Flaws in differential cryptanalysis of Skipjack

Louis Granboulan
École Normale Supérieure
Louis.Granboulan@ens.fr

Abstract

Motivation: the paper *Truncated Differentials and Skipjack*, of Knudsen, Robshaw and Wagner, presented at Crypto'99

Contains two types of flaws:

— unappropriate use of trivial probabilities

— unjustified approximations for computing the probabilities of differentials

There is a need of mathematical verification of academic attacks

1. Differential cryptanalysis

   filtering and counting

2. The first 16 rounds of Skipjack

   take care of trivial probabilities

3. Precise computation of probabilities

   take care of unjustified approximations

4. Boomerang attack

   take care of trivial probabilities

Differential cryptanalysis

Probability of a differential

Keyed cipher $E_k : x \mapsto y$

Differential $\Delta \to \Delta^*$

$$p = \mathrm{Pr}_{k,x,x'}[E_k(x) \oplus E_k(x') \in \Delta^* \;/\; x \oplus x' \in \Delta]$$

Usual hypothesis are

Stochastic equivalence $\Rightarrow$ p independant of k

Markov hypothesis $\Rightarrow$ p independant of x, x'

Filtering

Composition $x \xmapsto{E1_{k1}} y \xmapsto{E2_{k2}} z$

Differential characteristic $\Delta \to \Delta^\times \to \Delta^*$

Attack with filtering

Encrypt pairs s.t. $x \oplus x' \in \Delta$

Throw away if $z \oplus z' \notin \Delta^*$

Then $y \oplus y' \in \Delta^\times$ with higher probability

Deduce the value of $k1$ (with counting)

Success of filtering

$$
\begin{array}{lll}
\Delta \to \Delta^{\times} & \text{probability} & q \\
\quad \Delta^{\times} \to \Delta^{*} & \text{probability} & p \\
\Delta \to \Delta^{\times} \to \Delta^{*} & \text{probability} & q^{*} \\
\Delta \longrightarrow \Delta^{*} & \text{probability} & p^{*}
\end{array}
$$

Probability of $\Delta^{\times}$ is increased when:

$\Pr[\Delta \to \Delta^{\times} \to \Delta^{*} \,/\, \Delta \to \Delta^{*}] > \Pr[\Delta \to \Delta^{\times}]$ i.e. $q^{*}/p^{*} > q$

Markov hypothesis $\Rightarrow q^{*} = pq$

Filtering increases the probability of $\Delta^{\times}$ when $p > p^{*}$

Success of counting

A counter for each possible value for $k1$

For each filtered pair x, x', increase counter for $k1$ if

$$E1_{k1}(x) \oplus E1_{k1}(x') \in \Delta^{\times}$$

N the number of pairs after filtering

If no filtering, the mean value of a counter : qN.

After filtering, the right $k1$ counter : at least $(q^*/p^*)N$

Counting hypothesis: the right $k1$ has (one of) the highest counter value

Description of Skipjack

16-bits words   keyed bijective function G

Notation: $\Delta G(a)$ is the value of $G(x) \oplus G(x')$ when $x \oplus x' = a$

Action of Skipjack rounds on differences

A-rule (τ_A) $(a, b, c, d) \mapsto (d \oplus \Delta G(a), \Delta G(a), b, c)$
B-rule (τ_B) $(a, b, c, d) \mapsto (d, \Delta G(a), b \oplus a, c)$

Skipjack encryption: $8\tau_A 8\tau_B 8\tau_A 8\tau_B$

Some truncated differentials

$$(a,b,c,d) \xrightarrow{\tau_A} (d \oplus \Delta G(a), \Delta G(a), b, c)$$
$$(a,b,c,d) \xrightarrow{\tau_B} (d, \Delta G(a), b \oplus a, c)$$

With probability 1

$$(0,b,c,d) \xrightarrow{\tau_A \text{ or } \tau_B} (d,0,b,c)$$
$$(0,b,c,0) \xrightarrow{2\tau_A \text{ or } 2\tau_B} (c,0,0,b)$$
$$(0,b,0,0) \xrightarrow{3\tau_A \text{ or } 3\tau_B} (b,0,0,0)$$
$$(a,b,c,0) \xrightarrow{\tau_A} (e,e,b,c) \quad e = \Delta G(a)$$
$$(a,a,c,d) \xrightarrow{\tau_B} (d,e,0,c) \quad e = \Delta G(a)$$
$$(a,b,c,0) \xrightarrow{\tau_A \tau_B} (c,f,0,b) \quad f = \Delta G \circ \Delta G(a)$$
$$(0,a,0,0) \xrightarrow{4\tau_A 4\tau_B} (f,0,0,0) \quad f = \Delta G \circ \Delta G(a)$$

