Flaws in differential cryptanalysis of Skipjack

Louis Granboulan*

École Normale Supérieure
Louis.Granboulan@ens.fr

Abstract. This paper is motivated by some results presented by Knudsen, Robshaw and Wagner at Crypto'99 [3], that described many attacks of reduced versions of Skipjack, some of them being erroneous.
Differential cryptanalysis is based on distinguishers, any attack should prove that the events that triggers the analysis has not the same probability for the cipher than for a random function. In particular, the composition of differential for successive parts of a cipher should be done very carefully to lead to an attack.
This revised version of the paper includes the exact computations of some probabilities and repairs the attack of the first half of Skipjack.

1 What is differential cryptanalysis

Chosen plaintext attacks. If we have a "black box" containing a symmetric block cipher, we are able to encrypt anything we want. The goal of the attack is to decrypt some given ciphertext, or even better to retrieve the key. A partial success is obtained if we have a distinguisher, i.e. a technique that gives some information about what is in the box (e.g. the algorithm used).

Looking at differences. In order to check the security of a block cipher under chosen plaintext attacks, we can make statistical tests on the output when the input is cleverly chosen. The differential cryptanalysis [2] looks at the difference in the output of the cipher when a pair of input texts with some particular difference (XOR) is enciphered. If the pair of input texts is randomly chosen with their difference following some special distribution of probability, the difference of the outputs may give some information about what is inside.

Building a distinguisher using a differential. More precisely, if we know that, for some keys the input of two different plaintexts with a difference in the subset Δ gives two ciphertexts with a difference in the subset Δ^* with non trivial probability p (this is called a *differential* of probability p, the common notation is $\Delta \to_p \Delta^*$), then we are able to distinguish two black boxes, one with

* Part of this work has been supported by the CELAR, part of this work has been supported by the Commission of the European Communities through the IST Programme under Contract IST-1999-12324 (NESSIE).

the given cipher and the other with a random permutation. Formally, we fix the key and we take probabilities over all pairs (c, c') of cleartexts (or equivalently over all pairs (e, e') of ciphertexts, since the cipher is a permutation). Then $p = \Pr[e \oplus e' \in \Delta^*/c \oplus c' \in \Delta] = \Pr[c \oplus c' \in \Delta/e \oplus e' \in \Delta^*]\frac{\Pr[e \oplus e' \in \Delta^*]}{\Pr[c \oplus c' \in \Delta]}$. Regular differential cryptanalysis is looking for probability close to 1. Impossible cryptanalysis [1] is looking for probability 0. The "trivial probability" is the expected probability p^* that the differential holds for a random permutation. It is the probability that a random value is in Δ^*.

In practice, a regular differential cryptanalysis encrypts n independant random pairs of plaintexts (with $\frac{1}{p} < n < \frac{1}{p^*}$). If one of the pair of ciphertexts has difference in Δ^*, we recognise the cipher not being a random permutation. The probability that the encryption of n pairs of plaintexts produces no pair with difference in Δ^* is less than e^{-np} and the probability that a set of n random pairs of texts contains a pair with difference in Δ^* is less than np^*. If we need better probability of success, we can encrypt more pairs and have a threshold greater than one to decide if the black box is the cipher ; exact probabilities of success can be computed with Chernoff bounds.

Finding weak keys. If the differential holds only for some subset of the keys, the distinguisher allows to detect these keys.

Finding the key of the last rounds with reduced rounds differentials. Most block ciphers are based on a succession of identical rounds, that differ only by the subkey used. The first and last rounds may be different.

If we find a differential (a distinguisher) for the cipher reduced to all but a few last rounds, we can guess with non trivial probability what is the input difference for these few last rounds. Since we exactly know the output, we might be able to find the subkeys used in those rounds. Part of the analysis may be done using the structural properties of how the key bits are used in those rounds and part of the analysis may be done by exhaustive search.

The probability of success is deduced from the gap between the probability p of the differential and the trivial probability p^*. Detailed and practical analysis has been done e.g. in [2].

Composition of differentials. When we can split the cipher in two (ore more) successive ciphers (this is the case with most ciphers, putting the breakpoint between two internal rounds), a very tempting tool is to combine a differential for the first part and one for the second part. This is called a *differential characteristic* and the notation will be $\Delta \to \Delta^\times \to \Delta^*$.

