# Improved Cryptanalysis of the Block Cipher KASUMI

Keting Jia[1], Leibo Li[2], Christian Rechberger[3], Jiazhe Chen[2], and Xiaoyun Wang[1,3,⋆]

[1] Institute for Advanced Study, Tsinghua University, China
{ktjia,xiaoyunwang}@mail.tsinghua.edu.cn
[2] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, China
{lileibo,jiazhechen}@mail.sdu.edu.cn
[3] Department of Mathematics, Technical University of Denmark, Denmark
c.rechberger@mat.dtu.dk

**Abstract.** KASUMI is a block cipher which consists of eight Feistel rounds with a 128-bit key. Proposed more than 10 years ago, the confidentiality and integrity of 3G mobile communications systems depend on the security of KASUMI. In the practically interesting single key setting, only up to 6 rounds have been attacked so far. In this paper we use some observations on the FL and FO functions. Combining these observations with a key schedule weakness, we select some special input and output values to refine the general 5-round impossible differentials and propose the first 7-round attack on KASUMI with time and data complexities similar to the previously best 6-round attacks. This leaves now only a single round of security margin.

The new impossible differential attack on the last 7 rounds needs $2^{114.3}$ encryptions with $2^{52.5}$ chosen plaintexts. For the attack on the first 7 rounds, the data complexity is $2^{62}$ known plaintexts and the time complexity is $2^{115.8}$ encryptions.

**Keywords:** KASUMI, Impossible Differential, Cryptanalysis.

## 1 Introduction

The block cipher KASUMI is designed for 3GPP (3rd Generation Partnership Project, which is the body standardizing the next generation of mobile telephony) as the basis of confidentiality and integrity algorithms by ETSI SAGE [11]. Nowadays, it is widely used in UMTS, GSM and GPRS mobile communications systems [12].

KASUMI has eight Feistel rounds with a 128-bit key optimized for hardware performance, and is a slightly modified version of the block cipher MISTY1 [7]. Because of its importance, KASUMI attracts a great deal of attention of cryptology researchers. Several attacks on variants of KASUMI were published in

⋆ Corresponding author.

L.R. Knudsen and H. Wu (Eds.): SAC 2012, LNCS 7707, pp. 222–233, 2013.

past years [8,9,10]. In the single-key setting, the best result is an impossible differential attack on a 6-round version of the cipher presented by Kühn [5]. In the related-key setting, Blunden and Escott gave a differential attack of KASUMI reduced to 6 rounds [3]. Later, Biham et al. introduced related-key boomerang and rectangle attacks on the full 8-round KASUMI, which need $2^{78.7}$ and $2^{76.1}$ encryptions respectively [2]. At Crypto 2010, Dunkelman et al. proposed a practical related-key attack on the full KASUMI by using a new strategy named sandwich attack [4], which is a formal extension of boomerang attack. However, these attacks assume control over the differences of two or more related keys in all the 128 key bits. This gives not only the attacker a lot more degrees of freedom, it also renders the resulting attack inapplicable in most real-world usage scenarios.

For an impossible differential attack, the secret key is obtained by eliminating wrong keys which bring about the input and output values of the impossible differential. The general 5-round impossible differential $(0, a) \overset{5R}{\nrightarrow} (0, a)$ [1], that holds for any balanced Feistel scheme, was used to attack 6-round KASUMI, where $a$ is a 32-bit non-zero value [5]. We observe that the output difference only depends on 64 bits of the key when the input difference is selected as $(0, *\|0)$. Hence we consider a new, more fine-grained impossible differential $(0, a_l\|0) \overset{5R}{\nrightarrow} (0, a_l\|0)$, where $a_l$ is a 16-bit non-zero value. We mount this impossible differential on round 2 to 6 to analyze the last 7 rounds, and the input and output values of the impossible differential obtained by partial encryption and decryption in the extended rounds only depend on 112 bit keys. The attack costs $2^{52.5}$ chosen plaintexts and $2^{114.3}$ encryptions. Because the positions of the $FL$ and $FO$ functions are different in even rounds and odd rounds, the above impossible differential attack is not applied to the first 7 rounds. However, we have some new observations on the FL function, with which the wrong keys are eliminated earlier than before. The new attack on the first 7 rounds of KASUMI needs $2^{62}$ known plaintexts and $2^{115.8}$ encryptions. A summary of our attacks and previous attacks with a single key is given in Table 1.

