A Single-Key Attack on 6-Round KASUMI

Teruo Saito[1]

NEC Software Hokuriku, Ltd.
1, Anyoji, Hakusan, Ishikawa 920-2141, Japan
t-saito@qh.jp.nec.com

Abstract. KASUMI is a block cipher used in the confidentiality and integrity algorithms of the 3GPP (3rd Generation Partnership Project) mobile communications. In 2010, a related-key attack on full KASUMI was reported. The attack was very powerful and worked in practical complexity. However the attack was not a direct threat to full KASUMI because of the impractical assumptions related to the attack. Therefore, this paper concentrates on single-key attacks considered to be practical attacks. This paper proposes a single-key attack on 6-round KASUMI. The attack, which applies a technique of higher order differential attacks, requires $2^{60.8}$ data and $2^{65.4}$ encryption time. To the best of our knowledge, the attack reported in this paper is the most powerful single-key attack against reduced-round KASUMI in terms of time complexity.

Keywords: A5/3, Block cipher, GSM, Higher order differential attack, KASUMI, 3GPP.

1 Introduction

KASUMI [21] is a block cipher used in the confidentiality and integrity algorithms of the 3GPP (3rd Generation Partnership Project) [20] mobile communications, developed through the collaborative efforts of the 3GPP organizational partners. KASUMI is a modified version of the MISTY1 block cipher [14] having a provable security regarding differential and linear cryptanalysis [4, 13], optimized for implementation in hardware. It is also known as the A5/3 encryption algorithm [22] for GSM (Global System for Mobile Communications), and it will become one of the widely used block ciphers in the world.

Several cryptanalyses of KASUMI have been reported. In 2005, the first attack against full KASUMI was proposed [3]. The attack, which used the techniques of boomerang and rectangle attacks [2, 24], required the $2^{54.6}$ data and $2^{76.1}$ encryption time. In 2010, an improved attack on full KASUMI was reported [6]. The paper also proposed an attack, named sandwich attacks, and the attack required 2^{26} data and 2^{32} encryption time and 2^{32} memory. The complexity of the attack in [6] was very practical, and the authors could simulate the efficiency of their attack using a personal computer.

Both attacks described above are categorized as related-key attacks [1]. This kind of attacks requires the strong assumption that the attacker can input specific (sub)key differentials. The assumption is considered to be impractical in

most real cryptosystems that generate session keys at random. That's why, even though the two attacks are very powerful and work in practical complexity, the attacks described above are not a direct threat to full KASUMI and the cryptosystem using the cipher, e.g., the A5/3 cryptosystem.

This paper concentrates on single-key attacks since those are considered to be practical attacks. Some single-key attacks against reduced-round KASUMI have been proposed. In 2001, an impossible differential attack on 6-round KASUMI was reported [10]. The paper of [10] showed an attack using a 5-round impossible differential, which requires 2^{55} data and 2^{100} encryption time. In 2006, an integral-interpolation attack on 6-round KASUMI was reported [17]. The paper of [17] showed a 16th order differential and was applied to an attack that requires 2^{48} data and $2^{126.2}$ encryption time.

This paper proposes an improved single-key attack on 6-round KASUMI. The attack applies a technique of higher order differential attacks [9, 11]. We firstly show a 48th order differential of 4-round KASUMI by extending the previously known 3-round characteristic. We secondly demonstrate an attack using the 48th order differential. Our attack requires $2^{60.8}$ data and $2^{65.4}$ encryption time. The summary of the attacks on KASUMI is listed in Table 1. To the best of our knowledge, the attack reported in this paper is the most powerful single-key attack against reduced-round KASUMI in terms of time complexity.

Section 2 describes the structure of KASUMI. Section 3 explains higher order differential attacks. Section 4 shows a higher order differential of KASUMI and its application to attacks. Finally, section 5 concludes the paper and suggests future work.

