3-4 An Expansion Algorithm for Higher Order Differential Cryptanalysis of Secret Key Ciphers

TANAKA Hidema and KANEKO Toshinobu

We show an expansion algorithm for a higher order differential cryptanalysis which is one of chosen plaintext attack against symmetric block ciphers. Ordinary algorithm of higher order differential cryptanalysis derives an attack equation for sub-keys in the last round. Our algorithm derives an attack equation for sub-keys in previous round using brute force search to the sub-keys in last round. As the result, comparing with original algorithm, our algorithm can attack one more round. Though a five round modified MISTY1 which is a 64 bit block cipher can be attacked is well known, when our algorithm is used, a six round modified MISTY1 can be broken.

Keywords
Chosen plaintext attack, Block cipher, Higher order differential cryptanalysis, Two round elimination attack

1 Introduction

Cryptographic techniques are the essential components of information security systems. Security in cryptographic techniques is thus directly linked to security throughout the information security system. It is important to have a precise awareness of the security characteristics of any cryptographic technique. Cryptographic techniques are classified either as public-key ciphers or symmetric ciphers, depending on the type of keys involved. While public-key ciphers resolve security problems through the application of complex mathematical processes, symmetric ciphers evaluate security in each function they use and then combine these functions. Symmetric ciphers have also been subject to a remarkable evolution of attack methods. For example, attack methods tailored to characteristics of the target ciphers have been encountered, and these methods have now been applied to newly targeted ciphers. As a result, studying attack methods against symmetric ciphers is critical in any assessment of security.

In contemporary cryptographic techniques, the secret key is never obtained from the ciphertexts even if the cryptographic algorithm is disclosed. Thus, attacks against symmetric ciphers are based on a determination of the values of the keys used, provided that the attacker has obtained several sets of plaintexts and corresponding ciphertexts. This technique is referred to as a known plaintext attack. An even more successful attack method is referred to as a chosen plaintext attack, for which the plaintexts are selected to suit the attack. Linear cryptanalysis is a typical known plaintext attack, and differential cryptanalysis is a typical chosen plaintext attack. Generally, ciphers are required to be secure against chosen plaintext attacks. As described above, a symmetric cipher is a combination of several functions. Thus, security against attacks is

