On related-key attacks and KASUMI: the case of A5/3

Phuong Ha Nguyen[1], M.J.B. Robshaw[2], Huaxiong Wang[1]

[1] Nanyang Technological University, Singapore

[2] Applied Cryptography Group, Orange Labs, France
NG0007HA@e.ntu.edu.sg, hxwang@ntu.edu.sg
matt.robshaw@orange-ftgroup.com

INDOCRYPT 2011, 11-14 DEC 2011

Talk Overview

1. Motivation
2. 64-bit key version of Kasumi used for A5/3
   - Structure of 128-bit key version
   - Structure of 64-bit key version
3. Upper bound for any 3-round related-key differential over A5/3
4. Resistance against Crypto2010 Attack
5. Conclusion

Content and Motivation

- Presenting Kasumi version with 64-bit key used for A5/3.
- Prove that the upper bound for any three-round related-key differential over Kasumi with 64-bit key is 2^{-18}
- Based on the upper bound, the Crypto2010 attack on 128-bit key version of Kasumi is not applicable to 64-bit version.

128-bit key version of Kasumi

- The block cipher Kasumi with 128-bit key is used in 3G networks and it resists well against traditional linear and differential cryptanalysis. The 128-bit key K is divided into eight 16-bit word , i.e $K = (K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7)$.
- Related-key differential cryptanalysis is the differential cryptanalysis has not only the differences in the input and output texts but also in the key.
- The 128-bit version is broken in practical time by attack of Crypto2010 which based on the related-key techniques.

FIGURE 2: Computation graph for the encryption process of the KASUMI cipher

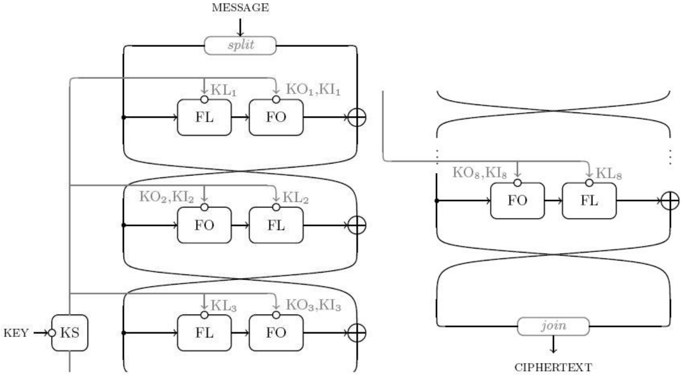


FIGURE 1: FUNCTION FL

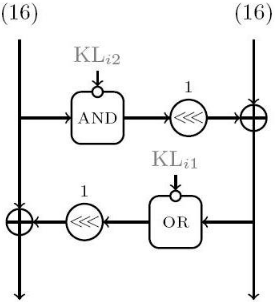


Fig. 1. Details of the FL function in the KASUMI cipher. Numbers in brackets indicate the size of the inputs in bits.

FIGURE 3: FUNCTION F0 AND FI

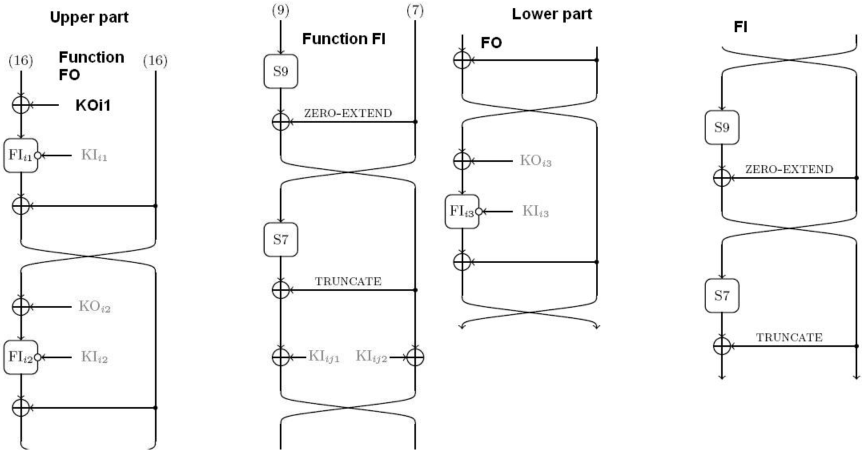
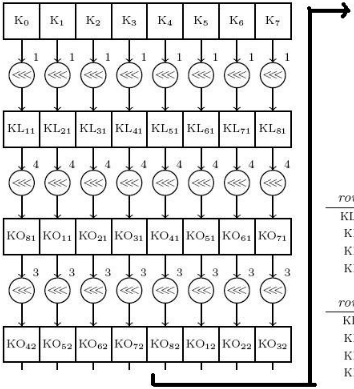
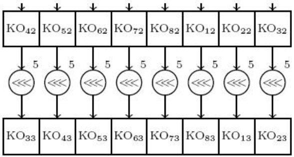