Table 1. Summary of the attacks on KASUMI

No. of rounds	Key constraint	Data	Time	Method
5	2 related keys	2^{19}	$2^{32.7}$	Related-key attack [5]
5	Single key	$2^{22.1}$	$2^{60.7}$	HOD attack [19]
5	Single key	$2^{28.9}$	$2^{31.2}$	HOD attack [18]
6	2 related keys	$2^{18.6}$	$2^{113.6}$	Related-key attack [5]
6 (2-7)	Single key	2^{48}	$2^{126.2}$	II attack [17]
6 (2-7)	Single key	2^{55}	2^{100}	ID attack [10]
6 (2-7)	Single key	$2^{60.8}$	$2^{65.4}$	HOD attack (this paper)
8	4 related keys	$2^{54.6}$	$2^{76.1}$	RKR attack [3]
8	4 related keys	2^{26}	2^{32}	RKS attack [6]

HOD attack : Higher order differential attack
II attack : Integral-interpolation attack
ID attack : Impossible differential attack
RKR attack : Related-key rectangle attack
RKS attack : Related-key sandwich attack

2 KASUMI

This section describes the structure of KASUMI. For a more detailed description refer to the specification document [21].

KASUMI is a 64-bit block cipher with a 128-bit secret key. It has a recursive Feistel structure in the same manner as the MISTY1 construction. KASUMI has 8 rounds; each round is composed of two functions: the FO function that has 3 rounds of the FI function, and the FL function that has a Feistel structure performing logical AND/OR operations with subkeys. The order of the two functions depends on the round number: in the even rounds the FO function is applied first, and in the odd rounds the FL function is applied first. The FI function is a 4-round unbalanced Feistel structure using two types of S-boxes, 9 bits and 7 bits in size.

The KASUMI encryption function is shown in Fig. 1. In this paper, bitwise AND, OR, exclusive OR, and one bit left rotation operations are denoted as $\cap$, $\cup$, $\oplus$, and $\lll$, respectively. We denote plaintext as P and ciphertext as C. We denote the subkey input to the FOi function as KO_i, the subkey input to the $FIij$ function as KI_{ij}, and the subkey input to the FLi function as KL_i.

