コンピュータセキュリティ　18−29
(2002. 7. 19)

FL関数の無い6段MISTY1の攻撃について

田中　秀磨†　　金子　敏信††

† 通信総合研究所 情報通信部門 非常時通信グループ 〒184-8795 小金井市貫井北町 4-2-1
†† 東京理科大学 理工学部 電気工学科 〒278-8510 野田市山崎 2641
E-mail: †hidema@crl.go.jp, ††kaneko@ee.noda.sut.ac.jp

あらまし　MISTY1はFO関数3段以上で構成されている時、線形解読法と差分解読法に対して証明可能安全性を持つブロック暗号である。本研究では、FO関数の高階差分解読法に対する強度評価を行い、平文固定値と拡大鍵の値によらず7階差分値が定数となることを発見した。この性質を用いて6段のFO関数構成に対する攻撃の可能性を考察し、その結果2^{12}個の選択平文組と2^{93}回のFO関数計算があれば攻撃可能であると見積もった。
キーワード　ブロック暗号, 証明可能安全性, MISTY1, 高階差分解読法

An Attack of 6-round MISTY1 without FL functions

Hidema TANAKA† and Toshinobu KANEKO††

† Emergency Communications Group, Communications Research Laboratory
4-2-1 Nukui-Kitamachi, Koganei, Tokyo, 184-8795, JAPAN
†† Department of Electrical Engineering, Science University of TOKYO
2641 Yamazaki, Noda, Chiba, 278-8510
E-mail: †hidema@crl.go.jp, ††kaneko@ee.noda.sut.ac.jp

Abstract　The encryption algorithm MISTY1 is provably secure, when it has 3-round FO functions, against linear cryptanalysis and differential cryptanalysis. We estimated the strength of FO function against higher order differential attack. We found that the value of 7th order differential of part of the output from 3-round FO function is constant, for any key or fixed value of plaintexts. The attack of 6 round MISTY1 without FL functions using this fact is demonstrated. It is attackable using 2^{12} chosen plaintexts and 2^{93} times the number of FO function operations.

Key words　Block cipher, Provably secure, MISTY1, Higher order differential attack

1. Introduction

Linear and differential cryptanalysis are powerful means of attack algorithm against Feistel-type block ciphers. The concept of provably secure has been proposed as a counter measure [6], [8]. The encryption algorithm MISTY1, proposed by Matsui in 1996, is a block cipher designed using this concept [6]. It generates a 64-bit ciphertext from a 64-bit plaintext under the control of a 128-bit user key. It is composed of 8-rounds of F functions called FO and linear functions called FL. Matsui showed that a 3-round MISTY1 without FL functions is strong enough to have provable security.

We estimated the strength of FO function in MISTY1 against higher order differential attack [4], [7], [9]. Higher order differential attack is a chosen plaitext attack that uses the fact that the value of the higher order differential in the output, which does not depend on the key or fixed value of the plaintexts. The order of the attack depends on the chosen plaintext, and it affects the number of plaintexts and the computational cost.

We found effective chosen plaintexts for MISTY1 without FL functions. And, we used two-round elimination algorithm. Our attack method required 2^{12} chosen plaintexts and 2^{93} times the number of FO function operations. As the results, we concluded that 6-round MISTY1 without FL function is not strong enough against higher order differential attack.

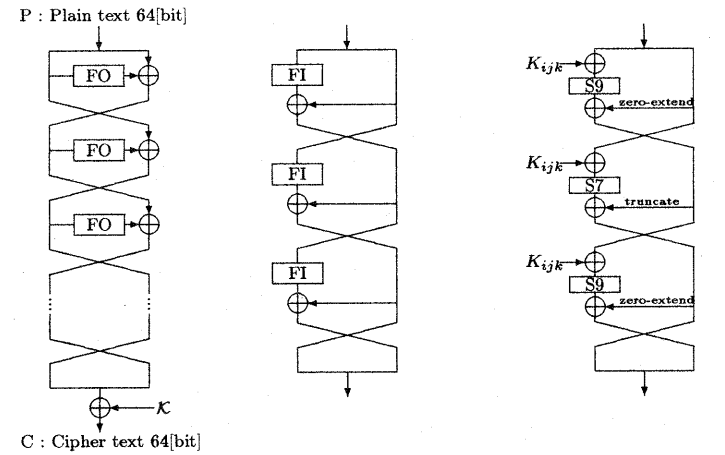


Figure 1 The modified MISTY (where $\mathcal{K}$ and K_{ijk} denote the eqivalent sub-keys)

2. MISTY1 and Modified MISTY1

The success of linear cryptanalysis or differential cryptanalysis depends on its maximum linear or differential probability. Let p be the average probability for F function. From the theorem given by Nyberg and Knudsen [5], the probability for 3-round F function equals p^2. If p^2 is low enough, this property is called "provably secure" against linear or differential cryptanalysis.