The probability of the differential $\Delta \to \Delta^*$ is greater than or equal to the probability of the differential characteristic $\Delta \to \Delta^\times \to \Delta^*$.

Warning : the probability of the differential characteristic can be unrelated to the probabilities of $\Delta \to \Delta^\times$ and $\Delta^\times \to \Delta^*$. The very simple example below illustrate this fact. $f : (a, b, c) \mapsto (a, b, (a\&b) \oplus c)$. An input difference `100` to f

give an output difference of `100` with probability $1/2$ and an output difference of `101` with probability $1/2$. However the differential characteristic $\texttt{100} \rightarrow_{1/2} \texttt{100} \rightarrow_{1/2} \texttt{100}$ has probability 1 and the differential characteristic $\texttt{100} \rightarrow_{1/2} \texttt{100} \rightarrow_{1/2} \texttt{101}$ has probability 0.

Markov ciphers [4] have the property that the probability of the differential characteristic $\Delta \rightarrow \Delta^{\times} \rightarrow \Delta^{*}$ is equal to the product of the probabilities of $\Delta \rightarrow \Delta^{\times}$ and $\Delta^{\times} \rightarrow \Delta^{*}$.

Finding the key of the first rounds : filtering and counting. Of course, finding the key of the last rounds with a chosen plaintext attack is similar to finding the key of the first rounds with a chosen ciphertext attack. But we limit ourself to the chosen plaintext attacks.

If we have a differential $\Delta^{\times} \rightarrow \Delta^{*}$ for the cipher reduced to all but some first rounds, and another differential $\Delta \rightarrow \Delta^{\times}$ for those rounds, then we use the differential characteristic $\Delta \rightarrow \Delta^{\times} \rightarrow \Delta^{*}$ to make an attack as follows.

The cryptanalysis will use (random) pairs of cleartexts having difference in Δ. The filtering selects all pairs of cleartexts such that the ciphertexts have difference in Δ^{*}. Let p be the probability of $\Delta^{\times} \rightarrow \Delta^{*}$, q the probability of $\Delta \rightarrow \Delta^{\times}$, p^{*} the probability of $\Delta \rightarrow \Delta^{*}$. and q^{*} the probability of $\Delta \rightarrow \Delta^{\times} \rightarrow \Delta^{*}$. If q^{*}/q is substantially greater than p^{*}, the filtering will increase the probability that a pair of cleartexts have their difference in $\Delta^{\times}$ after the first rounds. For a Markov cipher $q^{*} = pq$ and the condition rewrites to $p \gg p^{*}$. We name it the **filtering condition**. If $p = p^{*}$, then the highest counter has no reason to be related to the value of the key. The probability of the second differential should not be trivial.

To find the key used in the first part of the cipher, we build a table of counters indexed by all the possible values of this key. For each filtered pair (following $\Delta \rightarrow \Delta^{*}$), we increase the counters corresponding to all the values that lead to a difference in $\Delta^{\times}$ after the first rounds. The attack works because the highest counter after looking at all pairs should correspond to the value of the key. This is the **counting hypothesis**. It is not implied by the filtering condition.

2 Example: *Truncated Differentials and Skipjack*

Overview. Knudsen, Robshaw and Wagner presented at Crypto'99 [3] a paper that looks for differentials in Skipjack. They are interested in differentials for the general structure of the algorithm without looking at the details of the "G-boxes" and how the key is used. They propose five attacks of reduced variants of Skipjack:

- Section 4.1 attacks the first 16 round with a composition of a 4-rounds differential and a 12-rounds differential. The differential is used to find the key of the first round.
- Section 4.2 attacks the middle 16 rounds with a distinguisher for the first 12 of them (reduced rounds attack).

- Section 4.3 attacks the last 28 rounds with a composition of a 4-rounds differential and a 24-rounds differential (which is obtained by combining three 8-rounds differentials). The differential is used to find the key of the first round.
- Section 5.1 attacks the middle 24 rounds with a boomerang attack meeting in the middle.
- Section 5.2 is a variant of the previous one, for the middle 25 rounds.