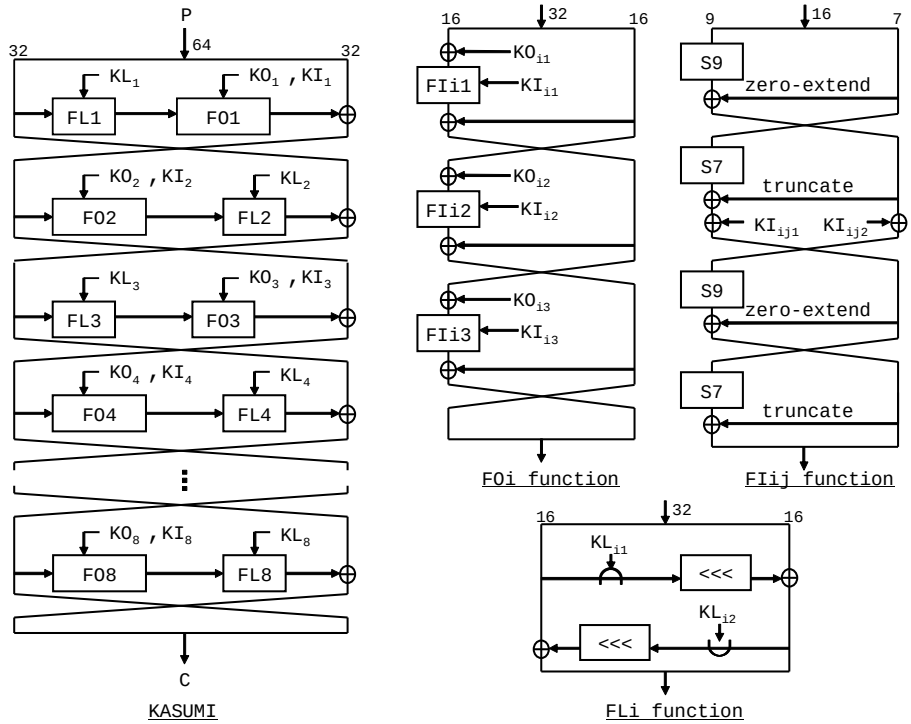

Fig. 1. Structure of KASUMI

The i-th-round output data is defined as X^i for the internal variables. In KASUMI, $0 \leq i \leq 8$, so $X^0 = P$ and $X^8 = C$. Considering the Feistel structure of KASUMI, 64-bit internal data Y consists of left and right 32-bit portions defined as Y_L and Y_R. Other divisions are also defined with regard to the FO function:

$$Y = Y_3 \parallel Y_2 \parallel Y_1 \parallel Y_0 \ , \ \ Y_i \in GF(2)^{16} \ .$$

The $\parallel$ indicates data concatenation. We denote the i-th ($0 \leq i < n$) bit of Z as $Z[i]$ and the range from the i-th bit of Z to the j-th bit of Z as $Z[i-j]$. For example, the leftmost 16 bits of plaintext P is denoted as

$$P[63-48] = P_L[31-16] = P_3 = X_3^0 \ .$$

The key schedule divides the 128-bit secret key into 16-bit data blocks K_i ($1 \leq i \leq 8$) and generates subkeys K_i'. Since the characteristics of the key schedule are not used in this paper, we omit a detailed description of its manner for deriving round keys.

3 Higher Order Differential Attacks

Here, we describe both the higher order differential characteristic and the method for solving the attack equation used in higher order differential attacks.

3.1 Higher Order Differential Characteristic

Let the encryption function be the $E(X;K)$ defined by Eq. (1) with data X and key K as input and data Y as output. Here, $X \in GF(2)^n$, $K \in GF(2)^s$, and $Y \in GF(2)^m$.

$$Y = E(X;K) \tag{1}$$

Let $(A_1, A_2, \cdots, A_d)$ be d linearly independent vectors on $GF(2)^n$, and denote the subspace of $GF(2)^d$ expanded by them as $V^{(d)}$. Then the d-th order differential with respect to X of $E(X;K)$ is defined by Eq. (2). Here, the symbol $\bigoplus_{A \in V^{(d)}}$ denotes the total sum by exclusive OR.

$$\Delta_{V^{(d)}} E(X;K) = \bigoplus_{A \in V^{(d)}} E(X \oplus A;K) \tag{2}$$

We call the subspace $V^{(d)}$ the variable sub-blocks and the subspace other than $V^{(d)}$ the fixed sub-blocks. In the following, we abbreviate $\Delta_{V^{(d)}}$ as $\Delta^{(d)}$, when the subspace $V^{(d)}$ is clearly understood. If the Boolean degree of $E(X;K)$ with respect to X is N, Eq. (3) necessarily holds without dependence on X.

$$\begin{cases} \Delta^{(N)} E(X;K) = constant \\ \Delta^{(N+1)} E(X;K) = 0 \end{cases} \tag{3}$$

3.2 Attack Equations

This section explains the equations required for an attack using the higher order differential characteristic described in section 3.1. If encryption function E comprises R rounds of functions F^i $(1 \leq i \leq R)$, the $(R-1)$th-round output for input X is expressed as

$$Y^{R-1}(X) = F^{R-1}(F^{R-2}(\cdots F^2(F^1(X;K_1);K_2)\cdots;K_{R-2});K_{R-1}) \ , \tag{4}$$

where K_i is the subkey input in the i-th round. If the Boolean degree of $Y^{R-1}(X)$ with respect to X is N, Eq. (5) necessarily holds according to Eq. (3).

$$\begin{cases} \Delta^{(N)} Y^{R-1}(X) = constant \\ \Delta^{(N+1)} Y^{R-1}(X) = 0 \end{cases} \tag{5}$$