Matsui, the designer of MISTY1, showed that the F function called FO has a probability of $p < 2^{-56}$ and that the 3-round FO function is provably secure. Though Matui asserted that the main part of the security is guaranteed by FO function, he added an auxiliary function FL, for higher security. FO function consists of 3 rounds of FI functions. FI function consists of two kinds of S-boxes, S7 and S9. The degree of S7 is 3, and that of S9 is 2.

In this paper, we estimated the strength of FO function against higher order differential attack. Thus, we neglected FL function. And to simplify the attack equation, we deduced the equivalent FO and FI function. We call MISTY1 without FL functions, Modified MISTY1 (Figure 1). We denoted the FO function in the i-th round as FO_i, and the j-th FI function in FO_i as FI_{ij}. We denoted the equivalent sub-keys as $\mathcal{K}$ and $\mathcal{K}_{ijk}$. In the following, we used input and output variables for FI_{ij} and the k-th S-box, as shown in figures 2(i) and (ii).

3. Higher order differential attack

3.1 Higher order differential

Let $F(X;K)$ be a function : $\mathrm{GF}(2)^n \times \mathrm{GF}(2)^s \mapsto \mathrm{GF}(2)^n$:

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

Let $(a_0, a_1, \ldots, a_{N-1})$ be a set of linear independent vectors in $\mathrm{GF}(2)^n$ and let $V_{[a_0,a_1,\ldots,a_{N-1}]}$ be a subspace spanned by the set. We define $\Delta^{(N)}_{(a_0,a_1,\ldots,a_{N-1})}F(X;K)$ as the N-th order differential of $F(X;K)$ with respect to X,

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

In the following, we denote $\Delta^{(N)}_{(a_0,a_1,\ldots,a_{N-1})}$ as $\Delta^{(N)}$ when $V_{[a_0,a_1,\ldots,a_{N-1}]}$ is understood. If $\deg_X\{F(X;K)\} = d$, we have the following properties.

Property1:

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

Property2: Let $F(X) : \mathrm{GF}(2)^n \mapsto \mathrm{GF}(2)^n$. If $V_{[a_0,a_1,\ldots,a_{n-1}]}=\mathrm{GF}(2)^n$, then for any fixed value $f \in \mathrm{GF}(2)^n$, $\Delta^{(n)}F(X+f;K) = \Delta^{(n)}F(X;K)$.

3.2 Attack equation

Figure 2(iii) shows the last round of an r-round Feistel block cipher. $H^{(r)}(X)$, which is the output of F function in $(r-2)$-th round, can be calculated using

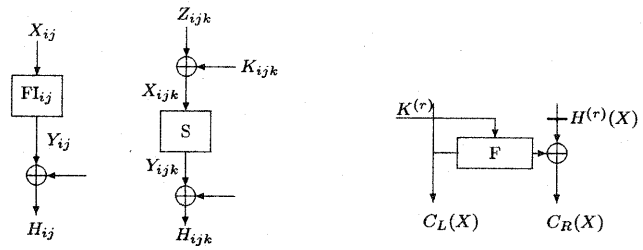
$$H^{(r)}(X) = \tilde{F}(X; K^{(1\cdots(r-2))}), \quad (4)$$

where $\tilde{F}(\cdot)$ denotes the function $\mathrm{GF}(2)^n \times \mathrm{GF}(2)^{s\times(r-2)} \mapsto \mathrm{GF}(2)^n$. $K^{(1\cdots(r-2))}$ denotes the set of keys for the previous $(r-2)$ rounds.

However, $H^{(r)}(X)$ can be calculated from the ciphertext side using $C_L(X)$, $C_R(X) \in \mathrm{GF}(2)^n$, and unknown sub-key $K^{(r)}$:

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

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



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

Figure 2 (i)(ii):The input and output variables for FI_{ij} and k-th S-box, (iii):The last round of r round Feistel Block Cipher

$$\Delta^{(d)}_{(a_0,a_1,\ldots,a_{d-1})}\tilde{F}(X;K^{(1\cdots(r-2))}) = \text{const} \quad (6)$$

From equations (2), (5), and (6), we can derive

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

If we can determine the value of const, we can determine the value of $K^{(r)}$ by solving this equation. So, we call this equation an attack equation.