**Table 1.** Summary of the attacks on KASUMI

| Attack Type | Rounds | Data | Time | Source |
|---|---|---|---|---|
| Higher-Order Differential | 5 | $2^{22.1}$ CP | $2^{60.7}$ Enc | [10] |
| Higher-Order Differential | 5 | $2^{28.9}$ CP | $2^{31.2}$ Enc | [9] |
| Integral-Interpolation | 6 | $2^{48}$ CP | $2^{126.2}$ Enc | [8] |
| Impossible Differential | 6 | $2^{55}$ CP | $2^{100}$ Enc | [5] |
| Impossible Differential | 7(2-8) | $2^{52.5}$ CP | $2^{114.3}$ Enc | Sect. 4 |
| Impossible Differential | 7(1-7) | $2^{62}$ KP | $2^{115.8}$ Enc | Sect. 5 |

CP refers to the number of chosen plaintexts.
KP refers to the number of known plaintexts.
Enc refers to the number of encryptions.

The paper is organized as follows. We give a brief description of the block cipher KASUMI in Sect. 2. Some observations used in our cryptanalysis are shown in Sect. 3. In Sect. 4, we propose an improved impossible differential attack on the last 7 rounds of KASUMI. And the impossible differential attack on the first 7 rounds of KASUMI is presented in Sect. 5. We summarize the findings and conclude in Sect. 6.

## 2 Description of KASUMI

KASUMI works on a 64-bit block and uses a 128-bit key. We give a brief description of KASUMI in this section and discuss cost models for evaluating attack complexities.

**Key Schedule.** In order to make the hardware significantly smaller and reduce key set-up time, the key schedule of KASUMI is much simpler than the original key schedule of MISTY1. The 128-bit key K is divided into eight 16-bit words: $k_1$,$k_2$, ..., $k_8$, i.e., $K = (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8)$. In each round, eight key words are used to compute the round subkeys, which are made up of three parts $KL_i$, $KO_i$ and $KI_i$. Here, $KL_i = (KL_{i,1}, KL_{i,2})$, $KO_i = (KO_{i,1}, KO_{i,2}, KO_{i,3})$ and $KI_i = (KI_{i,1}, KI_{i,2}, KI_{i,3})$. We summarize the details of the key schedule of KASUMI in Tab. 2.

**Table 2.** The key schedule of KASUMI

| Round | $KL_{i,1}$ | $KL_{i,2}$ | $KO_{i,1}$ | $KO_{i,2}$ | $KO_{i,3}$ | $KI_{i,1}$ | $KI_{i,2}$ | $KI_{i,3}$ |
|---|---|---|---|---|---|---|---|---|
| 1 | $k_1 \lll 1$ | $k'_3$ | $k_2 \lll 5$ | $k_6 \lll 8$ | $k_7 \lll 13$ | $k'_5$ | $k'_4$ | $k'_8$ |
| 2 | $k_2 \lll 1$ | $k'_4$ | $k_3 \lll 5$ | $k_7 \lll 8$ | $k_8 \lll 13$ | $k'_6$ | $k'_5$ | $k'_1$ |
| 3 | $k_3 \lll 1$ | $k'_5$ | $k_4 \lll 5$ | $k_8 \lll 8$ | $k_1 \lll 13$ | $k'_7$ | $k'_6$ | $k'_2$ |
| 4 | $k_4 \lll 1$ | $k'_6$ | $k_5 \lll 5$ | $k_1 \lll 8$ | $k_2 \lll 13$ | $k'_8$ | $k'_7$ | $k'_3$ |
| 5 | $k_5 \lll 1$ | $k'_7$ | $k_6 \lll 5$ | $k_2 \lll 8$ | $k_3 \lll 13$ | $k'_1$ | $k'_8$ | $k'_4$ |
| 6 | $k_6 \lll 1$ | $k'_8$ | $k_7 \lll 5$ | $k_3 \lll 8$ | $k_4 \lll 13$ | $k'_2$ | $k'_1$ | $k'_5$ |
| 7 | $k_7 \lll 1$ | $k'_1$ | $k_8 \lll 5$ | $k_4 \lll 8$ | $k_5 \lll 13$ | $k'_3$ | $k'_2$ | $k'_6$ |
| 8 | $k_8 \lll 1$ | $k'_2$ | $k_1 \lll 5$ | $k_5 \lll 8$ | $k_6 \lll 13$ | $k'_4$ | $k'_3$ | $k'_7$ |

$x \lll i : x$ rotates left by $i$ bits.
$k'_i = k_i \oplus c_i$, where the $c_i$s are fixed constants.

**Encryption.** KASUMI is a Feistel structure with 8 rounds. Each round is made up of an FL function and an FO function. In odd numbered rounds the FL function precedes the FO function, whereas in even numbered rounds the FO function precedes the FL function. See Fig. 1 ($a$) for an illustration.