FIGURE 4: KEY SCHEDULE


K_0 K_1 K_2 K_3 K_4 K_5 K_6 K_7
1 1 1 1 1 1 1 1
KL_{11} KL_{21} KL_{31} KL_{41} KL_{51} KL_{61} KL_{71} KL_{81}
4 4 4 4 4 4 4 4
KO_{81} KO_{11} KO_{21} KO_{31} KO_{41} KO_{51} KO_{61} KO_{71}
3 3 3 3 3 3 3 3
KO_{42} KO_{52} KO_{62} KO_{72} KO_{82} KO_{12} KO_{22} KO_{32}


KO_{42} KO_{52} KO_{62} KO_{72} KO_{82} KO_{12} KO_{22} KO_{32}
5 5 5 5 5 5 5 5
KO_{33} KO_{43} KO_{53} KO_{63} KO_{73} KO_{83} KO_{13} KO_{23}

round	1	2	3	4
KL_{i2}	$K_2 \oplus$ 89ab	$K_3 \oplus$ cdef	$K_4 \oplus$ fedc	$K_5 \oplus$ ba98
KI_{i1}	$K_4 \oplus$ fedc	$K_5 \oplus$ ba98	$K_6 \oplus$ 7654	$K_7 \oplus$ 3210
KI_{i2}	$K_3 \oplus$ cdef	$K_4 \oplus$ fedc	$K_5 \oplus$ ba98	$K_6 \oplus$ 7654
KI_{i3}	$K_7 \oplus$ 3210	$K_0 \oplus$ 0123	$K_1 \oplus$ 4567	$K_2 \oplus$ 89ab

round	5	6	7	8
KL_{i2}	$K_6 \oplus$ 7654	$K_7 \oplus$ 3210	$K_0 \oplus$ 0123	$K_1 \oplus$ 4567
KI_{i1}	$K_0 \oplus$ 0123	$K_1 \oplus$ 4567	$K_2 \oplus$ 89ab	$K_3 \oplus$ cdef
KI_{i2}	$K_7 \oplus$ 3210	$K_0 \oplus$ 0123	$K_1 \oplus$ 4567	$K_2 \oplus$ 89ab
KI_{i3}	$K_3 \oplus$ cdef	$K_4 \oplus$ fedc	$K_5 \oplus$ ba98	$K_6 \oplus$ 7654

64-bit key version of Kasumi

- The 64-bit key version of Kasumi is modified to adapt the requirement for the algorithm A5/3, i.e there are only 64-bit key used. The key schedule is similar to that of original one, the only difference is the redundancy is added, i.e $K = (K_0, K_1, K_2, K_3, K_0, K_1, K_2, K_3)$ or $K_0 = K_4, K_1 = K_5, K_2 = K_6, K_3 = K_7$.
- The 64-bit key version resists well again Crypto2010 attack.
- To deeply understand this resistance, the upper bound of any 3-round related key differential is studied. For the sake of convenience, the word ”block cipher Kasumi” refers to ”the 64-bit key version of Kasumi”.

the general structure of Kasumi

- The block cipher Kasumi consists of 8 rounds $R_1, \ldots, R_8$.
- In R_i:=$FL \rightarrow FO$ or $FO \rightarrow FL$
- In function FL:= (AND,ROTATION) $\rightarrow$ (OR,ROTATION).
- In function FO:= $FI_1 \rightarrow FI_2 \rightarrow FI_3$
- In function FI_i:= $S_9 \rightarrow S_7 \rightarrow S_9 \rightarrow S_7$.