3.3 Attack algorithm

3.3.1 One round elimination attack (algebraic method)

Algebraic method is proposed by Shimoyama, Moriai, and Kaneko [7], [9]. The method constructs linear equations from some attack equations. Though it needs more plain/ciphertexts than brute-force search, it succeeds in reducing the computational cost greatly.

We can rewrite attack equation (7):

$$\begin{aligned}&\sum_{A\in V[a_0,a_1,\ldots,a_{d-1}]} \{F(C_L(X+A);K^{(r)}) + C_R(X+A)\}\\ &= \sum_{A\in V[a_0,a_1,\ldots,a_{d-1}]} F(C_L(X+A);K^{(r)})\\ &\quad + \sum_{A\in V[a_0,a_1,\ldots,a_{d-1}]} C_R(X+A)\\ &= \text{const.}\end{aligned} \quad (8)$$

The first term of this equation can be analyzed:

$$\begin{aligned}&\sum_{A\in V[a_0,a_1,\ldots,a_{d-1}]} F(C_L(X+A);K^{(r)})\\ &= \sum_{A\in V[a_0,a_1,\ldots,a_{d-1}]\setminus\{0\}} \{F(C_L(X+A);K^{(r)})\\ &\qquad + F(C_L(X);K^{(r)})\},\end{aligned} \quad (9)$$

where $V[a_0,a_1,\ldots,a_{d-1}]\setminus\{0\}$ denotes the subspace spanned by $a_0,a_1,\ldots,a_{d-1}$ except all-zero.

As a result, we obtaine the following attack equation.

$$\begin{aligned}&\sum_{A\in V[a_0,a_1,\ldots,a_{d-1}]\setminus\{0\}} \{\Delta^{(1)}_{C_R(X+A)+C_R(X)} F(C_L(X+A);K^{(r)})\}\\ &\quad + \sum_{A\in V[a_0,a_1,\ldots,a_{d-1}]} C_R(X+A)\\ &= \text{const}\end{aligned} \quad (10)$$

If the total degree of $F(\cdot)$ is $D(\geqq)1$, equation (10) has degree $D-1$ with respect to $K^{(r)}$. Because $F(\cdot)\in \mathrm{GF}(2)^n$, we can regard equation (10) as the system of n equations on $\mathrm{GF}(2)$. We supposed that its degree with respect to unknown $K^{(r)}\in \mathrm{GF}(2)^s$ is $D-1$, and it has s unknown variables.

Algebraic method transforms equation (10) to the system of n linear equations by regarding all the variable terms with respect to an unknown $K^{(r)}$. Because the degree of equation (10) with respect to $K^{(r)}$ is $D-1$, $L=\sum_{i=1}^{D-1} {}_sC_i$ new unknowns emerged. As mentioned before, we can derive n vector equations from one attack equation using N-th order differential. Because we need L equations at least to determine unknowns, we need $M=\lfloor \frac{L}{n} \rfloor$ different attack equations. Thus, we need $M\times 2^N$ chosen plaintexts.

As a result, we obtaine the following.

$$\begin{bmatrix} & \mathcal{A} & \end{bmatrix} \begin{bmatrix} k_0 \\ \vdots \\ k_{s-1} \\ k_0k_1 \\ \vdots \\ k_{s-2}k_{s-1} \\ \vdots \\ k_0k_1\cdots k_{s-1} \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{L-1} \end{bmatrix}, \quad (11)$$

where $\mathcal{A}$ is the coefficient matrix $M'\times L, (M'=M\times 2^N)$, and $K^{(r)}=(k_0,k_1,\ldots,k_{s-1})$.