Let $L_{i-1}||R_{i-1}$ be the input of the $i$-th round, and then the round function is defined as

$$L_i = FO(FL(L_{i-1}, KL_i), KO_i, KI_i) \oplus R_{i-1},$$
$$R_i = L_{i-1},$$

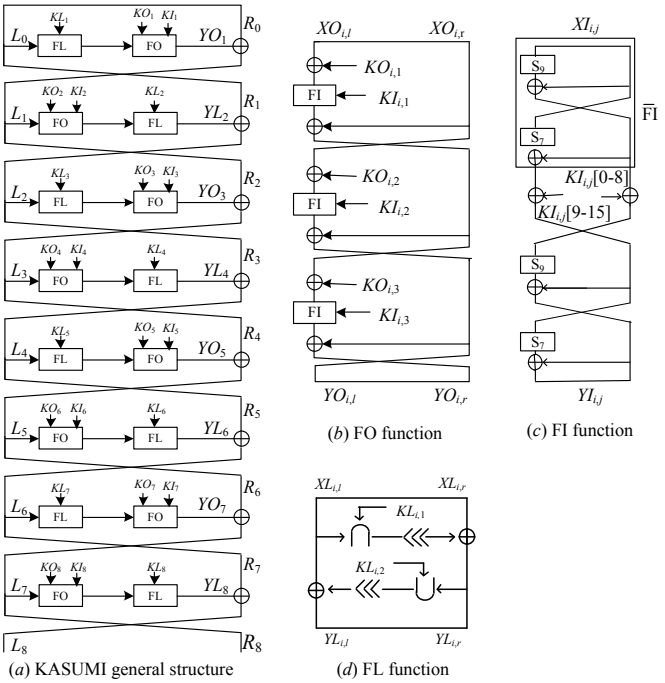


**Fig. 1.** The structure and building blocks of the block cipher KASUMI

where $i = 1, 3, 5, 7$.'$\oplus$' denotes the bitwise exclusive-or (XOR), and '$\|$' represents the concatenation. When $i = 2, 4, 6, 8$,

$$L_i = FL(FO(L_{i-1}, KO_i, KI_i), KL_i) \oplus R_{i-1},$$
$$R_i = L_{i-1}.$$

Here, $L_0\|R_0$, $L_8\|R_8$ are the plaintext and ciphertext respectively, and $L_{i-1}$, $R_{i-1}$ denote the left and right 32-bit halves of the $i$-th round input.

The FL function is a simple key-dependent boolean function, depicted in Fig. 1 (c). Let the inputs of the FL function of the $i$-th round be $XL_i = XL_{i,l}\|XL_{i,r}$, $KL_i = (KL_{i,1}, KL_{i,2})$, the output be $YL_i = YL_{i,l}\|YL_{i,r}$, where $XL_{i,l}, XL_{i,r}, YL_{i,l}$ and $YL_{i,r}$ are 16-bit integers. And the FL function is defined as follows:

$$YL_{i,r} = ((XL_{i,l} \wedge KL_{i,1}) \lll 1) \oplus XL_{i,r}, \quad (1)$$
$$YL_{i,l} = ((YL_{i,r} \vee KL_{i,2}) \lll 1) \oplus XL_{i,l}, \quad (2)$$

where '$\wedge$' and '$\vee$' denote bitwise AND and OR respectively, and '$x \lll i$' implies that $x$ rotates left by $i$ bits. $FL_i$ is the $FL$ function of $i$-th round with subkey $KL_i$.

The FO function provides the non-linear property in each round, which is another three-round Feistel structure consisting of three FI functions and key mixing stages. The FO function is depicted in Fig. 1 (b). There is a 96-bit subkey in FO function of each round (48 subkey bits used in the FI functions and 48 subkey bits in the key mixing stages). Let $XO_i = XO_{i,l} \| XO_{i,r}$, $KO_i = (KO_{i,1}, KO_{i,2}, KO_{i,3})$, $KI_i = (KI_{i,1}, KI_{i,2}, KI_{i,3})$ be the inputs of the FO function of $i$-th round, and $YO_i = YO_{i,l} \| YO_{i,r}$ be the corresponding output, where $XO_{i,l}, XO_{i,r}, YO_{i,l}, YO_{i,r}$ and $\overline{XI}_{i,3}$ are 16-bit integers. Then the FO function has the form

$$\begin{aligned} \overline{XI}_{i,3} &= FI((XO_{i,l} \oplus KO_{i,1}), KI_{i,1}) \oplus XO_{i,r}, \\ YO_{i,l} &= FI((XO_{i,r} \oplus KO_{i,2}), KI_{i,2}) \oplus \overline{XI}_{i,3}, \\ YO_{i,r} &= FI((\overline{XI}_{i,3} \oplus KO_{i,3}), KI_{i,3}) \oplus YO_{i,l}. \end{aligned}$$

For simplicity, define the $FO$ function of $i$-th round as $FO_i$.

