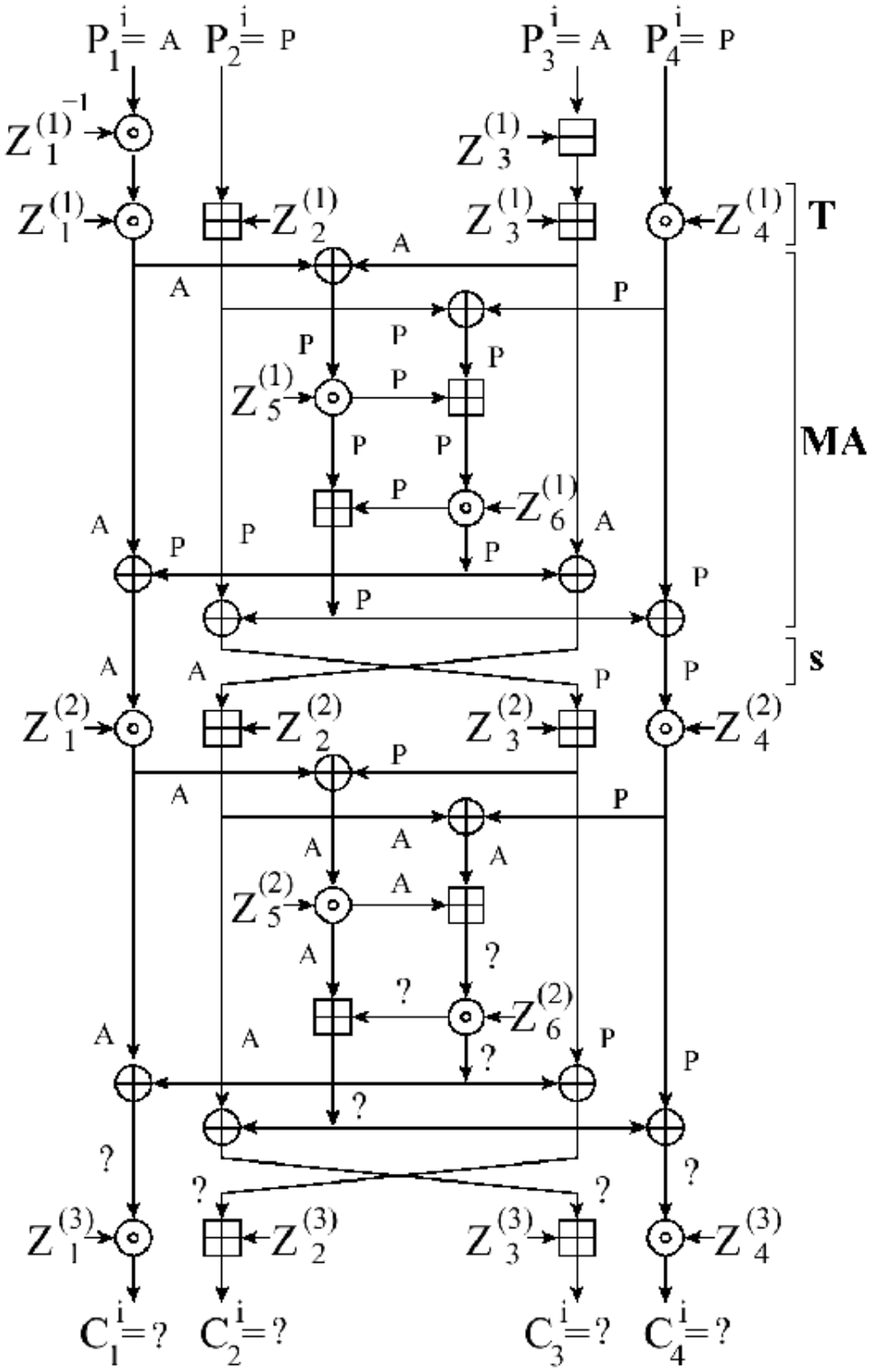


Figure 1: IDEA

4.1 An impossible differential distinguisher

An impossible-differential distinguisher for 2,5 rounds of IDEA, i.e. $M \circ T \circ M \circ T \circ M$, is presented in [2]. If we denote data during an encryption by quadruplets such as (X_1, X_2, X_3, X_4), the characteristic used can be pictured as:

$$(a,0,a,0) \xrightarrow{M} (a,a,0,0) \xrightarrow{T} (c,d,0,0) \overset{M}{\nrightarrow} (e,0,f,0) \xrightarrow{T} (b,0,b,0) \xrightarrow{M} (b,b,0,0)$$

where a, b, c, d, e, f are non-zero differences, and $\Delta_1 \rightarrow \Delta_2$ means that the difference Δ_1 always causes the difference Δ_2, while $\Delta_1 \nrightarrow \Delta_2$ means that the difference Δ_1 never causes the difference Δ_2.