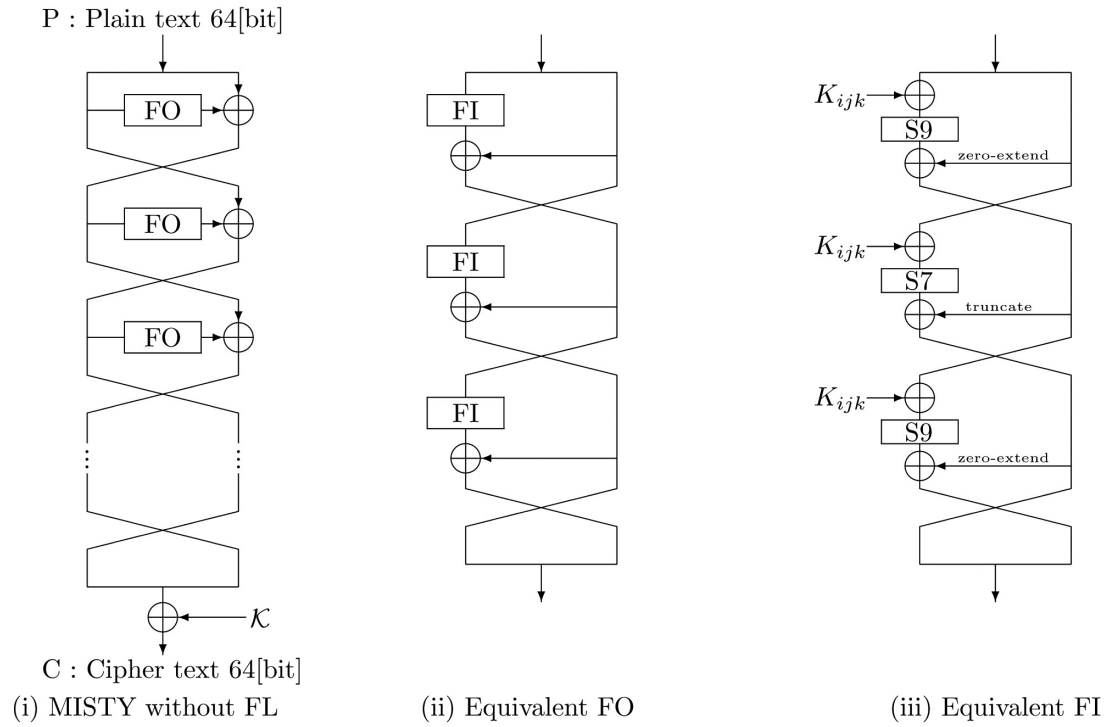
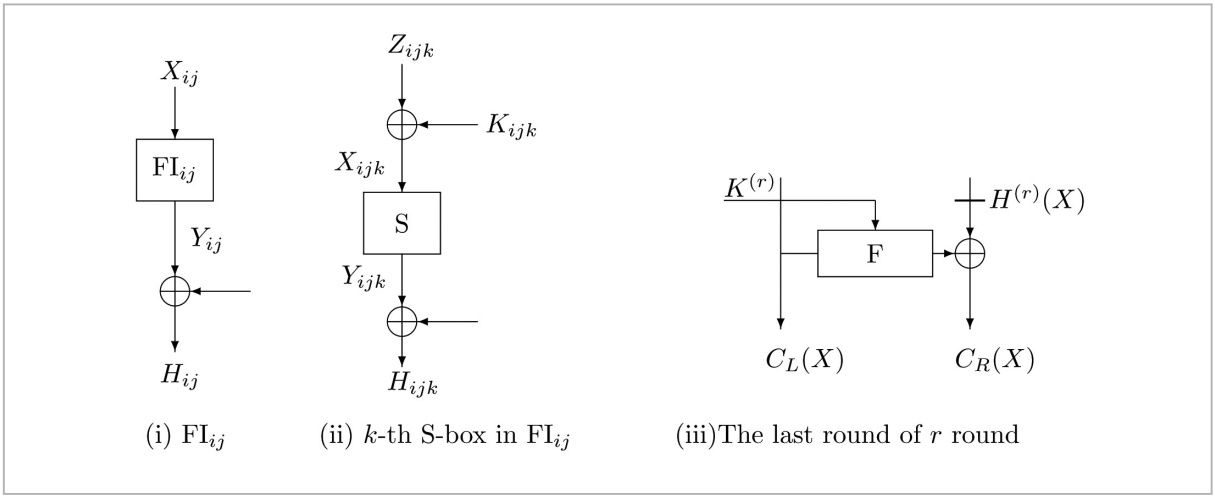


Fig.1 *Modified KASUMI*

evaluated for modified versions of the cipher (e.g., with a reduced number of functions or a reduced number of repetitions of functions); the difference between the limit of the possible attack and the security specification is then regarded as the security margin. As this margin decreases with the expansion in computing power among attackers, assessment of security conditions is becoming even more critical.

This paper discusses an expansion algorithm for higher order differential cryptanalysis [3] for a block cipher, which is a type of symmetric cipher. A block cipher has a repeating structure comprised of basic functions known as F functions. Each repetition is referred to as a "round". When the most effective attack against a block cipher constructed of a rounds can penetrate to the c-th round ($c < a$), rounds a to c are regarded as the security margin. The attacker does not necessarily require the secret key that the user directly specifies, but the attacker may use some portion of the sub-keys used in each round. This is because partial sub-keys may be used to find the remaining unknowns with less effort than that spent in finding the partial sub-keys themselves. The efficiency of the attack is judged based on the number of plaintext/ciphertext pairs and the required computational cost. The number of plaintext/ciphertext pairs is required to be less than 2^n for an n-bit block cipher. The computational cost is required to be less than 2^t F-function calculations for a t-bit secret key.

With the expansion method developed as described in this paper for higher order differential cryptanalysis, which is a type of chosen plaintext attack, one can attack more rounds than with conventional methods. The attack algorithm is applied to modified MISTY1 [6] (Fig.1), a 64-bit block cipher, and the effectiveness of the attack is confirmed. MISTY1 uses 64-bit plaintext input and ciphertext output and has a 128-bit secret key. The cipher function is constructed with F functions specifically referred to as FO functions and auxiliary functions called FL functions in an eight-round repeated structure. Modified MISTY1 consists only of FO functions and



(i) FI_{ij} (ii) k-th S-box in FI_{ij} (iii)The last round of r round

Fig.2 FL function

has a reduced number of rounds (Fig.1). This modification is based on appropriate assumptions, as the security of MISTY1 mostly depends on the FO functions within the structure. Further, proponents of this modification claim that a three-round structure ensures provable security against differential and linear cryptanalysis. Conventional security evaluations have shown that modified MISTY1 can be attacked for up to five rounds. The expanded algorithm for higher order differential cryptanalysis discussed in this paper can achieve up to six-round modified MISTY1. Section 2 discusses the higher order differential cryptanalysis algorithm and the two-round elimination attack that expands on this algorithm. Section 3 explains the structure of modified MISTY1. Section 4 shows examples of particular attacks against modified MISTY1. Finally, Section 5 provides a summary of the paper.