The FI function uses two sboxes S7 and S9 which are permutations of 7-bit to 7-bit and 9-bit to 9-bit respectively. Suppose the inputs of the $j$-th $FI$ function of the $i$-th round are $XI_{i,j}$, $KI_{i,j}$ and the output is $YI_{i,j}$, where $XI_{i,j}$ and $YI_{i,j}$ are 16-bit integers. In order to abbreviate the FI function, we define half of FI function as $\overline{FI}$, which is a 16-bit to 16-bit permutation. The structure of FI and $\overline{FI}$ is depicted in Fig. 1 (d). $\overline{YI}_{i,j} = \overline{FI}(XI_{i,j})$ is defined as

$$\begin{aligned} \overline{YI}_{i,j}[0-8] &= S9(XI_{i,j}[7-15]) \oplus XI_{i,j}[0-6], \\ \overline{YI}_{i,j}[9-15] &= S7(XI_{i,j}[0-6]) \oplus \overline{YI}_{i,j}[0-6], \end{aligned}$$

where $z[i_1 - i_2]$ denotes the $(i_2 - i_1 + 1)$ bits from the $i_1$-th bit to $i_2$-th bit of $z$, and '0' is the least significant bit. The FI function is simplified as

$$YI_{i,j} = FI(XI_{i,j}, KI_{i,j}) = \overline{FI}((\overline{FI}(XI_{i,j}) \oplus KI_{i,j}) \lll 7).$$

Denote $FI_{i,j}$ as the $j$-th $FI$ function of the $i$-th round with subkey $KI_{i,j}$.

## 3 Some Observations of KASUMI

Let $\Delta X = X \oplus X'$ be the difference of two values $X$ and $X'$. We describe some observations on the FO and FL functions, which are used in our cryptanalysis of KASUMI.

**Observation 1.** *Given a pair of input values $(XO, XO')$ of the FO function with difference $\Delta XO = (\Delta XO_l \| \ \Delta XO_r) = (a_l \| 0)$, where $a_l$ is a 16-bit non-zero value. Let $\Delta YO$ $(\Delta YO_l \| \Delta YO_r)$ be the corresponding output difference, and then $\Delta YO$ only depends on the 64-bit subkey $KI_1$, $KO_1$, $KI_3$ and $KO_3$.*

**Observation 2.** *[6] Let $X$, $X'$ be $l$-bit values, and $\Delta X = X \oplus X'$. Then there are two difference properties of AND and OR operations, such that*

$$\begin{aligned} (X \wedge K) \oplus (X' \wedge K) &= \Delta X \wedge K, \\ (X \vee K) \oplus (X' \vee K) &= \Delta X \oplus (\Delta X \wedge K). \end{aligned}$$

**Observation 3.** *Let $a_l \| a_r$ be the input differences of functions $FL_1$ and $FL_7$, and the input differences of $FI_{1,2}$ and $FI_{7,2}$ be zero. Then the following equations hold.*

$$(a_l \wedge (k_1 \lll 1)) \lll 1 = a_r, \tag{3}$$
$$(a_l \wedge (k_7 \lll 1)) \lll 1 = a_r. \tag{4}$$

The input differences of $FI_{1,2}$ and $FI_{7,2}$ are zero, so the right 16 bits of output differences of $FL_1$ and $FL_7$ are zero. By the definition of the FL function and Observation 2, equations (3) and (4) hold. The following two observations are deduced as well.

**Observation 4.** *Based on equations (3) and (4), we can get*

$$(a_l \lll 1) \vee \neg a_r = 0xffff. \tag{5}$$

Because the equations (3) and (4) can be represented as 16 parallel equations,

$$\begin{aligned} &a_l[j+1] \wedge k_1[j] = a_r[j+2], \\ &a_l[j+1] \wedge k_7[j] = a_r[j+2], \end{aligned} \qquad j = 0, 1, \ldots, 15. \tag{6}$$

it is obvious that there are only 3 out of 4 values of $(a_l[j+1], a_r[j+2])$ possible, i.e. $(0,0), (1,0), (1,1)$, where $j+1$ and $j+2$ are values mod 16. Therefore we have Observation 4. And the equation (5) holds with probability $(\frac{3}{4})^{16} = 2^{-6.64}$ when both $a_l$ and $a_r$ are uniformly chosen from $2^{16}$ values. This observation is used to select some special impossible differentials to decrease the time complexity of the key recovery in the attack on the first 7-round KASUMI.