4.2 A square distinguisher

In [7] Nakahara & al. presented a 1,5-round square distinguisher on IDEA, pictured in figure 1 (the multiplication and the substraction at the beginning represent a 0,5R-attack) . We will summarize it with 2 more words appended to the description of the state: it is thus represented as $(X_1, X_2, X_3, X_4; X_1 \oplus X_3, X_2 \oplus X_4)$.

$$\begin{array}{l}(A_1,p,A_1,p;p,p) \xrightarrow{M} (A_1,A_1,p,p;A,A) \xrightarrow{T} (A,A,p,p;A_2,A_3) \\ \xrightarrow{MA} (.,.,.,.;A_2,A_3)\end{array}$$

where $A, p, .$ denote respectively an active, passive, garbled word. The indices A_i emphasize on the fact that it is the same permutation that is used (in the same way as for impossible differential, for which the same letter always stood for the same difference). The interesting feature of the permutations being the same is that the sum of two such words is a passive word. Note that we just point an additional similarity that could be added to table 1: namely, while $\delta \oplus \delta \rightarrow 0$ (where δ denotes a given difference), the sum of two identical permutations is a constant.

4.3 Link between these two distinguishers

Looking at the two distinguishers just described, we observe that as far as only the first round (i.e. $T \circ M$) is concerned, one of them can be directly obtained from the other one by applying the parallelism we described in section 3. The impossible differential characteristic then applies the miss-in-the-middle technique to the second round, while the square characteristic pushes some active words through one more M function (remark that, for easiness in the notations, it is the state after the MA function that is given).

This difference is due to the fact that an impossible-differential is by nature based on miss-in-the-middle, while it is not possible to combine square attacks and miss-in-the-middle (we will give more details on this in section 5). Nevertheless the whole square characteristics can be converted into a truncated differential distinguisher (the . means that we do not know anything about the difference, a, c, d are non-zero differences):

$$(a,0,a,0;0,0) \stackrel{M}{\rightarrow} (a,a,0,0;a,a) \stackrel{T}{\rightarrow} (c,d,0,0;c,d) \stackrel{MA}{\rightarrow} (.,.,.,.;c,d)$$

Using our observations, we have thus converted a very selective 1,5-round distinguisher using batches of 2^{16} chosen plaintexts, into a less selective * 1,5 round distinguisher that can work with pairs of chosen plaintexts. Note furthermore that this transformation was done in an automatic way.

5 Skipjack

The algorithm Skipjack was developed by the NSA and was kept secret until 1998. The currently best known attack on Skipjack is an impossible differential cryptanalysis by Biham & al. (see [1]). We first build a square-like distinguisher on skipjack directly based on the impossible differential from [1]. We then show how this distinguisher can be improved.

5.1 Description of Skipjack

Skipjack is a 64-bit iterated blockcipher with 80-bit key, whose input is divided into four words of 16 bits. It is made out of 32 rounds of two types, called Rule A and Rule B (Skipjack applies 8 rounds of Rule A, followed by 8 rounds of Rule B, followed by another 8 rounds of Rule A and finally another 8 rounds of Rule B). In each round one of the four words passes through a bijective keyed transformation G, and at most two words are modified; furthermore a counter, which is incremented at each round, is xored to one of the words. The G function is a four-round Feistel permutation whose F-function is defined as an 8x8-bit S-box, and each round is keyed by 8 key bits.
The key schedule of Skipjack is very simple. Namely, four bytes of the key at a time are used to key each G permutation: the first four bytes are used to key the first G permutation, and each additional G permutation is keyed by the next four bytes cyclically, with a cycle of five rounds. In the remaining

