3-5 A Study on Higher Order Differential Cryptanalysis of 64 Bit Block Cipher KASUMI

TANAKA Hidema, SUGIO Nobuyuki, and KANEKO Toshinobu

In this paper, we show the strength of 128 bit secret key -64 bit block cipher KASUMI which is the standard cipher algorithm in the third generation mobile phone system, against higher order differential attack. KASUMI is a variant of MISTY1 which has provable security against linear and differential cryptanalysis. Our attack algorithm is a chosen plaintext attack and uses higher order differential property. We found an effective choice of plaintexts for the attack by computer simulations. When the effective chosen plaintexts are used, 5 round KASUMI (original has 8 round) can be attacked by 2^{22} chosen plaintexts and 2^{63} computational cost.

Keywords
Chosen plaintext attack, Block cipher, Higher order differential cryptanalysis, Probabilistic higher order differential, 3GPP

1 Introduction

KASUMI[3] is a 64-bit block cipher developed by 3GPP based on Mitsubishi Electric Corporation's MISTY1[7]. KASUMI builds upon the demonstrated security of MISTY1 against linear and differential cryptanalysis and also features improved security against algebraic method, the weak point of MISTY1. Developed for use in third-generation mobile phone systems, KASUMI is compatible with small hardware structures and high processing speeds.

Although 3GPP has itself demonstrated the security of KASUMI, independent results are also available, such as those in references[1] and[9]. Reference[1] deals with the evaluation of strength against related-key attacks. This type of attack identifies secret keys using differential cryptanalysis given a relationship between the secret keys of users A and B. As KASUMI is intended for mobile phones, this type of attack is easily possible, presenting the attacker with extremely advantageous conditions. Blunden et al. attacked five-round and six-round KASUMI and claimed that five-round KASUMI can be attacked with a computational cost of 2^{33} calculations, while six-round KASUMI can be attacked with a computational cost of 2^{112} calculations. Reference [9] presents an evaluation of the strength of modified KASUMI, i.e., without FL functions, based on higher order differential cryptanalysis, a type of algebraic method discussed in this paper. Results show that four-round KASUMI without FL functions can be attacked with 1,416 chosen plaintexts and 2^{22} calculations.

In this study we improved the attack method developed in Reference[9] and succeeded in attacking five-round KASUMI with FL functions. This is the highest achievement so far using chosen plaintext attacks. This method is based on discovering the most effective selection method for the chosen plaintexts, which are arranged in sub-block