**Observation 5.** *Suppose $(a_l[j+1], a_r[j+2])$ is chosen uniformly from the set $\{(1,1), (1,0), (0,0)\}$, where $j = 0, \ldots, 15$, the expected number of the subkey $(k_1, k_7)$ such that the equations (3) and (4) both hold together is $2^{16}$.*

For each equation (6), there are 4 values of the subkey $(k_1[j], k_7[j])$ when $(a_l[j+1], a_r[j+2]) = (0,0)$, and there is a value of the subkey $(k_1[j], k_7[j])$ when $(a_l[j+1], a_r[j+2]) = (1,0)$ or $(a_l[j+1], a_r[j+2]) = (1,1)$. Suppose $(a_l[j+1], a_r[j+2])$ is chosen uniformly from the set $\{(1,1), (1,0), (0,0)\}$, the expected number of the subkey $(k_1, k_7)$ is

$$\sum_{j=1}^{16} \binom{16}{j} \left(\frac{1}{3}\right)^j 4^j \left(\frac{2}{3}\right)^{16-j} = 2^{16}.$$

This observation is used to eliminate wrong keys for the impossible differential attack on the first 7 rounds of KASUMI.

**Precomputation.** In order to decrease the time complexity, we consider $FI$ as a big sbox, and construct two key dependent difference tables of $FI$. For all $2^{31}$ possible input pairs $(XI, XI')$ of the $FI$ function, and $2^{16}$ possible subkeys $KI$,

compute the corresponding output pairs $(YI, YI')$. Store the subkey $KI$ and output value $YI$ in a hash table $T_1$ indexed by 48-bit value $(XI\|XI'\|\Delta YI)$. Then there is one $KI$ for each index on average. Store the value $(XI, YI)$ in a hash table $T_2$ indexed by 48-bit value $(KI\|\Delta XI\|\Delta YI)$, and then each $XI$ corresponds to an index on average.

## 4 Impossible Differential Attack on the Last 7 Rounds of KASUMI

The generic 5-round impossible differential of Feistel structure is utilized to analyze 6-round KASUMI, which is: $(0, a) \overset{5R}{\nrightarrow} (0, a)$, where $a$ is a 32-bit non-zero value [5]. Combined with the Feistel structure of the round function, some special values of $a$ are selected to attack the 7-round version of KASUMI.

For the attack on the last 7 rounds, we select the 5-round impossible differential as:

$$(0, a_l\|0) \overset{5R}{\nrightarrow} (0, a_l\|0),$$

where $a_l$ is 16-bit non-zero value. The choice of difference $a_l\|0$ is to minimize the key words guessing when the differential is used to attack the last 7 rounds of KASUMI. We mount the 5-round impossible differential from round 3 to round 7, and extend one round forward and backward, respectively.

Based on observations 1 and 2, we know that, if the input difference of the second round is selected as $\Delta L_1 = (a_l\|0)$, $k_5$ and $k_7$ are not involved in the computation of the output difference $(\Delta L_2, \Delta R_2)$. Similarly, for the backward direction, the input difference of the 8th round $(\Delta L_7, \Delta R_7)$ can be obtained by avoiding guessing $(k_3, k_5)$. Apparently, $k_5$ does not affect either $(\Delta L_2, \Delta R_2)$ or $(\Delta L_7, \Delta R_7)$, which can help us to reduce the complexity of the attack.

The impossible differential attack on the last 7-round variant of KASUMI is demonstrated as follows, see also Fig. 2.

1. Choose $2^n$ structures of plaintexts, with each structure containing $2^{48}$ plaintexts $(L_1, R_1) = (*\|x, *\|*)$, where $x$ is a fixed 16-bit value, '*' takes all the possible 16-bit values. There exist $2^{95}$ pairs whose input differences are of the form $(*\|0, *\|*)$ in each structure. Query their corresponding ciphertexts $(L_8, R_8)$ and store $(L_1, R_1, L_8, R_8)$ in a hash table indexed by 32-bit values $L_{1,l} \oplus R_{8,l}$ and $R_{8,r}$. Save the plaintext-ciphertext pair, such that $\Delta L_{1,l} = \Delta R_{8,l}$ and $\Delta R_{8,r} = 0$. There are $2^{n+95-32} = 2^{n+63}$ kept pairs on average.
2. Considering the key schedule and the definition of the round function, the subkey $(k_4, k_6, k_7, k_8)$ can be deduced by guessing the 48-bit subkey $(k_1, k_2, k_3)$. Therefore we guess the subkey $(k_1, k_2, k_3)$ and compute the value $\Delta XL_{8,l} = \Delta YO_{8,l}$ for each plaintext-ciphertext pair. In accordance with the round-function FO, we get $\Delta YI_{8,1} = \Delta YO_{8,l}$. Partially decrypt $(R_{8,l}, R'_{8,l})$ to get the intermediate value $(XI_{8,1}, XI'_{8,1})$. Then obtain the candidate $k'_4$ by accessing table $T_1$.