Let $a_{ij}\in \mathrm{GF}(2)$ be the element of matrix $\mathcal{A}$. All coefficients a_{ij} and b_i can be calculated using

$$\tilde{F}_j = \sum_{A\in V[a_0,a_1,\ldots,a_{N-1}]} F(C_L(X+A;e_j)) \quad (12)$$

where $e_j (0\leqq j\leqq L)$ is

$$e_j = \begin{cases} \bar{e}_{i_1} & ,(0 \leqq j \leqq s-1) \\ \bar{e}_{i_1} + \bar{e}_{i_2} & ,(s \leqq j \leqq {}_sC_2 - 1) \\ \vdots & \\ (0,0,\ldots,0) \in \mathrm{GF}(2)^{(\frac{N}{2})} & ,(j = L) \end{cases} \quad (13)$$

where $\bar{e}_i$ is an initial vector as $(0,0,\ldots,\underset{\uparrow i\text{-th}}{1},\ldots,0) \in \mathrm{GF}(2)^{\frac{N}{2}}$.

Let $\mathcal{B} = {}^t(b_0, b_1, \ldots, b_{L-1})$is calculated

$$\mathcal{B} = \tilde{F}_L + \sum_{A \in V_{[a_0,a_1,\ldots,a_{N-1}]}} C_R(X+A) + \text{const.} \quad (14)$$

Let $\mathcal{A}_j = {}^t(a_{0,j}, a_{1,j}, \ldots, a_{M',j-1}), (0 \leqq j \leqq L)$.

$$\mathcal{A}_j = \begin{cases} \bar{F}_j + \bar{F}_M & \\ & ,(0 \leqq j \leqq s-1) \\ \bar{F}_j + \bar{F}_{i1} + \bar{F}_{i2} + \bar{F}_M & \\ & ,(s \leqq j \leqq {}_sC_2 - 1) \\ \vdots & \\ \bar{F}_j + \bar{F}_{i1} + \bar{F}_{i2} + \cdots + \bar{F}_M. & \end{cases} \quad (15)$$

From this procedure, we can determine n rows. The remaining coefficients can be calculated in the same way (repeat $M-1$ times).

To determine matrix $\mathcal{A}$ and $\mathcal{B}$, we have to calculate $M \times 2^N \times L$ times of F function operation. After determined them, we can solve the equation using Gauss-Jordan's elimination method. The required cost for this computation will be negligible by comparing it with the earlier cost. Thus, the computational cost for algebraic method is estimated as $M \times 2^N \times L$ times the number of F function operation.

3.3.2 Two round elimination attack

In this section, we show two round elimination attack using brute-force search and algebraic method. We decrypt ciphertexts for one previous round using an estimated last round sub-key $K^{(r)}$. By using these decrypted ciphertexts, we derive the attack equation. If the last round sub-key that we estimated is true, we can determine true $K^{(r-1)}$ by solving the attack equation. But if it is false, the attack equation will hold with the probability. And the equation, which is derived using another pair of plain/ciphertexts under the same false sub-key, does not always hold. We use the following equation

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

where $\mathcal{A}'$ is a coefficient matrix $(L+m) \times L$, and $\mathcal{K}^{(r-1)} = {}^t(k_0, k_1, \ldots, k_{L-1})$ is an unknown matrix with respect to an unknown sub-key $K^{(r-1)}$,

Let that equation be an attack equation derived using an estimated last round sub-key $K^{(r)}$. If $\mathrm{rank}(\mathcal{A}') = L$, the unknown $K^{(r-1)}$ can be determined using algebraic method. Let $\mathcal{A}'_i, (0 \leqq i \leqq L-1)$ be a column vector of a matrix $\mathcal{A}'$. Then the equation (16) can be rewritten as

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

When this equation holds, vector $\mathcal{B}$ is an element of subspace spanned by vectors $\mathcal{A}'_0, \mathcal{A}'_1, \ldots, \mathcal{A}'_{L-1}$. We can regard $\mathcal{A}'_0, \mathcal{A}'_1, \ldots, \mathcal{A}'_{L-1}$ and $\mathcal{B}$ as random vectors for a false last round sub-key $K^{(r)}$. Let P be the probability that holds the equation (17) for a false sub-key. The number of elements of subspace spanned by vectors $\mathcal{A}'_0, \mathcal{A}'_1, \ldots, \mathcal{A}'_{L-1}$ equals to 2^{L+m}. And the number of elements of $\mathcal{B}$ equals to 2^L. Thus the probability P is calculated as follows.

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

To exclude false sub-key, we need $L+m$ linear equations which holds $2^s 2^{-m} \ll 1$. As mentioned above, we can derive n linear equations from one N-th order differential. Thus we need $M' = \lfloor \frac{L+m}{n} \rfloor$ different N-th order differentials.