To prove the upper bound for 3-round related-key differential, we have done in 4 following steps:

1. proving the upper bound for FI with key difference $\Delta(KI) \neq 0$ is 2^{-6}
2. In a round of Kasumi, if FO has one active ΔKI then the upper bound of a differential characteristic of the round is 2^{-6}. If there are at least two active ΔKI, then the upper bound is 2^{-12}
3. The upper bound for any 3-round consecutive is less or equal to the product of upper bound of 2 any rounds of them.
4. Proving the upper bound for any 3-round related-key differential is 2^{-18}

All the above steps are formalized in the following lemmas and theorem.

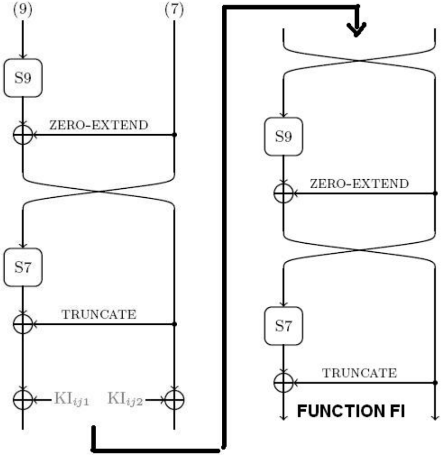
Lemma 1

Lemma

For any (active or inactive) input difference to the KASUMI function FI with key difference $\Delta(\mathrm{KI}) \neq 0$*, the probability of a differential characteristic is* $\leq 2^{-6}$.

Proof.

The result comes from the fact that when only one S_7 is active then the probability of differential is 2^{-6} and this probability is the upper bound. □


(9)
(7)
S9
ZERO-EXTEND
S7
TRUNCATE
KI_{ij1}
KI_{ij2}
S9
ZERO-EXTEND
S7
TRUNCATE
FUNCTION FI

Lemma 2

Lemma

In a round of KASUMI, if FO has one active $\Delta\mathrm{KI}$ *then the maximum probability of a differential characteristic is* 2^{-6}*. If there are at least two active* $\Delta\mathrm{KI}$ *then the maximum probability of a differential characteristic is* 2^{-12}*.*

Proof.

Please find the proof in paper. □

Lemma 3

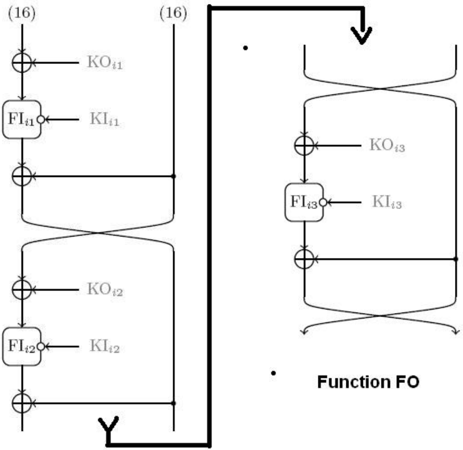
Lemma

Write the key inputs to FO as $(\mathrm{KO}_1, \mathrm{KO}_2, \mathrm{KO}_3)$ *and* $(\mathrm{KI}_1, \mathrm{KI}_2, \mathrm{KI}_3)$. *For any (active or inactive) text input to FO, and for any active key difference in at least one of* $(\mathrm{KO}_1, \mathrm{KO}_2,$ *or* $\mathrm{KO}_3)$ *there must be at least one FI function that is differentially active except in the following three cases:*

1. $\Delta(\mathrm{KO}_1) \neq 0$, $\Delta(\mathrm{KO}_2) = 0$, *and* $\Delta(\mathrm{KO}_3) = 0$.
2. $\Delta(\mathrm{KO}_1) = 0$, $\Delta(\mathrm{KO}_2) \neq 0$, *and* $\Delta(\mathrm{KO}_3) \neq 0$.
3. $\Delta(\mathrm{KO}_1) \neq 0$, $\Delta(\mathrm{KO}_2) \neq 0$, *and* $\Delta(\mathrm{KO}_3) \neq 0$.

Proof.