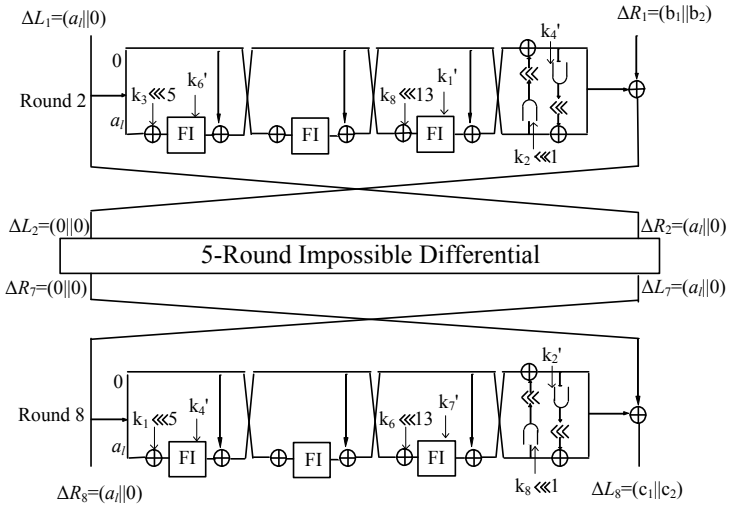


**Fig. 2.** Impossible differential attack on KASUMI reduced to rounds 2-8

3. Calculate the value $\Delta XL_{2,l} = \Delta YO_{2,l} = \Delta YI_{2,1}$, partially encrypt $(L_{1,l}, L'_{1,l})$ to get the intermediate value $(XI_{2,1}, XI'_{2,1})$, and then search the candidate $k'_6$ from table $T_1$.
4. Compute the value $\Delta XL_{2,r}$ $(\Delta YO_{2,r})$, and get the difference of intermediate value $\Delta YI_{2,3} = \Delta YO_{2,l} \oplus \Delta YO_{2,r}$. Since $\Delta XI_{2,3} = \Delta YO_{2,l}$ is known, we can get $(XI_{2,3}, XI'_{2,3})$ by a memory access to hash table $T_2$. Then partially encrypt $(XI_{2.1}, XI'_{2,1})$ to obtain $k_8$.
5. From $k_8$ and Observation 4, we get the value $\Delta XL_{8,r}$ $(\Delta YO_{8,r})$, and then obtain the difference of intermediate value $\Delta YI_{8,3} = \Delta YO_{8,l} \oplus \Delta YO_{8,r}$. Partially encrypt $(XI_{8,1}, XI'_{8,1})$ to get the value $(XI_{8,3}, XI'_{8,3})$, and then obtain the candidate of $k'_7$ through a memory access to hash table $T_1$. Thus 16-bit $k_7$, 48-bit subkey $k_4\|k_6\|k_8$ and 48-bit guessed value $k_1\|k_2\|k_3$ result in the impossible differential. Discard these 64-bit values from the list of all the $2^{64}$ possible values of the subkey $(k_4, k_6, k_7, k_8)$.
6. For each guess of $(k_1, k_2, k_3)$, there are several 64-bit key words ($k_4$, $k_6$, $k_7$, $k_8$) kept after the $2^{63+n}$-pair filters. Search for the remaining 16-bit key word $k_5$, and get the right key. Otherwise, return to Step 2, and repeat the above process.

**Complexity Evaluation.** In Step 6, the number of remaining values in the list is about $\epsilon = 2^{112}(1 - \frac{1}{2^{64}})^{2^{n+63}}$. To find a balance between the complexity of searching the right key in Step 6 and the complexity of Steps 1-5, we choose $n = 4.5$, and then $\epsilon = 2^{96}$. Then the attack needs about $2^{n+48} = 2^{52.5}$ chosen plaintexts.

In the first step, we need about $2^{n+48} = 2^{52.5}$ encryptions to get the corresponding ciphertexts. Step 2 costs $2^{n+63+32} = 2^{99.5}$ memory accesses to compute $k_4$. In Steps 3, 4 and 5, we need to access a table of size $2^{48}$ for each plaintext-ciphertext pair and subkey $(k_1, k_2, k_3)$. Step 6 requires about $2^{96} \times 2^{16} = 2^{112}$ encryptions to search for the correct key. We assume the complexity of one memory access to $T_1$ and $T_2$ to be about a one-round encryption. The total complexity of our attack is hence about $2^{n+63} \times 2^{48} \times 3/7 + 2^{112} = 2^{114.3}$ 7-round encryptions.