Denoting the ciphertext for input X as $C(X)$ and the function for obtaining Y^{R-1} from $C(X)$ as F^{-1}, we obtain

$$Y^{R-1}(X) = F^{-1}(C(X);K_R) \ . \tag{6}$$

Substituting Eq. (6) into Eq. (5), we obtain

$$\begin{cases} \bigoplus_{A \in V^{(N)}} F^{-1}(C(X \oplus A);K_R) = constant \\ \bigoplus_{A \in V^{(N+1)}} F^{-1}(C(X \oplus A);K_R) = 0 \end{cases} \ . \tag{7}$$

Equation (7) holds when the final round subkey K_R is correct, so the true key, K_R, can be determined by solving Eq. (7). Therefore, Eq. (7) is called the attack equation.

3.3 Algebraic Method

One method of solving the attack equation presented in section 3.2 is an algebraic method. This method regards attack equations as functions on $GF(2)$ and subjects them to linearization, that is, transforms them into linear equations, by redefining the higher degree terms related to the key as new first-degree unknown terms [15, 16]. This approach has the potential to reduce the time complexity of solving attack equations.

Let Eq. (7) be an n-bit attack equation derived using a d-th order differential. Denoting the key contained in the attack equation as $K_R = (K_{R1}, K_{R2})$, we determine K_{R1} by an exhaustive search and obtain K_{R2} by using an algebraic method. Here, we let L denote the number of unknown terms excluding constant terms included in the linearized attack equation with regard to K_{R2}. As for K_{R1}, we let $K_{R1} \in GF(2)^{s_1}$.

The K_{R2} for the true key K_{R1} can be obtained by solving the $L \times (L+1)$ extended coefficient matrix obtained from L independent linearized equations. Here, the coefficient matrix includes constant terms. However, if K_{R1} is guessed incorrectly, K_{R2} will be determined based on that guess, which means that false K_{R1} keys must be excluded. If $L+m$ linearized equations have been prepared

for determining K_{R2}, the probability that the linearized equations for a false K_{R1} key are not inconsistent is estimated to be 2^{-m}. Thus, by using $L+m$ linearized equations whose probability of not being inconsistent for a false K_{R1} key is extremely small, that is, that satisfy the condition $2^{-m} \times 2^{s_1} \ll 1$, false K_{R1} keys can be rejected with very high probability.

Because the attack equation is an n-bit attack equation, n linearized equations are obtained with one set of d-th order differentials. Therefore, the number of plaintexts needed to obtain $L+m$ linearized equations is given by

$$D = 2^d \times \left\lceil \frac{L+m}{n} \right\rceil . \tag{8}$$

Furthermore, to obtain n linearized equations, the round function must be calculated D times for each of L unknown terms and 1 constant term. Here, considering that the time complexity for Gaussian elimination to solve the simultaneous equation is negligibly small, the time complexity for solving the attack equation is equivalent to that of calculating the coefficient matrix. Thus, considering that K_{R1} is to be determined by an exhaustive search, time complexity T is given by

$$\begin{aligned} T &= 2^{s_1} \times D \times (L+1) \\ &= 2^{s_1+d} \times \left\lceil \frac{L+m}{n} \right\rceil \times (L+1) . \end{aligned} \tag{9}$$

Here, time complexity signifies the number of times the round function is calculated.

4 Higher Order Differential Attack on 6-Round KASUMI

The following section describes a higher order differential characteristic of KASUMI and an attack that make use of this characteristic.

4.1 Higher Order Differentials of KASUMI

Here, we describe higher order differential characteristics of KASUMI. First, we present Theorem 1 from [19] for KASUMI. In this theorem, α and β denote fixed and variable 16-bit sub-blocks, respectively.

Theorem 1 *Given a 16th order differential in the form of plaintext $P \in (\alpha, \alpha, \beta, \alpha)$ in KASUMI, intermediate data X_L^3 satisfies Eq. (10).*

$$\Delta^{(16)} X_L^3[24-16] = 0 \tag{10}$$

Theorem 2 can be obtained by adding 1 round to the upper side of Theorem 1 characteristics. However, Theorem 2 is only satisfied from the 2nd to 5th rounds since the even round function is not equal to the odd round function.