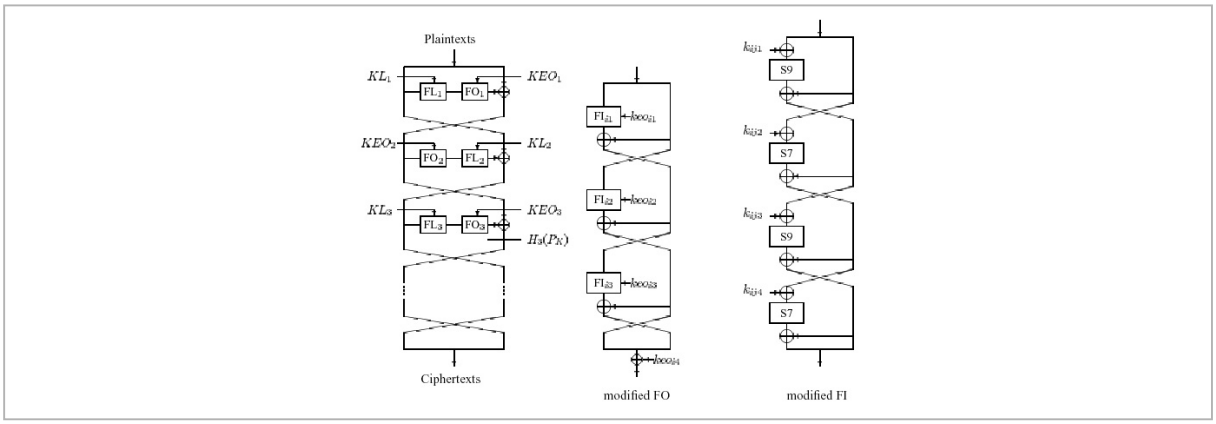

Fig.1 *Modified MISTY (K and K_{ijk} each express the equivalent sub-key.)*

units. We also successfully suppressed an explosive increase in the number of independent unknowns in algebraic method by determining a portion of unknowns in the derived attack equation by brute force search. Consequently, we found that five-round KASUMI can be attacked with 2^{22} chosen plaintexts and 2^{63} calculations. Section **2** below shows the structure of KASUMI. Section **3** outlines higher order differential cryptanalysis. In particular, see Article **3-4** for details of algebraic method. Section **4** discusses higher order differential cryptanalysis applied against KASUMI. Section **5** provides a summary.

2 64-bit block cipher KASUMI

KASUMI is a 64-bit block cipher with a 128-bit secret key. Figure 1 shows the structure of modified KASUMI. Modified KASUMI has a shifted position with reference to the original KASUMI using keys equivalent to the sub-keys used in each round; this shift allows for simplification of the expression of the attack equation, as discussed later. The basic structure is a Feistel structure similar to MISTY. Each round consists of 32-bit input/output FO and FL functions. In its specifications, modified KASUMI features eight rounds. Each FO function consists of three rounds of FI functions. Each FI function is composed of two non-linear functions, S7 and S9, known as S-boxes. S7 and S9 correspond to seven-bit and nine-bit input/output, respectively, forming an asymmetric Feistel structure. The orders are 3 and 2, respectively. FL functions are linear functions, as shown in Fig.2. However, it should be noted that the keys are sometimes used with OR operations, which are non-linear.

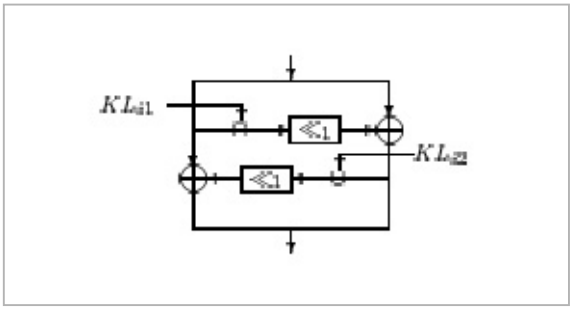

Fig.2 *Variables used in this paper*

3 Higher order differential cryptanalysis

3.1 Higher order differential

Let us consider $F(X;K)$, which is a function of $GF(2)^n \times GF(2)^s \rightarrow GF(2)^n$.

$$Y=F(X;K)$$
$$X \in GF(2)^n,\ Y \in GF(2)^n,\ K \doteqdot GF(2)^s \quad (1)$$

With $(a_0, a_1, ..., a_{N-1})$, a linearly independent set of vectors in $GF(2)^n$, we denote the subspace spanned by $(a_0, a_1, ..., a_{N-1})$ as $V[a_0, a_1, ..., a_{N-1}]$. Denoting the N-th differential of $F(X;K)$ with respect to X as $\Delta^{(N)}_{V_{[a_0,a_1,...,a_{N-1}]}}$, we can calculate as follows:

$$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}} F(X;K) = \sum_{A \in V_{[a_0,a_1,\ldots,a_{N-1}]}} F(X+A;K) \quad (2)$$

In the following, $\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}}$ is abbreviated as $\Delta^{(N)}$ when $V[a_0, a_1, \ldots, a_{N-1}]$ is obvious. If $\deg_X\{F(X;K)\}=d$ holds, the following property holds:

Property 1

$$\deg_X\{F(X;K)\} = d \rightarrow \begin{cases} \Delta^{(d+1)}F(X;K) = 0 \\ \Delta^{(d)}F(X;K) = \text{const.} \end{cases} \quad (3)$$