With probability 2^{-16}

$$(a,b,c,d) \xrightarrow{\tau_A} (0,d,b,c) \quad d = \Delta G(a)$$

Attacking the first 16 rounds

Attack of Knudsen, Robshaw and Wagner

The differential characteristic used is

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

Decomposition of the first 8 rounds

$$(a,b,0,c) \xrightarrow{\tau_A}_{2^{-16}} (0,c,b,0) \xrightarrow{2\tau_A}_{1} (b,0,0,c) \xrightarrow{\tau_A}_{2^{-16}} (0,d,0,0) \xrightarrow{4\tau_A}_{1} (e,e,0,0)$$

The attack is said to extract the key of the first round

Probabilities are computed with Markov hypothesis

$p = q = 2^{-16}$, $q^* = 2^{-32}$ $\quad (a,b,0,c) \xrightarrow{\tau_A} (0,c,b,0) \xrightarrow{7\tau_A 8\tau_B} (g,h,f,0)$

$p^* = 2^{-16}$ $\quad (a,b,0,c) \xrightarrow{8\tau_A 8\tau_B} (g,h,f,0)$

$p = p^*$: the attack does not work as described

Repairing the attack (filtering)

The Markov hypothesis does not hold in general
for Skipjack with Truncated Differentials

In the case of $(a, b, 0, c) \xrightarrow{\tau_A} (0, c, b, 0) \xrightarrow{7\tau_A 8\tau_B} (g, h, f, 0)$ the Markov hypothesis 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 $(0, c, b, 0)$

We only need to compute with precision the following probabilities

$$(0, c, b, 0) \xrightarrow{7\tau_A 8\tau_B} (g, h, f, 0) \quad p \simeq 2^{-16}$$

$$(a, b, 0, c) \xrightarrow{8\tau_A 8\tau_B} (g, h, f, 0) \quad p^* \simeq 2^{-16}$$

The filtering will work only if $p > p^*$

Success of the counting is another condition for the attack to work

Computation of the probability of $(0, c, b, 0) \overset{7\tau_A 8\tau_B}{\longrightarrow} (g, h, f, 0)$

	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	$U \oplus X \oplus R \oplus N$	$Y \oplus S \oplus P$	$M = \Delta G_{16}(U \oplus X \oplus R)$

Differential holds when $Y \oplus S \oplus P = 0$

Differential $(0, c, b, 0) \stackrel{7\tau_A 8\tau_B}{\longrightarrow} (g, h, f, 0)$ holds when $Y \oplus S \oplus P = 0$

The formulae are $Z = \Delta G_4(b)$ $\quad Y = \Delta G_5(c \oplus Z)$

$X = \Delta G_6(Y)$ $\quad W = \Delta G_7(X)$ $\quad T = \Delta G_{10}(X)$

$S = \Delta G_{11}(W)$ $\quad P = \Delta G_{14}(W \oplus T)$

The input pair is written $(\alpha, c_1, b_1, \beta)$, $(\alpha, c_2, b_2, \beta)$

Then $y_i = G_5(c_i \oplus G_4(b_i))$

Random uniform input pairs leads to random uniform pairs y_1, y_2

Differential holds when $\phi(y_1) = \phi(y_2)$ with

$$\phi : y \mapsto y \oplus G_{11}(G_7(G_6(y))) \oplus G_{14}(G_7(G_6(y)) \oplus G_{10}(G_6(y)))$$

Computing with exhaustive search the probability of $\phi(y_1) = \phi(y_2)$ for random uniform y_1, y_2 gives a probability p about 2^{-15}, slightly depending on the key (less than 1% variation)

Computation of the probability of $(a, b, 0, c) \xrightarrow{8\tau_A 8\tau_B} (g, h, f, 0)$

	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	$U \oplus X \oplus R \oplus N$	$Y \oplus S \oplus P$	$M = \Delta G_{16}(U \oplus X \oplus R)$