Theorem 2 *Given a 48th order differential in the form of 2nd-round input* $X^2 \in (\beta, \alpha, \beta, \beta)$ *in KASUMI, intermediate data* X_L^5 *satisfies Eq. (11).*

$$\Delta^{(48)} X_L^5[24-16] = 0 \tag{11}$$

The 48th order differential of 4-round KASUMI is illustrated in Fig. 2.

Proof. Data X_L^1 is equal to X_R^2 since KASUMI is the Feistel structure. The higher order differential characteristic is, therefore, unchanged. In addition, though 2^{16} values of random data are output from the $FL2$ function, X_L^2 can be given exhaustively by giving 2nd-round input X_R^1, exhaustively. Thus, since the value of the 16th order differential of Eq. (10) appears 2^{32} times in the intermediate data X_L^5 according to Theorem 1, its total sum is zero. □

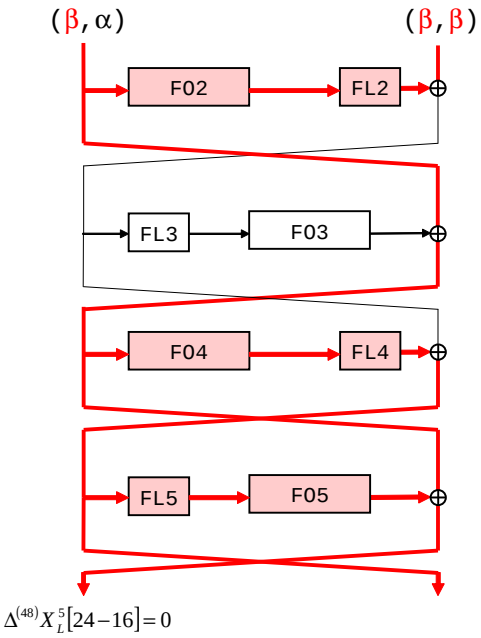

Fig. 2. The 48th order differential of 4-round KASUMI

4.2 Derivation of Attack Equation

In this section we explain the derivation of the attack equation using the 48th order differential characteristic described in section 4.1. The structure of 6-round KASUMI targeted by this attack is shown in Fig. 3.

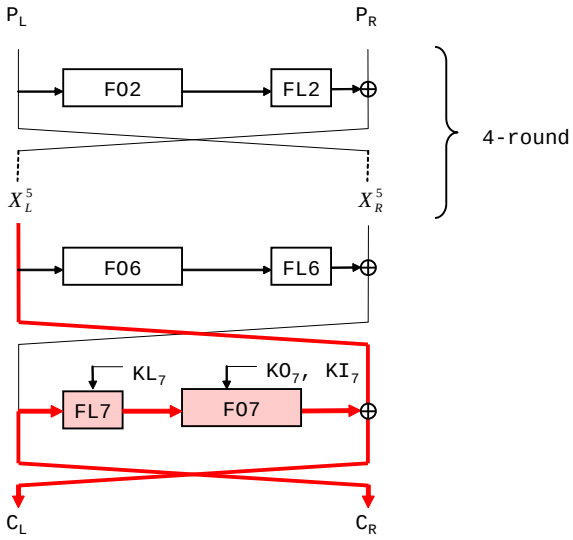

Fig. 3. Six-round KASUMI

We can derive Eq. (12) as the attack equation from Fig. 3 and Eq. (11).

$$\bigoplus_{A \in V^{(48)}} \{\ FO7(FL7(C_R; KL_7); KO_7, KI_7)[24-16] \oplus C_L[24-16]\ \}$$
$$= \Delta^{(48)} X_L^5[24-16] = 0 \tag{12}$$

To solve attack equation (12), we denote the function G_9 for obtaining $X_L^5[24-16]$ from the 41 bits of the ciphertext C and the 82 bits of the subkey $SK = \{KO_{71}, KO_{72}, KI_{712}, KI_{722}, KL_7\}$ relevant to the attack equation as:

$$X_L^5[24-16] = G_9(C; SK)\ . \tag{13}$$

We get the attack equation (14) from Eq. (12) and (13).

$$\bigoplus_{A \in V^{(48)}} G_9(C(X \oplus A); SK) = 0 \tag{14}$$

4.3 Complexity of the Attack

In this section, we perform a detailed estimation of the amount of data and time complexity required for solving the attack equation presented in section 4.2.