2 Higher order differential cryptanalysis

2.1 Higher order differentials [5]

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

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

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 the following:

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

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

Property 1

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

Property 2

When $F(X)$ is a function of $GF(2)^{ns} \rightarrow GF(2)^n$ and $V[a_0, a_1, ..., a_{N-1}] = GF(2)^n$ holds, $\Delta^{(n)}F(X ; K) = \Delta^{(n)}F(X + f ; K)$ holds for a constant, f.

2.2 Attack equation

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

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

Here, $\tilde{F}(\cdot)$ is a function of $GF(2)^n \times GF(2)^{s\times(r-2)} \rightarrow GF(2)^n$, and $K^{(1, 2, ..., (r-2))}$ 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, through estimation of key $K^{(r)}$ for the last round:

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

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

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

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

$$\sum_{A\in V[a0,a1,\ldots,ad-1]}\{F(C_L(X+A);K^{(r)})+C_R(X+A)\} = \text{const} \tag{7}$$

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

2.3 Attack algorithm

2.3.1 Single-round elimination attack (algebraic method)

Algebraic method[9] is an algorithm proposed by Shimoyama, Moriai, and Kaneko for an efficient solution to the attack equation. This cryptanalysis transforms an attack equation into a set of linear equations, which drastically reduces the computational cost. This linearization sometimes increases the number of chosen plaintext/ciphertext pairs significantly relative to a solution to the attack equation through a brute force search. Nevertheless, the computational cost decreases to a negligible amount.

The attack equation (7) can be rewritten as follows:

$$\begin{aligned}&\sum_{A\in V_{[a0,a1,\ldots,ad-1]}}\{F(C_L(X+A);K^{(r)})+C_R(X+A)\}\\ &=\sum_{A\in V_{[a0,a1,\ldots,ad-1]}}\{F(C_L(X+A);K^{(r)})\}+\sum_{A\in V_{[a0,a1,\ldots,ad-1]}}C_R(X+A)\\ &=\text{const}\end{aligned} \tag{8}$$

The first term is analyzed as follows:

$$\sum_{A\in V[a0,a1,\ldots,ad-1]}F(C_L(X+A);K^{(r)}) = \sum_{A\in V[a0,a1,\ldots,ad-1]\setminus\{0\}}\{F(C_L(X+A);K^{(r)})+F(C_L(X);K^{(r)})\} \tag{9}$$

Here $V[a0, a1, \ldots, ad-1]\setminus\{0\}$ is the subspace spanned by the vectors $a_0, a_1, \ldots, a_{d-1}$ with the all-zero vector removed. As a result, the following new attack equation is obtained:

$$\sum_{A\in V[a0,a1,\ldots,ad-1]\setminus\{0\}}\{\Delta^{(1)}_{CR(X+A)+CR(X)}F(C_L(X+A);K^{(r)})\}+\sum_{A\in V[a0,a1,\ldots,ad-1]}C_R(X+A)=\text{const} \tag{10}$$

When the entire order of $F(\cdot)$ is D(≥ 1), this equation should be a $(D-1)$-th order equation with respect to $K^{(r)}$. As $F(\cdot)\in GF(2)^n$, this equation can be regarded as a set of n equations in $GF(2)$. $K^{(r)}\in GF(2)^s$ serves as the coefficient of X only for terms not greater than the $(D-1)$-th order of X. Thus, s unknowns are considered to be present.

Algebraic method treats Equation (10) as a set of n linear simultaneous equations with respect to $K^{(r)}$. As the order of Equation (10) with respect to $K^{(r)}$ may be regarded as $D-1$ (the order- D term being a constant with respect to X), it appears that L new unknowns are present, where $L = \sum_{i=1}^{D-1} {}_sC_i$. As already discussed, a set of N-th differentials produces n linear equations. Now, as at least L equations are required to solve Equation (10), the number of N-th differentials required is $M=\left\lfloor\frac{L}{n}\right\rfloor$, which means that the number of chosen plaintexts required is $M\times 2^N$.