*The probability for a random permutation to *fail* the test is about 2^{-15}

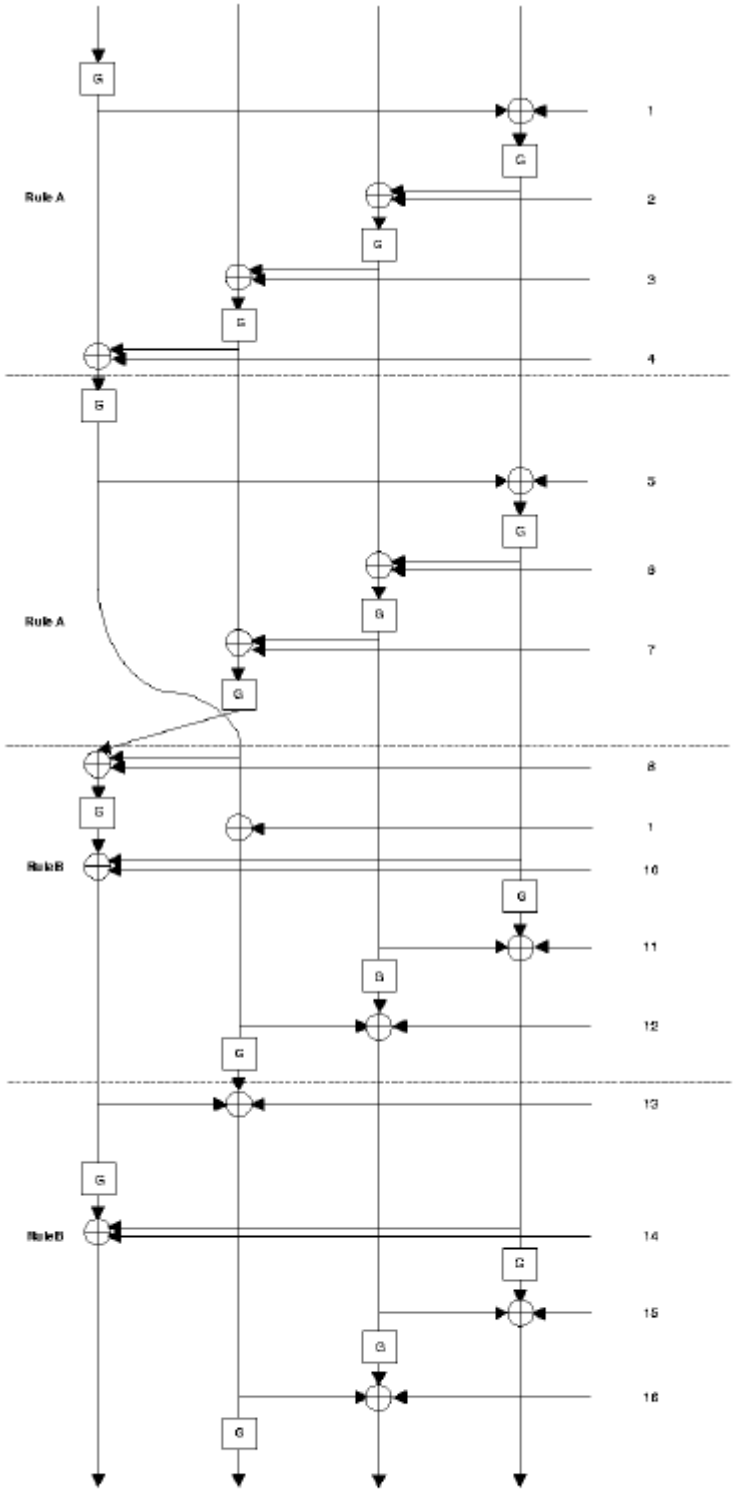


Figure 2: Skipjack

of this section we will denote by $k_{i \bmod 5}$ the key used in round i.
Figure 2 shows 16 rounds of Skipjack in an "unrolled" presentation.

5.2 A square-like distinguisher based on an impossible differential

In [1], Biham & al. show a 24-round distinguisher based on an impossible differential. They observe that a difference of $(0, a, 0, 0)$ (with $a \neq 0$) before round 5 always leads to a difference of $(c, d, e, 0)$ (with $c, d, e \neq 0$) after round 16. Considering the differential in the backward direction, they similarly note that if the difference after round 28 is of the form $(b, 0, 0, 0)$ (with $b \neq 0$), the difference after round 16 is of the form $(f, g, 0, h)$ (with $f, g, h \neq 0$). Because the differences $(c, d, e, 0)$ and $(f, g, 0, h)$ cannot both hold after round 16 (the authors talk about *miss-in-the-middle* to name this fact), we can conclude that there cannot be a pair with difference $(0, a, 0, 0)$ before round 5 and difference $(b, 0, 0, 0)$ after round 28.