First, we express Eq. (14) as a polynomial on $GF(2)$ by formula manipulation using a mathematical software (Mathematica) and derive the number of unknown coefficients Li. We also derive the number of unknown coefficients $L'i$ for the equivalent subkey obtained by the same modification in [18, 19]. The values of Li and $L'i$ obtained in this way are listed in Table 2.

Table 2. Number of unknown coefficients in the attack equation

Bit position, i	No. of unknowns for the original subkey, Li	No. of unknowns for the equivalent subkey, $L'i$
16th bit	34007	32321
17th bit	34086	31998
18th bit	32425	30583
19th bit	32213	30499
20th bit	32684	30852
21st bit	34285	32435
22nd bit	33309	31265
23rd bit	33927	31403
24th bit	36078	33616
Total	67746	62958

The number of plaintexts D required to collect the linear equations for 9 bits of Eq. (14) can be obtained by substituting the total number of unknown coefficients, $L'i$, into Eq. (8). Furthermore, there is no guessing key bits for solving Eq. (14), so $s_1 = 0$. Accordingly, from the condition for eliminating false keys, $2^{-m+s_1} << 1$, if we let $m = 10$,[1] we have

$$D = 2^{48} \times \left\lceil \frac{62958 + 10}{9} \right\rceil \approx 2^{60.78} . \tag{15}$$

In addition, the time complexity required for calculating the coefficients of the linear equation is obtained by substituting the sum of the numbers of unknown coefficients, $L'i$, into Eq. (9). Furthermore, as explained in section 3.3, the calculations must be performed 2^d times to determine the unknown coefficients of linearized equations. However, in the case that the unknown coefficients of the linearized equations can be calculated independently, it is known that time complexity T can be reduced provided that the size of data required for calculating the unknown coefficients is w bits and the relation $w < d$ is satisfied [8]. Specifically, it was shown in [8] that calculations for a value that appears an even number of times can be omitted since performing an exclusive-OR operation on the same value an even number of times results in a value of 0. With this technique, only the values of w-bit data that appear an odd number of times need to be used to calculate the unknown coefficients. As a result, time complexity T as expressed by Eq. (9) takes on the form of Eq. (16) when the relation $w < d$ is satisfied.[2]

$$T = 2^{s_1+w-1} \times \left\lceil \frac{L + m}{n} \right\rceil \times (L + 1) \tag{16}$$

[1] $10^{-3} << 1$

[2] There are about 2^{w-1} instances of ciphertext data on average for which the w-bit value appears an odd number of times.

Here, $d = 48$ and $w = 41$, so the condition $w < d$ is satisfied, we have

$$T = 2^{0+41-1} \times \left\lceil \frac{62958 + 10}{9} \right\rceil \times (62958 + 1) \approx 2^{68.72} \ . \tag{17}$$

This time complexity signifies the number of times one round function is performed.