Eventually, the following equation is obtained:

$$\begin{bmatrix} & A & \end{bmatrix}\begin{bmatrix} k_0\\ k_1\\ \vdots\\ k_{s-1}\\ k_0k_1\\ \vdots\\ k_{s-2}k_{s-1}\\ \vdots\\ k_0k_1k_2\ldots k_{s-1}\end{bmatrix}=\begin{bmatrix} b_0\\ b_1\\ \vdots\\ b_{L-1}\end{bmatrix} \tag{11}$$

Here, A is the $M'\times L(M' = M\times 2_N)$ coefficient matrix and $K^{(r)} = (k_0, k_1, \ldots, k_{s-1})$. Let $a_{ij}\in GF(2)$ be an element of A. The elements a_{ij} and b_i can be calculated as follows:

$$\tilde{F}_j = \sum_{A\in V[a0,a1,\ldots,aN-1]}F(C_L(X+A;e_j) \tag{12}$$

Here, e_j is calculated as follows:

$$e_j = \begin{cases} \bar{e}_{i1}, (0 \le j \le s-1) \\ \bar{e}_{i1} + \bar{e}_{i2}, (s \le j \le {}_sC_2 - 1) \\ \vdots \\ (0,0,0,...,0) \in GF(2)^{N/2}, (j = L) \end{cases} \quad (13)$$

And here, $\bar{e}_i = (0, 0, 0, \ldots \underset{i-th}{1}, \cdots 0)$. $B = {}^t(b_0, b_1, ..., b_{L-1})$ can be calculated as follows:

$$B = \tilde{F}_L + \sum_{A \in V[a0,a1,...,aN-1]} C_R(X + A) + \text{const} \quad (14)$$

Assuming $A_j = {}^t(a_{0,j}, a_{1,j}, ..., a_{M',j-1})$, $(0 \le j \le L)$, this can be calculated as follows:

$$A_j = \begin{cases} \tilde{F}_j + \tilde{F}_M, (0 \le j \le s-1) \\ \tilde{F}_j + \tilde{F}_{i1} + \tilde{F}_{i2} + \tilde{F}_M, (s \le j \le {}_sC_2 - 1) \\ \vdots \\ \tilde{F}_j + \tilde{F}_{i1} + \tilde{F}_{i2} + \cdots + \tilde{F}_M \end{cases} \quad (15)$$

All elements can be calculated repeating this calculation procedure.

The computational cost required to calculate the elements of matrices A and B is $M \times 2^N \times L$ F-function calculations. After these values are determined, one can obtain the inverse matrices with, for example, the Gauss-Jordan method, and thus determine the unknowns. The computational cost required for this procedure is negligibly small compared to the computational cost required to calculate the elements of matrices A and B. Thus, the computational cost required for the total process can be considered as $M \times 2^N \times L$ F-function calculations.

2.3.2 Two-round elimination attack

This section discusses the two-round elimination attack, which solves the last two rounds together using a brute force search. Simply stated, the algorithm uses a brute force search to derive an attack equation for the sub-keys in the last round and uses algebraic method for the last two rounds. If $K^{(r)}$ is correctly estimated, $K^{(r-1)}$ can be obtained and the attack equation remains possible. However, if $K^{(r)}$ is incorrectly estimated, the attack equation becomes impossible and cannot be solved. In this way, the attacker can deduce whether he or she has derived the correct sub-keys. Let us expand the attack equation as follows:

$$[A'][K^{(r-1)}] = [B] \quad (16)$$

Here A' is an $(L+m) \times L$ coefficient matrix.

Let us consider solving the attack equation while estimating the sub-key $K^{(r)}$ of the last round at the same time. If rank(A') = L, the unknown $K^{(r-1)}$ can be determined solving this equation. Taking A'_i, $(0 \le i \le L-1)$, a column vector of A', the attack equation can be rewritten as follows:

$$A'_0 k_0 + A'_1 k_1 + A'_2 k_2 + \cdots + A'_{L-1} k_{L-1} = B \quad (17)$$

If this equation holds, B is an element of the subspace spanned by $A'_0, A'_1, ..., A'_{L-1}$. If it does not hold, these can be regarded as randomly selected vectors. Let us consider the probability P that this equation holds. There are 2^{L+m} types of elements in the subspace spanned by vectors $A'_0, A'_1, ..., A'_{L-1}$. On the other hand, there are 2^L types of elements for B. Thus, P can be calculated as follows:

$$P = \frac{2^L}{2^{L+m}} = 2^{-m} \quad (18)$$

To remove false sub-keys, a set of linear equations is required with which $2^s 2^{-m} \ll 1$ holds.