Both attacks of sections 4.1 and 4.3 have the same flaw : the key found by the highest counter is not related to the key of the first round, due to the use of a differential with trivial probability. Then we will look at the boomerang attack of section 5.1, and show that it has a similar flaw.

Notations. We take the notations of [3]. The two different types of rounds of Skipjack are noted τ_A and τ_B. Skipjack is working on blocks of 64 bits splitted in four 16-bits words. The notation for some subset Δ will be $(0, a, a, b)$ for example, indicating that the difference in the first 16-bits word is zero, that the differences in the second and third 16-bits words are equal and non-zero and that the difference in the fourth 16-bits word is non-zero.

Section 4.1. The authors consider the following 16 rounds differential :

$$(a, b, 0, c) \xrightarrow{4\tau_A}_{2^{-32}} (0, d, 0, 0) \xrightarrow{4\tau_A 8\tau_B}_{1} (e, f, g, 0),$$

which is the composition of two differentials and has probability at least 2^{-32}. But we can notice that the differential for the first four rounds is built with the composition $(a, b, 0, c) \xrightarrow{\tau_A}_{2^{-16}} (0, c, b, 0) \xrightarrow{3\tau_A}_{2^{-16}} (0, d, 0, 0)$.

To attack the key of the first round, they use the filtering and counting attack we described before, with the differential :

$$(a, b, 0, c) \xrightarrow{\tau_A}_{2^{-16}} (0, c, b, 0) \xrightarrow{7\tau_A 8\tau_B}_{2^{-16}} (e, f, g, 0).$$

This attack does not work, because the second differential has trivial probability. The attack could be used to find simultaneously the subkeys of the first four rounds, but they use all the key. It might be corrected by looking at the G-boxes and computing more precisely the probability of $(0, c, b, 0) \xrightarrow{7\tau_A 8\tau_B} (e, f, g, 0)$ and $(a, b, 0, c) \xrightarrow{8\tau_A 8\tau_B} (e, f, g, 0)$. This is done in the annex.

Section 4.3. The authors consider the following 28-rounds differential :

$$(a,b,0,c) \xrightarrow{4\tau_A}_{2^{-16}} (d,e,0,0) \xrightarrow{8\tau_B}_{2^{-16}} (f,g,0,h) \xrightarrow{8\tau_A}_{2^{-32}} (i,i,0,0) \xrightarrow{8\tau_B}_{1} (j,k,l,0),$$

which is the composition of four differentials. We notice that each of them has non trivial probability, with the exception of $(d, e, 0, 0) \xrightarrow{8\tau_B}_{2^{-16}} (f, g, 0, h)$ which cannot distinguish the cipher $8\tau_B$ from a random cipher. The authors want to use this 28-rounds differential to get some information about the key used in its first round, but it is even not possible if the cipher is restricted to the first twelve rounds of this differential. Indeed, even if someone gives us the value $(f, g, 0, h)$, the differential $(a, b, 0, c) \xrightarrow{4\tau_A}_{2^{-16}} (d, e, 0, 0) \xrightarrow{8\tau_B}_{2^{-16}} (f, g, 0, h)$, which can be rewritten $(a, b, 0, c) \xrightarrow{\tau_A}_{2^{-16}} (0, c, b, 0) \xrightarrow{3\tau_A 8\tau_B}_{2^{-16}} (f, g, 0, h)$, has a second part with trivial probability.

Section 5.1. The authors consider the following 12-rounds forward differential $\Delta = (0, a, 0, 0) \xrightarrow{4\tau_A 8\tau_B}_1 \Delta^* = (c, d, e, 0)$ and the following 12-rounds backward differential $\nabla = (f, 0, 0, 0) \xrightarrow{4\tau_B^{-1} 8\tau_A^{-1}}_1 \nabla^* = (i, h, 0, j)$ that always hold, and build a boomerang attack. Boomerang attacks are chosen-plaintext, adaptive chosen-ciphertext attacks that allow to detect the occurence of some differences in the middle. The attack builds pairs such that $P \oplus P' \in \Delta$, encrypts them to C and C', chooses D and D' such that $C \oplus D \in \nabla$ and $C' \oplus D' \in \nabla$, decrypts them to Q and Q'. The result is a quartet of plaintext/ciphertext pairs that looks good if $Q \oplus Q' \in \Delta$. Good looking quartets have probability 2^{-48} for a random cipher. We will denote $\bar{P}$, $\bar{P}'$, $\bar{Q}$ and $\bar{Q}'$ the results of encryption by half of the cipher. Right quartets have $\bar{P} \oplus \bar{P}' \in \Delta^*$, $\bar{Q} \oplus \bar{Q}' \in \Delta^*$, $\bar{P} \oplus \bar{Q} \in \nabla^*$ and $\bar{P}' \oplus \bar{Q}' \in \nabla^*$.