Furthermore, in the estimation of time complexity below, we assumed that the processing times for one S-box lookup and for two logical operations are the same.[3] On the basis of this assumption, the estimated processing time of the one round function including the exclusive-OR of the Feistel structure is 55 logical operations. The required calculations of the $FO7$ function are illustrated in Fig. 4. In Fig. 4, EKI means the equivalent keys of KI_7. From Fig. 3 and Fig. 4, determining the coefficients of linearized equation (14) requires the calculation of the $FL7$ function, the 6 S-box lookups and 13 exclusive OR operations including the exclusive-OR of the Feistel structure. Thus, converting T to a number of 6-round encryptions, we get

$$T \approx 2^{68.72} \times \frac{6 + 2 \times 6 + 13}{55} \times \frac{1}{6} \approx 2^{65.31} \ . \tag{18}$$

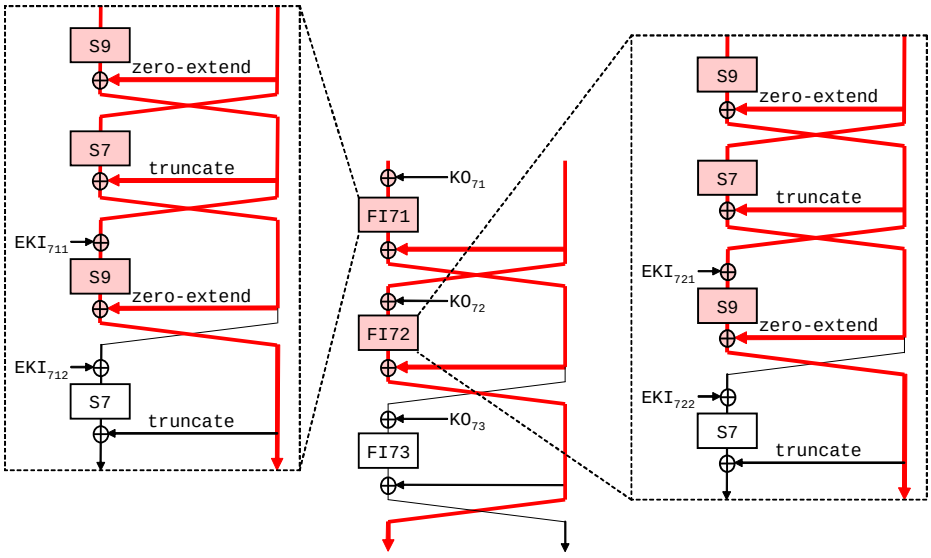

Fig. 4. The required calculations of the $FO7$ function

[3] We assumed that an S-box lookup can be achieved by two instructions for calculating an address and loading data. This assumption overestimates the time complexity described in this paper.

5 Conclusion and Future Work

This paper reports the higher order differential attack of 6-round KASUMI. This attack requires $2^{60.8}$ data and $2^{65.4}$ encryption time. The type of our attack is categorized as a single-key attack. This type of attack is considered to be a more practical attack than a related-key attack. Our attack is not a direct threat to full KASUMI, but to the best of our knowledge, the attack proposed in this paper is the most powerful single-key attack in terms of time complexity.

In another interesting topic, the comparison between MISTY1 and KASUMI was described in [6]. The authors of [6] argued that the transition from MISTY1 to KASUMI led to a much weaker cryptosystem. However, this argument is appropriate for only a situation in which related-key attacks can be mounted. The comparison had to be done on the same situation. The best attacks on MISTY1 and KASUMI are listed in Table 3.

Table 3. The best attacks on MISTY1 and KASUMI

Cipher	No. of rounds	Type of attacks	Data	Time	Method
MISTY1	7	Single-key	$2^{54.1}$	$2^{120.6}$	HOD attack [23]
KASUMI	6 (2-7)	Single-key	$2^{60.8}$	$2^{65.4}$	HOD attack (this paper)
MISTY1	7 (2-8)	Related-key	2^{54}	$2^{55.3}$	RKAB attack [12]
KASUMI	8	Related-key	2^{26}	2^{32}	RKS attack [6]

HOD attack : Higher order differential attack
RKAB attack : Related-key amplified boomerang attack
RKS attack : Related-key sandwich attack

From Table 3, the security margin of KASUMI, which is the modified version of MISTY1, is greater than that of MISTY1 regarding single-key attacks. However, the security margin of KASUMI is less than that of MISTY1 regarding related-key attacks because the key schedule of KASUMI is too simple to be secure against related-key attacks. Therefore, KASUMI is still stronger than MISTY1 in practical use.