This requirement means that there are 2^m candidates for the keys. As only the correct keys satisfy all of the equations, the false values are removed by performing 2^m extra calculation iterations. As already discussed, only n equations can be derived from a set of N-th differentials. Thus, M' sets of N-th differentials are required, where $M' = \left\lfloor \frac{L+m}{n} \right\rfloor$.

To decrypt $M' \times 2^N$ ciphertexts by one round, $M' \times 2^N$ F-function calculations are required. After having derived the attack equation, L F-function calculations are performed to determine the coefficient matrix. Thus, the computational cost required to solve two rounds of sub-keys while estimating the sub-keys for the last round at the same time corresponds to $M' \times 2^N \times L$ F-function calculations. In addition, excess calculations are also required to remove the 2^s candidates, so that $M' \times 2^{N+s} \times L$ F-function calculations are thus required.

Consequently, the two-round elimination attack requires $M' \times 2^{N+s} \times L$ F-function calculations and $M' \times 2^{N}$ chosen plaintexts.

3 Modified MISTY1

The strength of resistance to linear and differential cryptanalysis, both general and powerful attacks against block ciphers, depends on the maximum value of the linear or differential probabilities of the component functions. Let us denote the average of these probabilities as p. According to the theory presented by Nyberg and Knudsen[8], the maximum linear or differential probability is p^2 for a three-round Feistel structure. If p^2 is sufficiently small, this property is referred to as provable security for linear or differential cryptanalysis.

Proponents of MISTY1 have shown that MISTY1 offers provable security with $p < 2^{-56}$ if the FO functions are comprised of a three-round Feistel structure[6]. Although these proponents argue that the FO function alone ensures sufficient security, external functions referred to as FL functions are added to increase security even further.

MISTY1 has a nested structure with each FO function consisting of three rounds of FI functions. Each FI function is composed of S-boxes known as S7 and S9. An S-box is a substitution provided by a table. S7 is seven bits and S9 is nine bits, so that the FI function has an asymmetric structure. The order of S7 is 3 and the order of S9 is 2.

The basic specifications of MISTY1 set a structure with eight rounds of a repeating combination of FO and FL functions. This method uses 64-bit plaintext/ciphertext blocks and 128-bit secret keys. Thus, MISTY1 is judged as insecure if it can be attacked using less than 2^{64} pairs of plaintext/ciphertext pairs with less than 2^{128} calculations.

This paper focuses on the FO functions, which provide the essential security of MISTY1, and also examines security in the Feistel structure, the basic structure for block ciphers; however, this paper does not discuss the FL functions. Here, MISTY1 with the FL function removed is referred to as modified MISTY1. The security of modified MISTY1 against higher order differential cryptanalysis is evaluated using the two-round elimination attack. In the past, it has been shown that five-round modified MISTY1 can be attacked with higher order differential cryptanalysis. This paper examines the possibility of attacks for modified MISTY1 at higher rounds than previously examined. Fig.2 shows the positions and names of the variables used in the discussion below.

4 Example of attacks on modified MISTY1

4.1 Effectively selected chosen plaintexts

The order of higher order differential cryptanalysis depends on the choice of the plaintexts. As the order influences the number of chosen plaintext pairs and the computational cost, it is important to seek effective chosen plaintexts that enable an attack at a minimum order. The structure of MISTY1 enables division of the plaintexts into eight sub-blocks, as shown below.

$$P = (X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0)$$
$$X_i \in \begin{cases} GF(2)^7, i = even \\ GF(2)^9, i = odd \end{cases} \quad (19)$$

In this study the effective chosen plaintexts were searched in sub-block manner. Thus, output order depends on which sub-block is selected as the variable. We performed our search where the increase in order was the slowest, and found the most effective approach with the rightmost X_0 selected as the variable and the remaining sub-blocks fixed as constants. Fig.3 shows a formal estimation of the increase in order. The notation $<i|j>$ shows that the order of the sub-block on the left is i, and that the order of the sub-block on the right is j.