Differential holds when $Y \oplus S \oplus P = 0$

Differential $(a,b,0,c) \overset{8\tau_A 8\tau_B}{\longrightarrow} (g,h,f,0)$ holds when $Y \oplus S \oplus P = 0$

The formulae are $D = \Delta G_1(a)$ $\quad E = \Delta G_2(c \oplus D)$

$F = \Delta G_3(E)$ $\quad Z = \Delta G_4(b \oplus F)$ $\quad Y = \Delta G_5(D \oplus Z)$

$X = \Delta G_6(E \oplus Y)$ $\quad W = \Delta G_7(F \oplus X)$ $\quad T = \Delta G_{10}(X)$

$S = \Delta G_{11}(W)$ $\quad P = \Delta G_{14}(W \oplus T)$

The input pair is written (a_1, b_1, α, c_1) , (a_2, b_2, α, c_2)

Then $e_i = G_2(c_i + G_1(a_i))$ and $y_i = G_5(G_1(a_i) \oplus G_4(b_i \oplus G_3(e_i)))$

Random uniform input leads to random uniform pairs $(e_1, y_1), (e_2, y_2)$

Differential holds when $\psi(e_1, y_1) = \psi(e_1, y_2)$ with

$\psi : (e,y) \mapsto y \oplus G_{11}(G_7(G_3(e) \oplus G_6(e \oplus y))) \oplus G_{14}(G_7(G_3(e) \oplus G_6(e \oplus y)) \oplus G_{10}(G_6(e \oplus y)))$

Computing with semi-exhaustive search the probability of $\psi(e_1, y_1) = \psi(e_1, y_2)$ for random uniform $(e_1, y_1), (e_2, y_2)$ gives a probability p^* of 2^{-16} with precision better than 2%

Boomerang attacks

Technique due to David Wagner presented at FSE'99

Split the cipher in $E2 \circ E1$

1. For random $P \oplus P' \in \Delta$ encrypt $P \overset{E1}{\to} \bar{P} \overset{E2}{\to} C$ and $P' \overset{E1}{\to} \bar{P}' \overset{E2}{\to} C'$
2. Create random D and D' such that $C \oplus D \in \nabla$ and $C' \oplus D' \in \nabla$
3. Decrypt $D \overset{E2^{-1}}{\to} \bar{Q} \overset{E1^{-1}}{\to} Q$ and $D' \overset{E2^{-1}}{\to} \bar{Q}' \overset{E1^{-1}}{\to} Q'$
4. With some probability p we have $Q \oplus Q' \in \Delta$

   A distinguisher works if p is different of the trivial $\frac{\#\Delta}{2^{\text{blocksize}}}$

$$p = \sum_{w \oplus x \oplus y \oplus z = 0} \Pr[\Delta \xrightarrow{E1} w] \Pr[\nabla \xrightarrow{E2^{-1}} x] \Pr[\nabla \xrightarrow{E2^{-1}} y] \Pr[z \xrightarrow{E1^{-1}} \Delta]$$

The middle 24 rounds of Skipjack

Attack of Knudsen, Robshaw and Wagner

The forward differential $\Delta = (0, a, 0, 0) \overset{4\tau_A 8\tau_B}{\longrightarrow}_1 \Delta^* = (c, d, e, 0)$

The backward differential $\nabla = (f, 0, 0, 0) \overset{4\tau_A^{-1} 8\tau_B^{-1}}{\longrightarrow}_1 \nabla^* = (i, h, 0, j)$

Good looking quartets are those where $Q \oplus Q' \in \Delta$

Right quartets have also $\bar{P} \oplus \bar{P}' \in \Delta^*$, $\bar{Q} \oplus \bar{Q}' \in \Delta^*$, $\bar{P} \oplus \bar{Q} \in \nabla^*$ and $\bar{P}' \oplus \bar{Q}' \in \nabla^*$

For a random cipher, in 2^{-48} quartets we can expect one good looking

For Skipjack, in 2^{-48} quartets we can expect one right quartet

Wrong conclusion: for Skipjack, in 2^{-48} quartets we can expect two good looking

In reality: for Skipjack, all good looking quartets are right ones

Conclusion

Trivial probabilities should be avoided

Markov hypothesis should be carefully checked

Truncated differentials are more complicated than regular ones