## 5 Impossible Differential Attack on the First 7 Rounds of KASUMI

To analyze the first 7 rounds of KASUMI, we specify the 5-round impossible differential as:

$$(0, a_l \| a_r) \stackrel{5R}{\nrightarrow} (0, a_l \| a_r).$$

Combined with the key words distribution, we mount the 5-round impossible differential from round 2 to round 6, and extend one round forward and backward respectively (see Fig. 3). The difference $a_l \| a_r$ that satisfies Observation 4 is used to make the input difference of $FI_{1,2}$ and $FI_{7,2}$ be 0. Then we utilize Observation 1 to decrease the time complexity. In this case, the difference $\Delta L_1$ and $\Delta R_6$ do not depend on the key word $k_4$ by key schedule algorithm (see Fig. 3). In the following, we demonstrate a known plaintext attack on 7-round KASUMI.

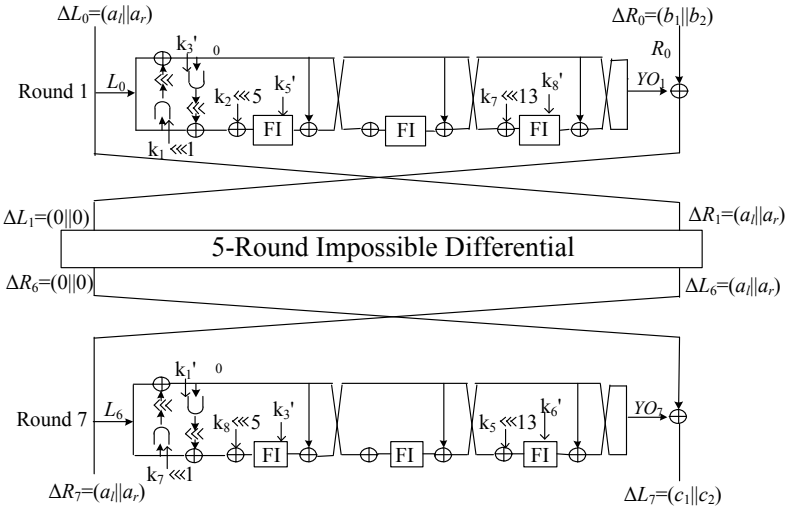


**Fig. 3.** Impossible differential attack on the first 7 rounds of KASUMI

**Data Collection.** For $2^m$ plaintexts $P(L_0, R_0)$, query their ciphertexts $C(L_7, R_7)$, and store the $(P, C)$ pairs in a hash table with index $L_0 \oplus R_7$. There are about $2^{2m-33}$ pairs whose input and output differences are $(a_l \| a_r, *)$ and $(*, a_l \| a_r)$ respectively, where '*' is any 32-bit value. Save the pairs whose differences $(a_l \| a_r)$ make the equation (5) hold. There are about $2^{2m-33} \times (3/4)^{16} = 2^{2m-39.64}$ pairs kept on average. For the remaining plaintext-ciphertext pairs, the differences satisfy $\Delta L_0 = (a_l \| a_r)$, $\Delta R_7 = (a_l \| a_r)$ and $(a_l \lll 1) \vee \neg a_r = 0xffff$. We use the difference $(a_l \| a_r)$ as the index for kept plaintext-ciphertext pairs.

**Key Recovery**

1. Guess $(k_1, k_7)$, for all the differences $(a_l \| a_r)$, apply Observation 3 to filter the pairs. Keep the pairs whose differences satisfy equations (3) and (4). By Observation 5, there are $2^{2m-39.64+16-32} = 2^{2m-55.64}$ pairs left for every $(k_1, k_7)$ on average.
2. Guess $k_5$, for each remaining pair, the input and output differences of $FI_{1,1}$ are computed as $\Delta XI_{1,1} = \Delta L_{0,l}$, $\Delta YI_{1,1} = \Delta R_{0,l}$. Then look up table $T_2$ to get the input and output values $XI_{1,1}$, $YI_{1,1}$ of $FI_{1,1}$. Compute the input values $XI_{1,3}$ and $XI'_{1,3}$ by partial encryption, and thoutput difference $\Delta YI_{1,3} = \Delta R_{0,l} \oplus \Delta R_{0,r}$. Then $k_8$ is obtained by accessing table $T_1$.
3. By partial decryption, the intermediate values $XI_{7,1}$ and $XI'_{7,1}$ are deduced from $L_6 = R_7$ and $L'_6 = R'_7$, and $\Delta YI_{7,1} = \Delta L_{7,l}$. Then access table $T_1$ to get $k_3$ and $YI_{7,1}$.
4. $XI_{7,3}$ and $XI'_{7,3}$ are deduced by partial decryption, and the output difference $\Delta YI_{7,3} = \Delta L_{7,l} \oplus \Delta L_{7,r}$, so $k_6$ is obtained by looking up in table $T_1$. Then compute $YL_1$ by the function $FL_1$, and $k_2 = (YL_{1,l} \oplus XI_{1,1}) \ggg 5$. Thus the key words $(k_2, k_3, k_6, k_8)$ produce the impossible differential, discard it from the list of the $2^{64}$ possible values and start a new guess.
5. For every guess $(k_1, k_5, k_7)$, there are about $2^{64} \times (1 - 2^{-64})^{2m-55.64}$ key words $(k_2, k_3, k_6, k_8)$ kept after the $2^{2m-55.64}$ pairs filter. Exhaustively search for the 16-bit key word $k_4$ for the kept values of key words, and get the right key. Otherwise go to Step 1, and repeat the above process.