4.2 Attacks using the seventh differentials

The chosen plaintexts selected in the pre-

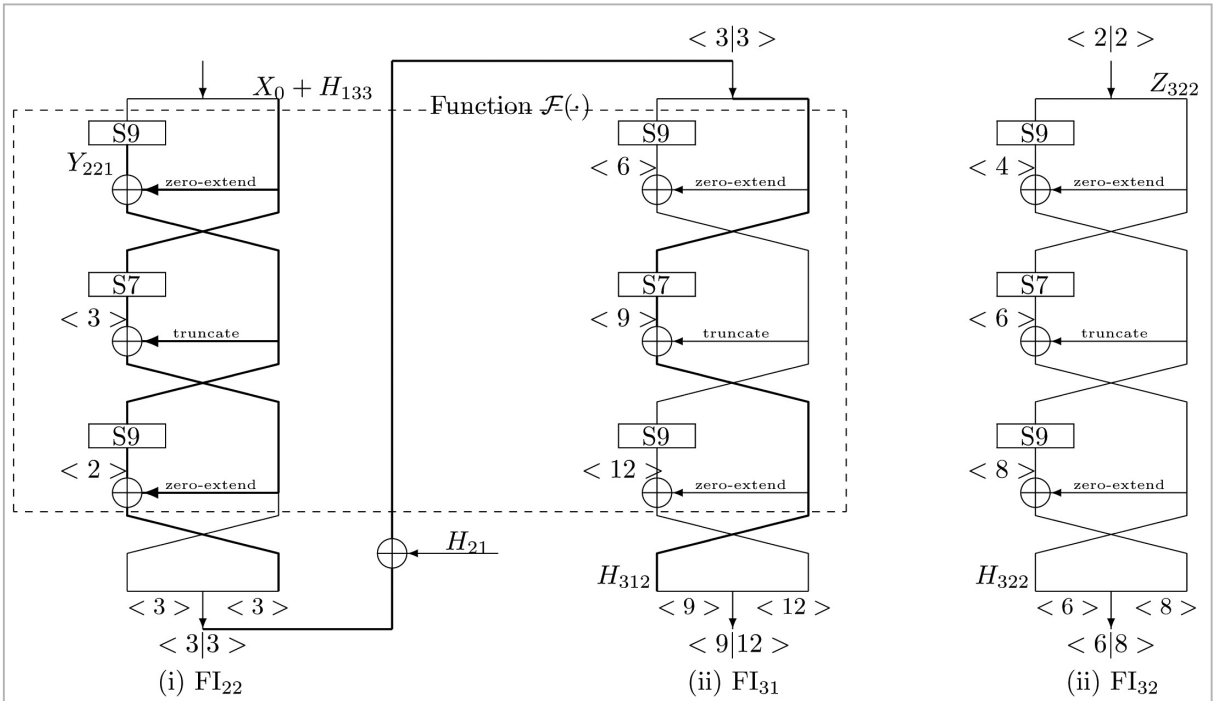


Fig.3 *r-round Feistel*

vious section form a seven-bit variable; this section therefore discusses attacks using seventh differentials. Let us utilize the subspace $V^{(7)}$ as follows:

$$V^{(7)}=V_{[a0,a1,\ldots,a6]} \quad ai=(0,0,\ldots,1,\ldots,0)\in GF(2)^{64} \quad (20)$$
$$\uparrow i\text{-th}$$

$H_{32}{}^{L7}$ expresses the left most seven bits of output from the FO_3 function.

$$H_{32}{}^{L7}=H_{312}+H_{322}+Z_{322} \quad (21)$$

Due to Property 1, the following equation holds:

$$\Delta^{(7)}H_{32}{}^{L7}=\Delta^{(7)}(H_{312}+H_{322}+Z_{322})]_7 = \Delta^{(7)}H_{312}]_7 \quad (22)$$

Here, the notation $]_d$ indicates an operation that ignores terms of orders less than d. As shown in Fig.3, let $F(\cdot)$ be a function of $GF(2)^7\times GF(2)^9\rightarrow GF(2)^7$.

$$H_{312}=F(X_0+H_{133}+K_{222};Y_{221}) \quad (23)$$

It should be noted that Y_{221} is a fixed constant in the chosen plaintexts. As X_0 spans a subspace of $GF(2)^7$, the following equation holds, due to Property 2:

$$\Delta^{(7)}H_{312}=\Delta^{(7)}F(X_0+H_{133}+K_{222};Y_{221}) = \Delta^{(7)}F(X_0;Y_{221}) \quad (24)$$

Thus, the following seventh differential is obtained.

$$\Delta^{(7)}H_{32}^{L7}=\Delta^{(7)}F(X_0;Y_{221})]_7 \quad (25)$$

Calculating the Boolean algebraic equation of H_{312} clarifies the following:

1) The order of H_{312} is 7.
2) The value of the seventh differential for $H_{32}{}^{L7}$ is *0x6D*.
3) The coefficient of the sixth-order term is a polynomial with respect to Y_{221}.