The authors compute the probability for a quartet of being a right one. The two differentials have probability one, so we have $\bar{P} \oplus \bar{P}' \in \Delta^*$, $\bar{P} \oplus \bar{Q} \in \nabla^*$ and $\bar{P}' \oplus \bar{Q}' \in \nabla^*$ with probability one. The conclusion (footnote in the article) is that $\bar{Q} \oplus \bar{Q}' \in \Delta^*$ happens with probability 2^{-16}. The backward differential $\Delta^* \to \Delta$ having probability 2^{-32} the conclusion of [3] is that right quartets have probability 2^{-48}.

Their error is that they expect two good looking quartets in 2^{48} : one right and one wrong, and that is what distinguishes Skipjack from a random cipher. But with Skipjack (reduced to the middle twenty-four rounds) all good looking quartets are right one, because both differentials $\Delta \to \Delta^*$ and $\nabla \to \nabla^*$ have probability one.

We consider that this mistake is similar to the error in sections 4.1 and 4.3, in the sense that the occurence of some event should not only have interesting probability, but this event should be related to the input of the analysis. If the property $\bar{Q} \oplus \bar{Q}' \in \Delta^*$ had depended on $\bar{P}$ and $\bar{P}'$, the attack could have worked.

References

1. Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *Advances in Cryptology – EUROCRYPT'99*, volume 1592 of *LNCS*, pages 12–23, Prague, May 1999. Springer-Verlag.
2. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

3. Lars R. Knudsen, M.J.B. Robshaw, and David Wagner. Truncated differentials and skipjack. In Michael Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *LNCS*, pages 165–180, Santa-Barbara, California, August 1999. Springer-Verlag.
4. Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald Watts Davies, editor, *Advances in Cryptology, proceedings of Eurocrypt'91*, volume 547 of *LNCS*, pages 17–38, Brighton, UK, April 1991. Springer-Verlag.

A Attacking Skipjack reduced to the first 16 rounds

Lemma 1. *We start with N values $(\alpha_i)_{i=1..N}$ taken uniform randomly and independantly from K possible values. We choose randomly two of them α_i and α_j. The expected value for the probablility of $\alpha_i = \alpha_j$ is $\pi = \frac{K+N-1}{NK^2}$. We remark that if $N = K$ then $\pi \simeq \frac{2}{K}$ and if $N = K^2$ then $\pi \simeq \frac{1}{K} + \frac{1}{K^2}$.*
Below we apply this lemma to estimate the probability of $\phi(i) = \phi(j)$ for some random cryptographic function ϕ. [1]

Description of the attack. To attack by fitering and counting the key of the first round of Skipjack reduced to its first 16 rounds, the differential characteristic used in [3, section 4.1] is

$$\Delta = (a, b, 0, c) \quad \xrightarrow{\tau_A} \quad \Delta^\times = (0, c, b, 0) \quad \xrightarrow{3\tau_A 8\tau_B} \quad \Delta^* = (g, h, f, 0).$$

Let us recall the notations for the probabilities of the differentials. Let p be the probability of $\Delta^\times \to \Delta^*$, q the probability of $\Delta \to \Delta^\times$, p^* the probability of $\Delta \to \Delta^*$. and q^* the probability of $\Delta \to \Delta^\times \to \Delta^*$. The filtering condition is $q^*/q \gg p^*$, which rewrites $p \gg p^*$ if the Markov hypothesis holds.