To decrypt $M' \times 2^N$ ciphertexts for one previous round using an estimated last round sub-key, we need $M' \times 2^N$ times the number of F function operation. After deriving attack equation, we need L times the number of F function operation to calculate coefficient matrix. Thus, to solve attack equation estimating a last round sub-key $K^{(r)}$, necessary computational cost is estimated as $M' \times 2^L \times L$ times the number of F function operation. Since there are 2^s candidates of the last round sub-key, the total computational cost is estimated as $M' \times 2^{N+s} \times L$ times the number of F function operation.

As the result, two round elimination attack using brute-force search and algebraic method, requires $M' \times 2^N$ chosen plaintexts and $M' \times 2^{N+s} \times L$ computational cost.

4. Attack of Modified MISTY1

4.1 Effective chosen plaintext

The order for higher order differential attack depends on the chosen plaintext. Since the order affects the number of chosen plaintexts and the computational cost, searching for the effective chosen plaintext is important. The plain text can be divided into 8 sub-blocks according to the S-boxes where inputted to be done.

$$P = (X_7, X_6, \ldots, X_1, X_0), \quad X_i \in \begin{cases} \mathrm{GF}(2)^7, & i = \text{even} \\ \mathrm{GF}(2)^9, & i = \text{odd}. \end{cases} \quad (19)$$

The degree of output depends on which sub-block we chose as a variable. We searched for the effective choice, which makes the slowest increase in degree. As a result, the effective one is keeping all the sub-blocks fixed except the right most sub-block $X_0 \in \mathrm{GF}(2)^7$. The increase in degree by the formal analysis is shown in Figure 3 for this chosen plain

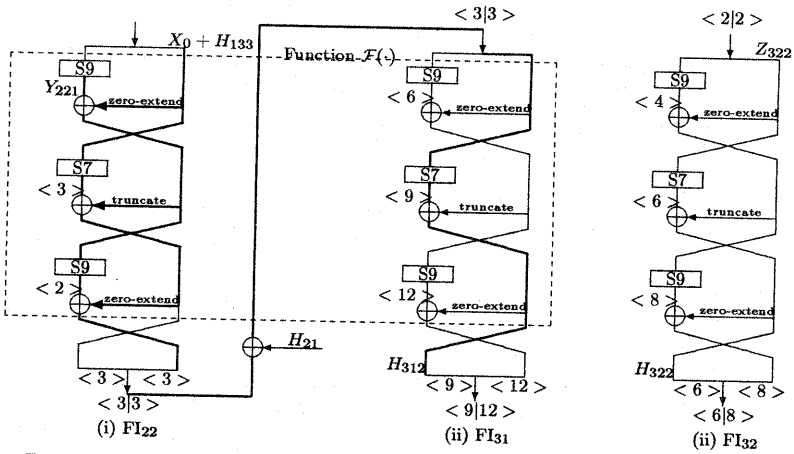


Figure 3 The increase of degree by the formal analysis (To simplify the expression, we omit sub-keys in these figures.)

text. The symbol $< i|j >$ denotes that the degree of the left block is i and the right block is j.

4.2 Attack equation using 7th order differential

We have 7[bit] variable for the chosen plain text P. Let's discuss the attack using 7th order differential. We use a subspace $V^{(7)}$ as

$$V^{(7)} = V_{[a_0,a_1,\ldots,a_6]}, \quad a_i = (0,0,\ldots,\underset{\uparrow i\text{-th bit}}{1},\ldots,0)) \in \mathrm{GF}(2)^{64}. \tag{20}$$

In the following, we denote $\Delta^{(7)}_{[a_0,a_1,\ldots,a_6]}$ as $\Delta^{(7)}$ when $V^{(7)}$ is understood.

Let H^{L7}_{32} be the left 7[bit] of the output from FO_3:

$$H^{L7}_{32} = H_{312} + H_{322} + Z_{322}. \tag{21}$$

From Property 1, the following holds.

$$\begin{aligned}\Delta^{(7)} H^{L7}_{32} &= \Delta^{(7)}(H_{312} + H_{322} + Z_{322})]_7 \\ &= \Delta^{(7)} H_{312}]_7, \end{aligned} \tag{22}$$

where symbol "$]_d$" denotes the operation that omits terms whose degree is smaller than d.