Table 1 shows part of the calculation results.

$$X_{222}=(x_6,\ldots,x_0), \quad (X_{222}=X_0+H_{133}+K_{222})$$
$$Y_{221}=(y_8,\ldots,y_0), \quad H_{312}=(\grave{h}_6,\ldots,\grave{h}_0) \quad (26)$$

With $\Delta^{(7)}H_{32}{}^{L7}=0x6D$, the following attack equation is derived:

$$\sum_{\substack{A\in V^{(7)}\\ K=(K_L,K_R)}}\{FO(C_L(P+A)+K_L;K_{522},K_{521},K_{512},K_{511})+C_R(P+A)+K_R\}=0x6D \quad (27)$$

The equivalent key K added at the end can be moved as shown in Fig.4. In the FO_5 func-

Table 1

$\hat{h}_0$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_3 + y_5 + y_6 + y_8)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_1$	$(y_0 + y_2 + y_4 + y_7)x_0x_1x_2x_3x_4x_5 + \cdots + y_5y_7 + y_5y_8 + y_6y_8 + y_6$
$\hat{h}_2$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_2 + y_4 + y_5 + y_7 + y_8 + 1)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_3$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_3 + y_4 + y_6 + y_8)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_4$	$(y_0 + y_2 + y_3 + y_6 + y_7)x_0x_1x_2x_3x_4x_5 + \cdots + y_6y_7y_8 + y_7 + y_8 + 1$
$\hat{h}_5$	$x_0x_1x_2x_3x_4x_5x_6 + (y_1 + y_6 + y_8 + 1)x_0x_1x_2x_3x_4x_5 + \cdots + y_8$
$\hat{h}_6$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0 + y_2 + y_5 + y_7 + 1)x_0x_1x_2x_3x_4x_5 + \cdots + y_6 + y_7$

tion, K_L can be further divided into K_{LI} and K_{Lr}.

Figure 4: Last round of a five-round modified MISTY1

$$K_{511}=K_{511}+K_{LI}^{L9}$$
$$K_{512}=K_{512}+K_{LI}^{R7} \quad (28)$$

Further, these values can be expressed as follows in FI_{51}.

$$K_{521}=K_{521}+K_{LI}^{L9}$$
$$K_{522}=K_{522}+K_{LI}^{R7} \quad (29)$$

Thus, the attack equation can be rewritten as follows:

$$\sum_{A\in V^{(7)}}\{FO(C_L(P+A);\ K_{522}\ \ K_{521},\ \ K_{512},\ \ K_{511})+C_R(P+A)\}=0x6D \quad (30)$$

As the attack equation is derived based on seven-bit H_{32}^{L7}, it is a seven-bit equation. Thus, it should be ensured that appropriate values are selected for quantities of seven bits or greater.

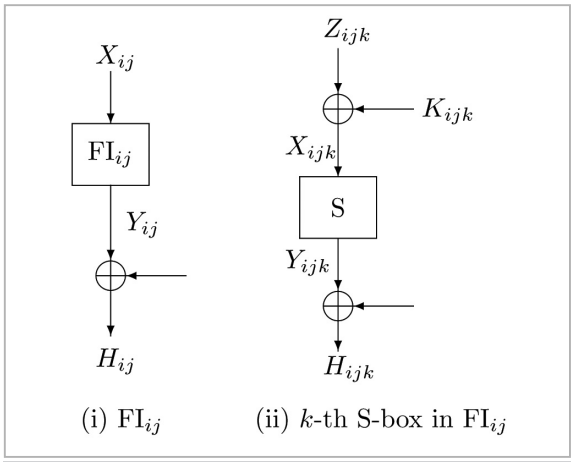


Fig.4 *Last round of a five-round modified MISTY1*

4.3 Number of chosen plaintext pairs and computational cost required

4.3.1 Single-round elimination attack

The attack applies the algebraic method shown in Section 2.3. We calculated the number