3.2 Attack equation

Figure 3 shows the last round of an r-round Feistel block cipher. Output $H^{(r)}(X)$ from round $(r-2)$ can be calculated as follows:

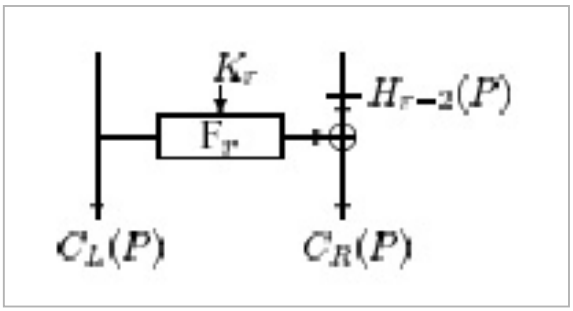

Fig.3 Increase in order due to formal analysis (Sub-keys are omitted from the figure.)

$$H^{(r)}(X) = \tilde{F}(X;K^{(1,2,\ldots,(r-2))}) \quad (4)$$

Here, $\tilde{F}(\cdot)$ is a function of $GF(2)^n \times GF(2)^{s\times(r-2)} \rightarrow GF(2)^n$, and $K^{(1,2,\ldots,(r-2))}$ are the keys for round 1 to round $(r-2)$. As such, $H^{(r)}(X)$ can be calculated from the plaintexts. On the other hand, the ciphertexts can be used to calculate as follows, by estimating key $K^{(r)}$ for the last round:

$$H^{(r)}(X)=F(C_L(X);K^{(r)})+C_R(X) \quad (5)$$

If $\deg_X\{H^{(r)}(X)\}=d$ holds, the following equation holds:

$$\Delta^{(d)}\tilde{F}(X;K^{(1,2,\ldots,(r-2))}) = \text{const} \quad (6)$$

From Equations (4), (5), and (6), the following expression is derived:

$$\sum_{A \in V_{[a_0,a_1,\ldots,a_{d-1}]}} \{F(C_L(X+A);K^{(r)}) + C_R(X+A)\} = \text{const} \quad (7)$$

If the value for "const" is determined, the solution of this equation provides the value for $K^{(r)}$. Thus, this equation is hereinafter referred to as the attack equation.

3.3 Solution of the attack equation using brute force search

Using a brute force search to solve the attack equation means that Equation (7) is verified for all possible values of $K^{(r)}$. Applying the N-th differential to s-bit sub-keys entails a computational cost of at least $2^n \times 2^s$ F-function calculations. This method generally involves the largest computational cost but the least number of chosen plaintexts.

3.4 Solution of the attack equation using algebraic method

Let us consider applying the algebraic method presented in Reference[8]. This method transforms the attack equation into a set of linear equations, leading to a significant reduction in computational cost. The details of this method are discussed in Article **3-4**. Taking L as the total number of independent unknowns redefined in the linearization, and H as the width of the attack equation, this method requires $\left\lfloor \frac{L}{H} \right\rfloor \times 2^N$ chosen plaintexts and $\left\lfloor \frac{L}{H} \right\rfloor \times 2^N \times L$ F-function calculations. Relative to a brute force search, the number of required chosen plaintexts increases significantly; however, the computational cost becomes negligibly small.

4 Higher order differential properties of modified KASUMI

4.1 Effective selection of chosen plaintexts

The order for higher order differential cryptanalysis depends on the order of the F functions. However, effective determination of the input value can decrease the apparent order of the F functions. The order for higher order differential cryptanalysis has a large effect both on the increase in the number of chosen plaintexts and on computational cost; it is thus important to minimize the number of

rounds.