Using the observations we made in section 3, we build a square-like distinguisher for the rounds 5-20, corresponding to the impossible differential found by Biham & al. Table 2 shows the state of the different words after each round. We note the four words obtained after round i by the quadruplet $(a_0^i, a_1^i, a_2^i, a_3^i)$; an active (respectively passive, balanced, garbled) word is denoted by A (respectively p, b, .). One can observe that the state after round 16 is (A, A, A, p), which is not a surprise, as it corresponds to the difference $(c, d, e, 0)$ after round 16 in the impossible-differential characteristic.

A good question is whether we can still apply a miss-in-the middle approach to a square-like characteristic. Indeed if the data after round 28 is in state (A, p, p, p), then the data after round 16 is in state (A, A, p, A) (we still refer to the impossible differential characteristic). Because data after round 16 cannot be simultaneously in state (A, A, A, p) and (A, A, p, A), we conclude that (p, A, p, p) before round 5 cannot cause (A, p, p, p) after round 28.
But the problem is the following: what is the probability, for a random permutation, that a batch of 2^{16} plaintexts with state (p, A, p, p) cause their ciphertexts to satisfy (A, p, p, p)? In fact, it is so small that we are almost sure that this event would never occur even if we consider all the 2^{48} possible batches! Building a distinguisher based on the miss-in-the-middle technique applied on square characteristics is therefore impossible.

Round number	a_0^i	a_1^i	a_2^i	a_3^i
Before 5	p	A	p	p
5	p	A	p	p
6	p	A	p	p
7	p	A	p	p
8	A	p	p	p
9	A	p	p	p
10	A	p	p	p
11	A	p	p	p
12	A	p	p	p
13	A	A	p	p
14	A	A	p	p
15	A	A	p	p
16	A	A	A	p
17	A	A	A	A
18	A	A	b	A
19	A	.	.	A
20	.	.	.	A
21	.	.	.	.

Table 2: 16-round square-like characteristic of Skipjack

5.3 A 19-round square-like distinguisher

Do we thus have to be satisfied with the 16-round distinguisher we just presented? In fact it is possible to do slightly better.

Indeed, suppose that instead of considering only the four 16-bit words $(a_0^i, a_1^i, a_2^i, a_3^i)$, we also consider the 32-bit words made up of the concatenation of two of the earlier 16-bit words; there are six of them, namely $(b_{01}^i, b_{02}^i, b_{03}^i, b_{12}^i, b_{13}^i, b_{23}^i)$. A detailed analysis shows us that the best distinguisher is a 19-round distinguisher between rounds 2 and 20, obtained with $(b_{01}^1, b_{02}^1, b_{03}^1, b_{12}^1, b_{13}^1, b_{23}^1) = (Act, ., ., ., Pas)$ as input. Table 3 shows the state of the different words after each round.

The following properties were intensively used to construct this table:

Theorem 5. *Let $\{(a_i, b_i)\}_{i=0\ldots 2^{32}-1}$ be a 32-bit active multiset, a_i and b_i being 16-bit words. Then $\{a_i\}_{i=0\ldots 2^{32}-1}$ is also an active multiset.*

Proof. By hypothesis, every value (i, j) appears once. Thus for every fixed $\bar{i}$, $(\bar{i}, .)$ appears exactly 2^{16} times (the right side taking whatever value). We conclude that $\{a_i\}_{i=0\ldots 2^{32}-1}$ is active.

Round number	b_{01}^i	b_{02}^i	b_{03}^i	b_{12}^i	b_{13}^i	b_{23}^i	a_0^i	a_1^i	a_2^i	a_3^i
Before 2	A	.	.	.	.	p	A	A	p	p
2	A	.	.	.	.	p	A	A	p	p
3	A	.	.	.	.	p	A	A	p	p
4	A	.	.	.	.	p	A	A	p	p
5	A	.	.	.	A	.	A	A	p	.
6	A	.	.	A	A	.	A	A	A	A
7	A	.	.	A	A	.	A	A	A	A
8	A	A	A	.	.	.	A	A	A	A
9	A	A	A	.	.	.	A	A	A	A
10	A	A	A	.	.	.	A	A	A	A
11	A	A	.	.	.	.	A	A	A	.
12	A	.	.	.	.	.	A	A	.	.
13	A	.	.	.	.	.	A	A	.	.
14	.	.	.	.	.	.	A	A	.	.
15	.	.	.	.	.	.	A	A	.	.
16	.	.	.	.	.	.	A	A	A	.
17	.	.	.	.	.	.	A	A	A	A
18	.	.	.	.	.	.	A	A	.	A
19	.	.	.	.	.	.	A	.	.	A
20	.	.	.	.	.	.	.	.	.	A
21	.	.	.	.	.	.	.	.	.	.