The Markov hypothesis does not hold in general for Skipjack with truncated differentials, but in that case it holds, because uniform random pairs with difference $(a, b, 0, c)$ such that $(a, b, 0, c) \xrightarrow{\tau_A} (0, c, b, 0)$ give uniform random pairs with difference $(0, c, b, 0)$.

In [3] $p = 2^{-16}$ is computed assuming Markov hypothesis for all truncated differentials and Skipkack, and $p^* = 2^{-16}$ can be computed with the same hypothesis. That result implies that the the attack cannot work. However we see below that the Markov hypothesis does not hold in that case and that $p \simeq 2^{-15}$ and $p^* \simeq 2^{-16}$.

Computation of the probability p of $(0, c, b, 0) \xrightarrow{7\tau_A 8\tau_B} (g, h, f, 0)$. To make an exact computation of p we need to write the result of the encryption of a pair through those 15 rounds of SkipJack. Let G_2 to G_{16} the keyed G functions.

[1] If ϕ is a permutation, this probability is equal to $\frac{1}{K}$. However, if ϕ is obtained by the exclusive XOR of permutations, or similar operations, then the values $\phi(i)$ appear to be taken uniform randomly and the lemma applies.

We also write $\Delta G_i(X)$ the value of $G_i(x_1) \oplus G_i(x_2)$ for some $x_1 \oplus x_2 = X$. If the input pair has difference $(0, c, b, 0)$ then the values of the differences through the 15 rounds are shown in figure 1.

	0	c	b	0	
τ_A	0	0	c	b	
τ_A	b	0	0	c	
τ_A	$c \oplus Z$	Z	0	0	$Z = \Delta G_4(b)$
τ_A	Y	Y	Z	0	$Y = \Delta G_5(c \oplus Z)$
τ_A	X	X	Y	Z	$X = \Delta G_6(Y)$
τ_A	$Z \oplus W$	W	X	Y	$W = \Delta G_7(X)$
τ_A	$Y \oplus V$	V	W	X	$V = \Delta G_8(Z \oplus W)$
τ_B	X	U	Y	W	$U = \Delta G_9(Y \oplus V)$
τ_B	W	T	$U \oplus X$	Y	$T = \Delta G_{10}(X)$
τ_B	Y	S	$W \oplus T$	$U \oplus X$	$S = \Delta G_{11}(W)$
τ_B	$U \oplus X$	R	$Y \oplus S$	$W \oplus T$	$R = \Delta G_{12}(Y)$
τ_B	$W \oplus T$	Q	$U \oplus X \oplus R$	$Y \oplus S$	$Q = \Delta G_{13}(U \oplus X)$
τ_B	$Y \oplus S$	P	$W \oplus T \oplus Q$	$U \oplus X \oplus R$	$P = \Delta G_{14}(W \oplus T)$
τ_B	$U \oplus X \oplus R$	N	$Y \oplus S \oplus P$	$W \oplus T \oplus Q$	$N = \Delta G_{15}(Y \oplus S)$
τ_B	$W \oplus T \oplus Q$	M	$U \oplus X \oplus R \oplus N$	$Y \oplus S \oplus P$	$M = \Delta G_{16}(U \oplus X \oplus R)$

Fig. 1. Differences during $7\tau_A 8\tau_B$ with input difference $(0, c, b, 0)$

Let the input pair be $(\beta, c_1, b_1, \alpha)$, $(\beta, c_2, b_2, \alpha)$ uniform random. Let $\gamma = \alpha \oplus G_2(\beta)$ and $y'_i = \beta \oplus G_5(c_i \oplus G_4(b_i \oplus G_3(\gamma)))$, then the triplet (γ, y'_1, y'_2) is uniform random.

Let $\phi_\gamma : y \mapsto y \oplus G_{11}(G_7(\gamma \oplus G_6(y))) \oplus G_{14}(G_7(\gamma \oplus G_6(y)) \oplus G_{10}(G_6(y)))$. The differential holds if $Y \oplus S \oplus P = 0$, i.e. $\phi_\gamma(y'_1) = \phi_\gamma(y'_2)$.

The function ϕ_γ is a random cryptographic function for our lemma 1 with $N = K = 2^{16}$. The probability of the differential is then estimated to be 2^{-15}.