Due to the structure of the FO functions in KASUMI, the plaintexts can be divided into sub-blocks as follows:

$$P=(X_7,X_6,X_5,X_4,X_3,X_2,X_1,X_0)$$
$$X_i\in\begin{cases}GF(2)^7, i=even\\ GF(2)^9, i=odd\end{cases} \quad (8)$$

In this study each sub-block was allocated either to the variable sub-block or to the constant sub-block to search for the effective chosen plaintexts. Computer simulations were performed with the sixteenth differentials as shown below; it was found as a result that some of the sub-blocks in the third-round output featured 0 value sixteenth differentials.

$$P_K=(0,0,0,0,X_3,X_2,0,0)$$
$$X_3,X_2:\text{variable}\qquad 0:\text{fixed} \quad (9)$$

Let $H_3(P_K)$ be the output from the third round, as follows:

$$H_3(P_K)=(h_3,h_2,h_1,h_0)$$
$$\begin{cases}h_3,h_1\in GF(2)^7\\ h_2,h_0\in GF(2)^9\end{cases} \quad (10)$$

The discovered property can be expressed as $\Delta^{(16)}h_2(P_K)=0$.

4.2 Derivation of the attack equation against five-round KASUMI

Figure 4 shows the discovered property. Based on this property, the following attack equation is derived:

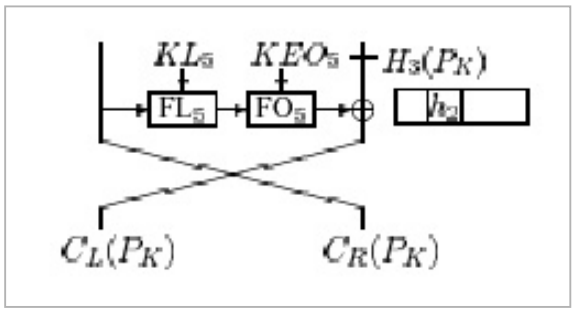

Fig.4 FL ij and input to the k-th S-box

$$\Delta^{(16)}\{FO_5(FL_4(C_R(P_K);KL_5);KEO_5)+C_L(P_K)\}=\Delta^{(16)}h_2(P_K)=0 \quad (11)$$

This equation contains the following unknowns:

$$\begin{cases}KL_5=\{KL_{51},KL_{52}\}:32[bit]\\ KEO_5=\{k_{511},k_{512},k_{513},k_{521},k_{522},k_{523},\}:50[bit]\end{cases} \quad (12)$$

Figure 5 shows the relationship between these quantities. Solving Equation (11) enables determination of the (32+50)-bit sub-keys.

4.3 Number of plaintexts and required computational cost

This attack uses a brute force search to determine the 32-bit unknown variables and uses algebraic method to determine the 50-bit unknowns.

Let us estimate the total number of independent unknowns for the sub-keys determined through algebraic method. Order analysis is performed taking into account that the order of S9 is 2 and the order of S7 is 3; we must also consider that some of the sub-keys are input to more than a single S-box. As a result, we find that the order of k_{511} and k_{521} is 4, the order for k_{512} and k_{522} is 3, and the order for k_{513} and k_{523} is 2. (See Fig.5.) Consequently, the number of independent unknowns is estimated as follows:

$$L=2\times({}_9C_3+{}_9C_2+{}_9C_2)+2\times({}_7C_2+{}_7C_1)+2\times{}_9C_1$$
$$=494$$

When finding the unknowns using brute force search, the attack equation will hold with both true and false values if the width of the equation is smaller than the number of unknowns. Thus, two or more equations are required to remove such false keys. Assuming that m equations are prepared, the required value for m to determine the true 32-bit values for the unknowns should be in a range that satisfies $2^{32}\times 2^{-m}<1$. As setting $m=33$ can eliminate the false keys, adding this value 33 to $L=494$ yields 527 as the number of required equations.

As the attack equation is derived based on 9-bit $h_2(P_K)$, nine equations can be derived from a set of sixteenth differentials. Thus, the attack requires $\left\lfloor\frac{527}{9}\right\rfloor\times 2^{16}\approx 2^{22}$ chosen plaintexts and $\left\lfloor\frac{527}{9}\right\rfloor\times 2^{16}\times 494\approx 2^{63}$ F-function calculations.