**Complexity Evaluation.** Let $m = 62$. In the data collection process, we need $2^m = 2^{62}$ encryptions and $2^{2m-33} = 2^{91}$ computations of equation (5). There are $3^{16}$ values for $(a_l \| a_r)$ in total by Ovservation 3. For each $(k_1, k_7)$ and $a_l \| a_r$, compute the equations (3) and (4) in Step 1, which needs $2^{32} \times 3^{16} \times 1/4 \times 1/7$ encryptions of 7-round KASUMI. Steps 2-4 cost $2^{2m-55.64} \times 2^{48} \times 4 = 2^{118.36}$ accesses to memory of size $2^{48}$ and $2^{2m-55.64} \times 2^{48} = 2^{116.36}$ accesses to memory of size $2^{64}$. In Step 5, the expected number of remaining keys is $2^{34.4}$. We spend $2^{48} \times 2^{34.4} \times 2^{16} = 2^{98.4}$ 7-round computations to exhaustively search for the right key. Suppose one memory access is equivalent to one round encryption. Hence the total time complexity is about $2^{98.4} + 2^{118.36} \times 1/7 + 2^{116.36} \times 1/7 = 2^{115.8}$ 7-round encryptions, and the data complexity is about $2^{62}$ known plaintexts and the memory complexity is estimated by the storage of the pairs, which is $2^{2m-39.64} \times 16 = 2^{84.36}$ bytes.

## 6 Conclusion

In this paper, we extend the 12-year old impossible differential attack on 6-round KASUMI to 7 rounds, thereby reducing the security margin from 2 rounds to 1 round. We refine the impossible differential by selecting some special input difference values. In order to get the secret key with lower computational complexity we treat $FI$ as a big sbox and construct the difference distribution table with the dependent 16-bit subkey $KI$. Besides, we give some observations on the FL function with a special input difference, with which we give the first impossible differential attack on the first 7 rounds. The impossible differential attack on the last 7 round needs $2^{114.3}$ encryptions with $2^{52.5}$ chosen plaintexts, and $2^{115.8}$ encryptions with $2^{62}$ known plaintexts for the first 7 rounds.

**Acknowledgments.** We would like to thank anonymous reviewers for their very helpful comments on the paper. This work is supported by 973 Program(2013CB834205) and the National Natural Science Foundation of China (61133013 and 60931160442), China Postdoctoral Science Foundation(20110490442) and the European Commission under contract ICT-2007-216646 (ECRYPT II). This author Jiazhe Chen is visiting KU Leuven, ESAT/COSIC (Belgium).

## References

1. Biham, E., Biryukov, A., Shamir, A.: Miss in the Middle Attacks on IDEA and Khufu. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 124–138. Springer, Heidelberg (1999)
2. Biham, E., Dunkelman, O., Keller, N.: A Related-Key Rectangle Attack on the Full KASUMI. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 443–461. Springer, Heidelberg (2005)
3. Blunden, M., Escott, A.: Related Key Attacks on Reduced Round KASUMI. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 277–285. Springer, Heidelberg (2002)
4. Dunkelman, O., Keller, N., Shamir, A.: A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 393–410. Springer, Heidelberg (2010)
5. Kühn, U.: Cryptanalysis of Reduced-Round MISTY. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 325–339. Springer, Heidelberg (2001)
6. Kühn, U.: Improved Cryptanalysis of MISTY1. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 61–75. Springer, Heidelberg (2002)
7. Matsui, M.: New Block Encryption Algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)
8. Sugio, N., Aono, H., Hongo, S., Kaneko, T.: A Study on Integral-Interpolation Attack of MISTY1 and KASUMI. In: Computer Security Symposium 2006, pp.173–178 (2006) (in Japanese)
9. Sugio, N., Aono, H., Hongo, S., Kaneko, T.: A Study on Higher Order Differential Attack of KASUMI. IEICE Transactions 90-A(1), 14–21 (2007)

10. Sugio, N., Tanaka, H., Kaneko, T.: A Study on Higher Order Differential Attack of KASUMI. In: 2002 International Symposium on Information Theory and its Applications (2002)
11. 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification, V3.1.1 (2001)
12. 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the A5/3 Encryption Algorithms for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 4: Design and evaluation report, V6.1.0 (2002)