Computing with exhaustive search for random uniform y'_1, y'_2 the probability of $\phi_\gamma(y'_1) = \phi_\gamma(y'_2)$, we check that the value of p is around 2^{-15}, slightly depending on γ and the key (less than 1% variation).

Computation of the probability p^* of $(a, b, 0, c) \stackrel{8\tau_A 8\tau_B}{\longrightarrow} (g, h, f, 0)$. The values of the differences through those 16 rounds are shown in figure 2.

Let the input pair be (a_1, b_1, α, c_1) , (a_2, b_2, α, c_2) uniform random. Let $e'_i = \alpha \oplus G_2(c_i + G_1(a_i))$ and $y'_i = \alpha \oplus G_5(G_1(a_i) \oplus G_4(b_i \oplus G_3(e_i)))$, then the values e'_1, y'_1, e'_2, y'_2 are random uniform.

Let $\psi : (e, y) \mapsto y \oplus G_{11}(G_7(G_3(e) \oplus G_6(e \oplus y))) \oplus G_{14}(G_7(G_3(e) \oplus G_6(e \oplus y)) \oplus G_{10}(G_6(e \oplus y)))$. The differential holds if $\psi(e'_1, y'_1) = \psi(e'_1, y'_2)$. The function ψ is a random cryptographic function for our lemma 1 with $N = 2^{32}$ and $K = 2^{16}$. The probability of the differential is then estimated to be $2^{-16} + 2^{-32}$.

	a	b	0	c	
τ_A	$c \oplus D$	D	b	0	$D = \Delta G_1(a)$
τ_A	E	E	D	b	$E = \Delta G_2(c \oplus D)$
τ_A	$b \oplus F$	F	E	D	$F = \Delta G_3(E)$
τ_A	$D \oplus Z$	Z	F	E	$Z = \Delta G_4(b \oplus F)$
τ_A	$E \oplus Y$	Y	Z	F	$Y = \Delta G_5(D \oplus Z)$
τ_A	$F \oplus X$	X	Y	Z	$X = \Delta G_6(E \oplus Y)$
τ_A	$Z \oplus W$	W	X	Y	$W = \Delta G_7(F \oplus X)$
τ_A	$Y \oplus V$	V	W	X	$V = \Delta G_8(Z \oplus W)$
τ_B	X	U	Y	W	$U = \Delta G_9(Y \oplus V)$
τ_B	W	T	$U \oplus X$	Y	$T = \Delta G_{10}(X)$
τ_B	Y	S	$W \oplus T$	$U \oplus X$	$S = \Delta G_{11}(W)$
τ_B	$U \oplus X$	R	$Y \oplus S$	$W \oplus T$	$R = \Delta G_{12}(Y)$
τ_B	$W \oplus T$	Q	$U \oplus X \oplus R$	$Y \oplus S$	$Q = \Delta G_{13}(U \oplus X)$
τ_B	$Y \oplus S$	P	$W \oplus T \oplus Q$	$U \oplus X \oplus R$	$P = \Delta G_{14}(W \oplus T)$
τ_B	$U \oplus X \oplus R$	N	$Y \oplus S \oplus P$	$W \oplus T \oplus Q$	$N = \Delta G_{15}(Y \oplus S)$
τ_B	$W \oplus T \oplus Q$	M	$U \oplus X \oplus R \oplus N$	$Y \oplus S \oplus P$	$M = \Delta G_{16}(U \oplus X \oplus R)$

Fig. 2. Differences during $8\tau_A 8\tau_B$ with input difference $(a, b, 0, c)$

Computing with semi-exhaustive search for random uniform $(e'_1, y'_1), (e'_2, y'_2)$ the probability of $\psi(e'_1, y'_1) = \psi(e'_1, y'_2)$, we check that the value of p^* is indeed about 2^{-16} with precision better than 2%.

Conclusion. The actual probabilities are $p \simeq 2p^*$. The filtering condition holds and the attack can work. To validate the counting hypothesis and check if the attacks really works, an implementation of the attack is needed.

The attack from [3, section 4.3] of Skipjack reduced to the last 28 rounds is not repaired by similar exact computations.