Please find the proof in the paper. □



- Function FO

Lemma3 continue

The lemma shows that how the inputs of FO might cause the inner function FI to become differentially active. The lemmas implies that if there are only active key differences $\Delta KO1, \Delta KO2$, then at least one FI function become active. According to design and evaluation report of Kasumi, if the difference of the inner key KI $\Delta KI = 0$ then the maximum probability of differential characteristic is 2^{-14}. Hence the upper bound for related-key differential characteristic of FO is 2^{-14}.

Lemma 4

Lemma

For any three-round differential of KASUMI across rounds i, $i+1$, and $i+2$, the probability of the differential (in a related-key setting) is upper-bounded by $\min\{\Pr_{max}.(\Delta^i) \times \Pr_{max}.(\Delta^{i+1}), \Pr_{max}.(\Delta^{i+1}) \times \Pr_{max}.(\Delta^{i+2}), \Pr_{max}.(\Delta^i) \times \Pr_{max}.(\Delta^{i+2})\}$ *where* $\Pr_{max}.(\Delta^i)$ *denotes the maximum probability of any non-trivial differential characteristic across round i in the related-key setting.*

Theorem

The probability of any three-round related-key differential over KASUMI, when used as A5/3, is $\leq 2^{-18}$.

theorem continue

Table: Key differences in the 64-bit user-supplied key lead to *at least* the above-noted subkeys being differentially active in the specified round.

round	$\{k_0, k_4\}$	$\{k_1, k_5\}$	$\{k_2, k_6\}$	$\{k_3, k_7\}$
1	KI_1	KO_1, KO_2	KO_3	KI_2, KI_3
2	KI_2, KI_3	KI_1	KO_1, KO_2	KO_3
3	KO_3	KI_2, KI_3	KI_1	KO_1, KO_2
4	KO_1, KO_2	KO_3	KI_2, KI_3	KI_1
5	KI_1	KO_1, KO_2	KO_3	KI_2, KI_3
6	KI_2, KI_3	KI_1	KO_1, KO_2	KO_3
7	KO_3	KI_2, KI_3	KI_1	KO_1, KO_2
8	KO_1, KO_2	KO_3	KI_2, KI_3	KI_1

Theorem continue

We appeal to Lemmas 3, 1, 2, and 4. First we construct Table 1 where we note that, due to rotational symmetries in the way subkeys are used, it suffices to consider the first three rounds only. There are 15 cases to consider, depending on which pairs $\{k_0, k_4\}$, $\{k_1, k_5\}$, $\{k_2, k_6\}$, or $\{k_3, k_7\}$ are active. However these are easily broken down into a few cases and enumerated.

- If either of the pairs $\{k_0, k_4\}$ or $\{k_1, k_5\}$ are active, then the result follows from Lemmas 1, 2, and 4.
- If the pair $\{k_2, k_6\}$ or $\{k_1, k_5\}$ are active then the result follows from Lemmas 1, 3, 2, and 4. $\square$.

Crypto2010 attack or sandwich attack

- In the Crypto2010 attack on 128-bit key version of Kasumi, the block cipher is considered as the concatenation of 3 sub-ciphers $E_1 \circ M \circ E_2$.
- E_1 and E_2 have 3 rounds in each sub-cipher and M has only 1 round of Kasumi.
- There are 2 related-key differential characteristics with very high probability p_1, p_2 cover 2 ciphers E_1 and E_2 respectively and one special technique is appealed to concatenate the E_1 and E_2 over M with high probability r. Actually, this attack may be considered as a special application of boomerang related-key attack.
- Hence there are 7-round distinguisher constructed which helps to launch the 8-round key recovered attack in Kasumi. The number of text pairs needed is

Resistance against sandwich attack

- In 64-bit key version, according to the theorem above, any 3-round related-key attack has the upper bound for differential is 2^{-18}.
- Hence, the number of text pairs needed is $> 1/(2^{-18\times 4}) = 2^{72} > 2^{64}$ which is out of possible number of text pairs. Hence, the sandwich attack does not work on 64-bit version of Kasumi.

Conclusion

- In this paper, the 64-bit key version of Kasumi is introduced which is able to be used in A5/3.
- The upper bound for any 3-round related-key differential is provided, i.e the upper bound is 2^{-18}.
- Based on the above upper bound, the sandwich attack does not work for 64-bit key version although it works very well for 128-bit key version.

Q & A

Thank you