Finally, we suggest future work. It is known that the amount of data and time complexity can be reduced if any of the L unknown coefficients have a linear sum relation in the linearized equations [7]. In section 4.3, we could not calculate the rank of $L \times (L+2)$ coefficient matrix because of the computational difficulty to perform the Gaussian elimination. If we can derive the upper bound of rank by dividing the attack equation to multiple linearized equations, the data and time complexity must be reduced.

Acknowledgments. I greatly thank Maki Shigeri and Hirokatsu Nakagawa for their useful comments to improve the result of this paper. I also express special

thanks to Erin Hayashi who checked this paper from the viewpoit of English usage.

References

1. Biham, E.: New Types of Cryptanalytic Attacks Using Related Keys. J. Cryptology 7(4), pp. 229–246 (1994)
2. Biham, E., Dunkelman, O., Keller, N.: The Rectangle Attack - Rectangling the Serpent. In: Pfitzmann, B. (ed.) EUROCRYPT 2001, LNCS, vol. 2045, pp. 340–357. Springer, Heidelberg (2001)
3. 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)
4. Biham E., Shamir A.: Differential Cryptanalysis of DES-Like Cryptosystems. J. Cryptology 4(1), pp. 3–72 (1991)
5. 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)
6. Dunkelman, O., Keller, N., Shamir, A.: A Practical-Time 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)
7. Hatano Y., Tanaka H., Kaneko T.: Optimization for the Algebraic Method and Its Application to an Attack of MISTY1. IEICE Transactions 87-A(1), pp. 18–27 (2004)
8. Igarashi, Y., Kaneko, T.: The 32nd-order differential attack on MISTY1 without FL functions. In: 2008 International Symposium on Information Theory and its Applications, WTI-4-4 (2008)
9. Knudsen L.R.: Truncated and Higher Order Differentials. In: Preneel B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995)
10. Kühn U.: Cryptanalysis of Reduced-Round MISTY. In: Pfitzmann B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 325–339. Springer, Heidelberg (2001)
11. Lai X.: Higher Order Derivatives and Differential Cryptanalysis. In: Symposium on Communication, Coding and Cryptography, pp. 227–233. Kluwer Academic Publishers (1994)
12. Lee E., Kim J., Hong D., Lee C., Sung J., Hong S., Lim J.: Weak-Key Classes of 7-Round MISTY 1 and 2 for Related-Key Amplified Boomerang Attacks. IEICE Transactions 91-A(2), pp. 642–649 (2008)
13. Matsui M.: Linear Cryptanalysis of the Data Encryption Standard. In: Helleseth T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
14. Matsui M.: New Block Encryption Algorithm MISTY. In: Biham E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)
15. Moriai S., Shimoyama T., Kaneko T.: Higher Order Differential Attak of CAST Cipher. In: Vaudenay S. (ed.) FSE 1998. LNCS, vol. 1372, pp. 17–31. Springer, Heidelberg (1998)
16. Shimoyama T., Moriai S., Kaneko T., Tsujii S.: Improved Higher Order Differential Attack and Its Application to Nyberg-Knudsen's Designed Block Cipher. IEICE Transactions 82-A(9), pp. 1971–1980 (1999)

17. 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)
18. Sugio, N., Aono, H., Hongo, S., Kaneko, T.: A Study on Higher Order Differential Attack of KASUMI. IEICE Transactions 90-A(1), pp. 14–21 (2007)
19. 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)
20. 3rd Generation Partnership Project (3GPP), `http://www.3gpp.org/`
21. 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, V.3.1.1 (2001)
22. 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)
23. Tsunoo Y., Saito T., Shigeri M., Kawabata T.: Security Analysis of 7-Round MISTY1 against Higher Order Differential Attacks. IEICE Transactions 93-A(1), pp. 144–152 (2010)
24. Wagner, D.: The Boomerang Attack. In: Knudsen, L.R. (ed.) FSE 1999, LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)