Let $\mathcal{F}(\cdot)$ be the function $\mathrm{GF}(2)^7 \times \mathrm{GF}(2)^9 \mapsto \mathrm{GF}(2)^7$ shown in Figure 3:

$$H_{312} = \mathcal{F}(X_0 + H_{133} + K_{222}, Y_{221}). \tag{23}$$

Note that Y_{221} is a constant for the chosen plaintext P. As X_0 spans $\mathrm{GF}(2)^7$, from Property 2, the following holds.

$$\begin{aligned}\Delta^{(7)} H_{312} &= \Delta^{(7)} \mathcal{F}(X_0 + H_{133} + K_{222}, Y_{221}) \\ &= \Delta^{(7)} \mathcal{F}(X_0, Y_{221}) \end{aligned} \tag{24}$$

From equation (22) and (24), we obtaine 7th order differential of H^{L7}_{32}:

$$\Delta^{(7)} H^{L7}_{32} = \Delta^{(7)} \mathcal{F}(X_0, Y_{221})]_7. \tag{25}$$

We calculated the Boolean expressions of H_{312} by using the computer algebra software REDUCE. As a result, we found the followings.

(1) The degree of H_{312} equals to 7.

(2) The value of 7th order differential of H^{L7}_{32} equals to 0x6D.

(3) The coefficients of terms whose degree is 6, are functions of elements in Y_{221}.

We show a part of them in Table 1.

$$X_{222} = (x_8,\ldots,x_0), \quad (X_{222} = X_0 + H_{133} + K_{222})$$
$$Y_{221} = (y_8,\ldots,y_0), \quad H_{312} = (\hat{h}_6,\ldots,\hat{h}_0)$$

The following attack equation can be derived using $\Delta^{(7)} H^{L7}_{32} = 0\text{x}6\text{D}$.

$$\begin{aligned}\sum_{A \in V^{(7)}} \{&FO(C_L(P+A) + \mathcal{K}_L; K_{522}, K_{521}, K_{512}, K_{511}) \\ &+ C_R(P+A) + \mathcal{K}_R\} \\ = 0&\text{x}6\text{D} \\ \mathcal{K} = (\mathcal{K}_L, \mathcal{K}_R), \quad &\mathcal{K}_L, \mathcal{K}_R \in \mathrm{GF}(2)^{32} \end{aligned} \tag{26}$$

The last equivalent key $\mathcal{K}$ can be moved as Figure 4. The equivalent key $\mathcal{K}_L$ is divided into $\mathcal{K}_{Ll}$ and $\mathcal{K}_{Lr}$ ($\in \mathrm{GF}(2)^{16}$) in FO_5 function. In FI_{51}, following holds.

$$\begin{aligned}\mathcal{K}_{511} &= K_{511} + \mathcal{K}^{L9}_{Ll} \\ \mathcal{K}_{512} &= K_{512} + \mathcal{K}^{R7}_{Ll} \end{aligned} \tag{27}$$

And In FI_{52}, the following holds.

$$\begin{aligned}\mathcal{K}_{521} &= K_{521} + \mathcal{K}^{L9}_{Lr} \\ \mathcal{K}_{522} &= K_{522} + \mathcal{K}^{R7}_{Lr} \end{aligned} \tag{28}$$

Thus, we can rewrite equation (26) as follows.

$$\sum_{A \in V^{(7)}} \{FO(C_L(P+A); \mathcal{K}_{522}, \mathcal{K}_{521}, \mathcal{K}_{512}, \mathcal{K}_{511})$$

Table 1 The Boolean expression of H_{312}

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

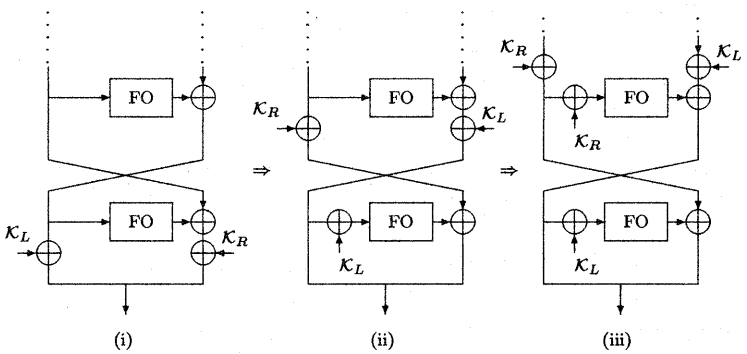


Figure 4 Transformation of Last Equivalent Key $\mathcal{K}$

$$+C_R(P + A)\}$$
$$= 0x6D \tag{29}$$

Because we construct the attack equation for 7[bit] output H_{32}^{L7}, the resultant equation is the vector equation on GF(2)^7. Note that the appropriate bit of $C_L(P)$, $C_R(P)$, and FO$(\cdot)$ is selected for the attack equation (29). We can calculate the true value of the last equivalent key $\mathcal{K}$ after all equivalent sub-keys are determined.