of independent types of unknowns generated from terms related to K_{511}, K_{512}, K_{521}, and K_{522}. The attack equation consists of two nine-bit variables, K_{511} and K_{521}, and two seven-bit variables, K_{512} and K_{522}. The order of the nine-bit variables is 1 and the order of the seven-bit variables is 2. Thus, the total number of unknowns is $L = 2\times(9+7+{}_7C_2)=74$. As a set of seventh differentials derives seven linear equations, the number of seventh differentials required is $\left\lfloor\frac{74}{77}\right\rfloor+1=11$. Consequently, the number of chosen plaintexts required is

$$M\times 2^N=11\times 2^7=1{,}408 \quad (31)$$

and the number of F-function calculations required is

$$M\times 2^N\times L=11\times 2^7\times 74\fallingdotseq 2^{17} \quad (32)$$

These results show that the attacker can attack five-round modified MISTY1 more efficiently than performing a brute force search for the keys.

4.3.2 Two-round elimination attack

This section shows the application of the two-round elimination attack shown in Section

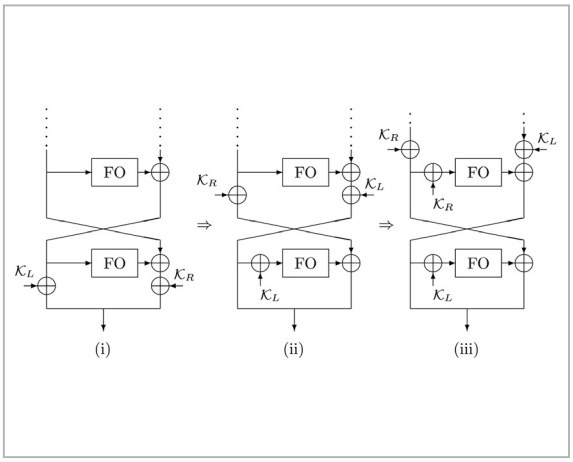


Fig.5 *Sub-keys in Round 5*

3.2. As the FO functions have 75-bit keys, $s=75$. Thus, $m=91$ is set.

$$2^s \times 2^{-m} = 2^{75} \times 2^{-91} \ll 1 \tag{33}$$

Thus, the number of seventh differential pairs required is $M' = \left\lfloor \frac{74+91}{7} \right\rfloor \approx 24$. Consequently, the number of chosen plaintexts required is

$$M \times 2^N = 24 \times 2^7 \fallingdotseq 2^{12} \tag{34}$$

and the number of F-function calculations required is

$$M \times 2^{N+s} \times L = 11 \times 2^{7+75} \times 74 \fallingdotseq 2^{93} \tag{35}$$

These results show that the attacker can attack six-round modified MISTY1 more efficiently than performing a brute force search for the keys.

5 Summary

This paper proposes a two-round elimination attack that combines algebraic method and brute force search as an expansion of higher order differential cryptanalysis. The requirements for the chosen plaintexts and the computational cost are shown and the effectiveness of the attack is confirmed with a model attack on modified MISTY1.

The results of this study show that MISTY1 without FL functions can be attacked using seventh differentials. Using a brute force search for the Round-6 sub-keys and algebraic method for the Round-5 sub-keys, 2^{12} chosen plaintexts and 2^{93} F-function calculations are required. Thus, this attack is 2^{30} -fold faster than the brute force search for a 128-bit secret key. In conclusion, we can say at the least that a block cipher with a Feistel structure that uses the FO functions of MISTY1 is not secure against higher order differential cryptanalysis if not constructed with at least seven rounds.

References

1 Babbage, Frisch, "On MISTY1 Higher Order Differential Cryptanalysis", 3rd International Conference on Information Security and Cryptology 2000, LNCS2015, pp.1-13, Springer- Verlag, 2000.

2 Daemen, Govaerts, Rijmen, "The Block Cipher SQUARE", 4th Fast Software Encryption. LNCS1267, pp.149-165, Springer-Verlag, 1997.

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

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

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

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

7 Moriai, Shimoyama, and Kaneko, "Higher order differential attack of CAST cipher", 4th Fast Software Encryption LNCS1372, pp.17-31, Springer-Verlag, 1997.

8 Nyberg, Knudsen “Provable security against differential cryptanalysis”, Journal of Cryptology, Vol.8, No.1, pp.27-37, 1995.
9 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.
10 Tanaka, Hisamatsu, and Kaneko, “Strength of MISTY1 without FL functions for higher order differential attack”, 13th International Symposium, Applied Algebra - Algebraic Algorithm and Error-Correcting Codes 1999 LNCS1719, pp.221-230, Springer-Verlag, 1999.

***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