Table 3: 19-round square-like characteristic of Skipjack

Theorem 6. *Let $\{(a_i, b_i)\}_{i=0\ldots 2^{32}-1}$ be a 32-bit active multiset, a_i and b_i being 16-bit words (we will denote it more simply by (α, β)). Then the following multisets are also active:*

- $(\alpha, \beta \oplus \alpha)$
- $(\alpha, G(\beta))$*, with G a bijective function.*

Proof. This result is an immediate consequence from the fact that $(a, b) \rightarrow (a, b \oplus a)$ and $(a, b) \rightarrow (a, G(b))$ are both bijections.

We also used the following theorem to prove that a_2^{16} and a_3^{17} are active, by expressing them as functions of a_0^5 and a_1^5.

Theorem 7. *Let $\{(a_i, b_i)\}_{i=0\ldots 2^{32}-1}$ be a 32-bit active multiset, a_i and b_i being 16-bit words. Let $H : \{0,1\}^{32} \rightarrow \{0,1\}^{16}$ be a function such that $\forall \bar{a} : H_{\bar{a}}(b) := H(\bar{a}, b)$ is a bijection. Then $H((\alpha, \beta))$ if an active multiset.*

Proof. For any given $\bar{a}$, $\{H(\bar{a}, i)\}_{i=0\ldots 2^{16}}$ is an active multiset, as it is the image of an active multiset by a bijection. Considering all these $\bar{a}$, it is clear from the definition that the resulting multiset will be active.

One should ask whether it is possible to derive an impossible differential from our new square characteristic. In fact it is not the case, because theorems 5 and 7 have no impossible differential counterpart.

On the same wavelength, the utility of the notion of *balance* presented in section 2 is the fact that the sum of two active words is a balanced word. This property has no impossible differential counterpart: we cannot say anything about the sum of two non-zero differences $\Delta_{\neq 0}$. Thus a square characteristic using balance cannot be translated into an impossible differential characteristic.

5.4 Two attacks on respectively 22 and 24 rounds of Skipjack using our distinguisher

5.4.1 Attack on 22-round Skipjack

We first present a very simple attack. It is able to break a 22-round Skipjack, from round 2 to round 23, using 2^{32} chosen plaintexts. The attack proceeds as follows (we keep the original round numbers for easiness):

1. We choose the 2^{32} plaintexts of the form $\{(a_i, b_i, c, d)\}_{i=0\ldots 2^{32}-1}$. Note that $\{(a_i, b_i)\}_{i=0\ldots 2^{32}-1}$ is an active multiset.

2. We guess the key k_1, and compute the value $G_{k_1}^{-1}(t)$ for each t once and for all.

3. The value $a_0^{19} = G_{k_1}^{-1}(a_0^{23}) \oplus a_1^{23} \oplus a_2^{23} \oplus rk_{20} \oplus rk_{23}$ is computed for each ciphertext (by rk_i we denote the i^{th} round constant). 2^{16} counters are maintained, one for each possible value of a_0^{19}. Once one of the counters exceeds 2^{16}, we can conclude that a_0^{19} is not an active word, and thus that the key guess was wrong.

4. Return to step (2) until the test in (3) succeeds.

It is worth noting that the distinguisher used is very selective, as the event we test is extremely unlikely to occur for a random permutation[†]. Thus we can bet that all subkeys but the good one will be discarded with a single batch.

The average complexity of this attack is $22 \cdot 2^{32} + 2^{31}\text{keys} \cdot 2^{16} \cong 2^{47}$ G-computations, against about $2^{83,5}$ G-computations for exhaustive search.

5.4.2 Attack on 24-round Skipjack

It is possible to gain two more rounds by guessing on 48 key bits instead of 32. More precisely, we guess the two keys k_1 and k_4, that are overlapping on 16 bits. However we now need 2^{48} chosen plaintexts. We can then attack the first 24 rounds of Skipjack as follows:

1. We choose the 2^{48} plaintexts of the form $\{(a_i, b_i, c, d_i)\}_{i=0\ldots 2^{48}-1}$.

2. We guess the keys k_1 and k_4, and compute the values $\{G_{k_1}(t)\}_{t=0\ldots 2^{16}-1}$ and $\{G_{k_4}(t)\}_{t=0\ldots 2^{16}-1}$ once and for all.