4.3 Number of chosen plaintexts and computational cost

4.3.1 One round elimination attack

We used algebraic method mentioned in Section 3.3. We regard all the variable terms with respect to $\mathcal{K}_{522}$, $\mathcal{K}_{521}$, $\mathcal{K}_{512}$ and $\mathcal{K}_{511}$ as the independent variables. The attack equation has two 9[bit] unknowns ($\mathcal{K}_{521}$ and $\mathcal{K}_{511}$) whose degree is 1, and two 7[bit] unknowns ($\mathcal{K}_{522}$ and $\mathcal{K}_{512}$) whose degree is 2. Thus the equation can be regarded as the linear equation taht has $L = 2 \times (9 + 7 + {}_7C_2) = 74$ unknowns. We can derive $n = 7$ linear equations from one 7th order differential. To solve the equation, we need $M = \lfloor \frac{74}{7} \rfloor \simeq 11$ different 7th order differentials. As a result, we need

$$M \times 2^N = 11 \times 2^7 = 1,408 \tag{30}$$

chosen plaintexts and

$$M \times 2^N \times L = 11 \times 2^7 \times 74 \simeq 2^{17} \tag{31}$$

times the number of FO function operation.

4.3.2 Two rounds elimination attack

In this section, we used two rounds elimination attack mentioned in Section 3.3. Because each FO function has a 75[bit] equivalent sub-key, $s = K^{(6)} = 75$. If we set up $m = 91$, the following holds.

$$2^s \times 2^{-m} = 2^{75} \times 2^{-91} \ll 1 \tag{32}$$

Thus we need $M' = \lfloor \frac{74 + 91}{7} \rfloor \simeq 24$ different 7th order differentials. As a result, we need

$$M' \times 2^N = 24 \times 2^7 \simeq 2^{12} \tag{33}$$

chosen plaintexts and

$$M \times 2^{N+s} \times L = 24 \times 2^{7+75} \times 74 \simeq 2^{93} \tag{34}$$

times the number of FO function operation.

5. Conclusion and discussions

Our results showed that 6-round MISTY1 without FL functions is attackable using 7th order differentials. Because our attack method used brute-force search for the 6th round sub-keys and algebraic method for part of 5th round sub-keys, it required 2^{12} chosen plaintexts and 2^{93} times the number of FO function operations. Thus, our attack method is estimated to be about 2^{30} times faster than the attack using a brute-force search for a 128-bit user key. Therefore, at least 7-rounds is necessary to resist higher order differential attack.

References

[1] Babbage, Frisch, "On MISTY1 Higher Order Differential Cryptanalysis", 3rd International Conference on Information Security and Cryptology 2000

[2] Daemen, Knudsen, Rijmen, "The Block Cipher SQUARE", FSE-6th International Workshop, LNCS.1636

[3] Jakobsen, Knudsen, "The Interpolation Attack on Block Cipher", FSE-4th International Workshop, LNCS.1372

[4] Knudsen, "Trancated and Higher Order Diferentials", FSE-2nd International Workshop, LNCS.1008

[5] Lai,"Higher Order Derivatives and Differential Cryptanalysis", Communications and Cryptography

[6] Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear cryptanalysis", FSE-3rd International Workshop, LNCS.1039

[7] Moriai, Shimoyama, Kaneko, "Higher Order Attack of a CAST Cipher", FSE-4th International Workshop, LNCS.1372

[8] Nyberg, Knudsen, "Provable Security against Differential Cryptanalysis", Jounal of Cryptology, Vol.8-no.1 (1995)

[9] Shimoyama, Moriai, Kaneko, "Improving the Higher Order Differential Attack and Cryptanalysis of the $\mathcal{KN}$ Cipher", 1997 Information Security Workshop, LNCS.1396

[10] Tanaka, Hisamatsu, Kaneko, "Strength of MISTY1 without FL function for Higher Order Differential Attack", 13th International Symposium, Applied Algebra - Algebraic Algorithms and Error-Correcting Codes 1999, LNCS.1719