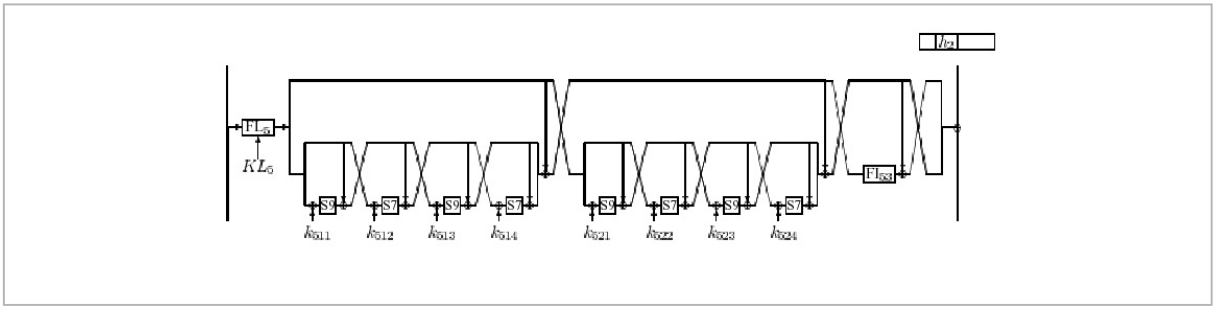

Fig.5 *Movement of equivalent sub-key K in the last round*

5 Conclusions

The current study found that five-round KASUMI can be attacked with 2^{22} plaintexts and 2^{63} calculations. This attack is based on higher order differential cryptanalysis and combines brute force search and algebraic method. Results under this method significantly surpass those described elsewhere to date. KASUMI is the standard cipher algorithm for third-generation mobile phone systems. However, as it can be implemented in small hardware structures, other applications are also planned. The results of the attacks studied in this paper indicate that KASUMI implemented according to the specifications provides sufficient strength against linear, differential, and higher order differential cryptanalysis, all general attack methods. Thus, we conclude that KASUMI may be applied with confidence to applications beyond mobile phones, to other areas in which data traffic is restricted.

References

1 Blunden, Escott, "Related key attack on reduced round KASUMI", FSE2001, LNCS2355, pp.289-297, Springer-Verlag, 2001.

2 Jakobsen, Knudsen, "The interpolation attack on block cipher", 4th Fast Software Encryption LNCS1267, pp.28-40, Springer-Verlag, 1997.

3 KASUMI, http://www.etsi.org/dvbandca/3gpp/3gppspecs.htm

4 Knudsen, "Truncated and higher order differentials", 2nd Fast Software Encryption LNCS1008, pp.196-211, Springer-Verlag, 1995.

5 Kuhn, "Cryptanalysis of reduced round MISTY", Eurocrypt2001, LNCS2045, pp.325-339, Springer-Verlag, 2001.

6 Lai "Higher order derivatives and differential cryptanalysis", Communications and Cryptology, pp.227-233, Kluwer Academic Publishers, 1994.

7 Matsui, "New structure of block ciphers with provable security against differential and linear cryptanalysis", 3rd Fast Software Encryption LNCS1039, pp.205-218, Springer-Verlag, 1996.

8 Shimoyama, Moriai, and Kaneko, "Improving the higher order differential attack and cryptanalysis of the KN cipher", 1997 Information Security Workshop LNCS 1396, pp.32-42, Springer-Verlag, 1997.

9 Tanaka, Ishii, and Kaneko, "On the strength of KASUMI without FL functions against higher order differential attack", ICISC2000, LNCS.2015, pp.14-21, Springer-Verlag, 2000.

***TANAKA Hidema**, Ph.D.*

Researcher, Security Fundamentals Group, Information and Network System Department

Cryptology, Information security

***KANEKO Toshinobu**, Ph.D.*

Professor, Tokyo university of science

Cryptology, Information security

SUGIO Nobuyuki

Tokyo university of science

Cryptology, Information security