3. It is now easy to select 2^{32} plaintexts such as the data after round 1 has state (A, A, p, p). We then compute the value $a_0^{19} = G_{k_1}^{-1}(a_1^{24}) \oplus G_{k_4}^{-1}(a_0^{24}) \oplus a_2^{24} \oplus rk_{20} \oplus rk_{23}$ for each of them, and perform the same kind of test than in the previous attack.

4. Return to step (2) until the test in (3) succeeds.

The average complexity of this attack is $24 \cdot 2^{48} + 2^{47} \cdot 2^{16} + 2^{31} \cdot 2^{16} \cong 2^{63}$ G-computations.

[†]It is exactly the contrary with impossible differentials, for which the tested event (i.e. that the outputs do **not** have a given difference) is very likely to occur.

6 Conclusion

In this paper we showed how strong is the link between square and impossible differential characteristics. Although the similarity we showed is factual rather than conceptual, it is nevertheless important. Indeed, one conclusion of this paper that must be retained is that for every impossible differential attack, one should try to convert it into a square attack, and vice versa. A good illustration of this was given in section 4, where we showed that one of the square characteristics presented in [7] could have been automatically found from the Miss-in-the-middle attack developed in [2], by using our observations.

However each of these two techniques have strong and weak points, that make one of them more convenient for such or such algorithm. One of the strong points of square attacks is that the sum of two active words still has this remarkable property, that is called *balance*. Another interesting specificity of the square attack is the fact we mentioned in theorem 5, namely that any subword of an active word is itself active. These two points, that have no counterpart in impossible differential attacks, are very useful to build the longest characteristic possible.

However impossible differentials have by essence a great advantage: they are constructed using the miss-in-the-middle technique, that virtually doubles the number of rounds attacked compared to the square attacks. We have seen that the miss-in-the-middle technique is not applicable to the square attack.

Therefore our prognostic is that impossible differentials will globally remain a more powerful tool for the cryptanalyst than the square attack, although the latter will sometimes be a better choice than the former.

To demonstrate our assertions, we also tried to apply the square attack to Skipjack. Skipjack is not a square-like cipher, and the best known attack on it uses the impossible-differential technique. Our results are clearly not so good as those obtained by impossible differential. On the other hand, it must be pointed out that it is the first time that so big a part of a non-square-like cipher is attacked using the square attack: while Lucks attacks 8 out of 16 rounds of Twofish using a 6-rounds distinguisher ([9]), and Nakahara & al. attack 2,5 out of 8 rounds of IDEA using a 1,5-round distinguisher ([7]), we attack 24 out of 32 rounds of Skipjack with a 19-rounds distinguisher. This tends to make us optimistic about the ability of square attacks to really run through a cipher.

References

[1] E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In J. Stern, editor, *Advances in Cryptology – Eurocrypt'99*, volume 1592 of LNCS, pages 12–23, Berlin, 1999. Springer-Verlag.

[2] E. Biham, A. Biryukov, and A. Shamir. Miss in the middle attacks on idea, khufu, and khafre. In L.R. Knudsen, editor, *Fast Software Encryption (FSE '99)*, volume 1636 of LNCS, pages 124–138, Berlin, 1999. Springer-Verlag.

[3] E. Biham and V. Furman. Impossible differential on 8-round MARS' core. In *The Third AES Candidate Conference*, pages 186–194, 2000.

[4] E. Biham and V. Furman. Improved impossible differentials on twofish. In B. Roy and E. Okamoto, editors, *Proceedings of Indocrypt 2000*, volume 1977 of LNCS, pages 80–92, Berlin, 2000. Springer-Verlag.

[5] J. Daemen, L. Knudsen, and V. Rijmen. The block cipher square. In E. Biham, editor, *Fast Software Encryption (FSE '97)*, volume 1267 of LNCS, pages 149–165. Springer-Verlag, 1997.

[6] N. Ferguson. Impossible differentials in twofish. In *Twofish technical report 5*. Counterpane Systems, October 1999.

[7] J. Nakahara Jr, P. S.L.M. Barreto, B. Preneel, and al. Square attacks on reduced-round pes and idea block ciphers. Available at http://eprint.iacr.org/complete/.

[8] L.R. Knudsen, M.J.B. Robshaw, and D. Wagner. Truncated differentials and skipjack. In M. Wiener, editor, *Advances in Cryptology – Crypto'99*, volume 1666 of LNCS, pages 165–180, Berlin, 1999. Springer-Verlag.

[9] S. Lucks. The saturation attack - a bait for twofish. In *Preproceedings of FSE 2001*, 2001.