A Practical-time Attack on Reduced-round MISTY1

Nobuyuki Sugio1, Yasutaka Igarashi2, Toshinobu Kaneko2 and Kenichi Higuchi2

1NTT DOCOMO, INC., 3-6 Hikarinooka, Yokosuka, Kanagawa, 239-8536, Japan
2Tokyo University of Science, 2641 Yamazaki, Noda, Chiba, 278-8510, Japan

Keywords: MISTY1, Symmetric Key Algorithm, Block Cipher, Higher Order Differential Attack.

Abstract: MISTY1 is a symmetric key algorithm which has been standardized by ISO and that its modified version is used in GSM and 3G mobile networks. MISTY1 is a 64-bit block cipher supporting key length of 128 bits. In this paper, we focused on evaluating the security of MISTY1 against higher order differential attack. We show 6-round MISTY1 with 4 FL layers is attackable with $2^{43}$ blocks of chosen plaintexts and $2^{53.31}$ times of data encryption. This is the best practical-time attack on reduced-round MISTY1.

1 INTRODUCTION

MISTY1 is one of the symmetric key algorithms. MISTY1 is a 64-bit block cipher supporting key length of 128 bits. MISTY1 was proposed by Matsui in 1997 (Matsui, 1997). The number of rounds is 8. MISTY1 achieves a provable security against differential cryptanalysis and linear cryptanalysis with round function FO. Designer adds on an auxiliary function FL in order to become secure against other attacks. MISTY1 was selected as one of the NESSIE-recommended ciphers portfolio and was adopted as the international standard by ISO/IEC 18033-3 (ISO, 2010). CRYPTREC project has chosen MISTY1 as one of the e-Government Recommended candidate ciphers in 2013 (CRYPTREC, 2013). Furthermore, the block cipher KASUMI designed as a slight modification of MISTY1 is used in the GSM/3G mobile networks, which makes it one of the most widely used block ciphers today.

Up to now, many cryptanalytic methods were used to evaluate the security of MISTY1 such as higher order differential attack, impossible differential attack, integral attack, and multi-dimensional zero correlation linear attack. The main previous attacks are as follows. Tsunoo et. al. proposed 46-th order differential and showed 7-round MISTY1 with 4 FL layers was attackable with $2^{34.1}$ chosen plaintexts and $2^{210.7}$ encryptions (Y. Tsunoo and Kawabata, 2008). Jia et. al. constructed a 7-round impossible differential and mounted impossible differential attack on 7-round MISTY1 with 3 FL layers (Jia and Li, 2012). Yi presented zero-correlation linear attack on 7-round MISTY1 with 4 FL layers, that requires $2^{62.9}$ known plaintexts and $2^{118}$ encryptions (Yi and Chen, 2014). Todo introduced Integral attack by division property, and showed that the secret key of the full MISTY1 can be recovered with $2^{63.58}$ chosen plaintexts and $2^{121}$ time complexity (Todo, 2015). Bar On improved the attack proposed by Todo, and presented full MISTY1 was attackable with $2^{54}$ chosen plaintexts and $2^{69.5}$ encryptions (Bar-On, 2015a).

Most of the previous attacks aimed at maximizing the number of attacked rounds, and as a result, their complexities are highly impractical. In this paper, we focused on evaluating the security of MISTY1 in terms of practical-time complexity. The previous practical-time attack was proposed by Hatano et. al. (Y. Hatano and Kaneko, 2004), and Dunkelman et. al. (Dunkelman and Keller, 2013), respectively. The best practical-time attack was higher order differential attack on 5-round MISTY1 with 4 FL layers. The necessary computational complexity by using higher order differential can be estimated as sum of the following 2-steps.

1. Preparation of data
2. Key recovery

The order of differential affects both steps. Therefore, it is very important to discover the lower order differential characteristics to reduce the complexity for an attack. The results we obtain are the following.

1. We implemented the 46th-order differential for 4-round MISTY1 introduced in (Y. Tsunoo and Kawabata, 2008) on a computer which mounted Graphics Processing Unit (GPU) co-processors.
and found 16-bits of the above characteristic was always 0. We gradually reduced the order of differentials for 4-round MISTY1 by computer experiment, and discovered new 38-th order differential characteristics for 4-round MISTY1 which held 7-bits of those differential characteristics 0.  

2. We can attack 6-round MISTY1 with 4 FL layers by using the 38-th order differential characteristic. The complexity for the attack needs 214.1 chosen plaintexts and 221.4 encryptions. Our method can reduce the necessary number of chosen plaintexts and the computational cost for the attack of 6-round MISTY1 with 4 FL layers illustrated in (Y. Tsunoo and Kawabata, 2008) by a factor of 210. This is the best practical-time attack on 6-round MISTY1.

2 MISTY1

MISTY1 is a Feistel type 64-bit block cipher supporting secret key length of 128 bits. MISTY1 was proposed by Matsui in 1997 (Matsui, 1997). The number of rounds which designer recommends is 8. MISTY1 achieves a provable security against differential cryptanalysis and linear cryptanalysis with round function FO. Designer adds on an auxiliary function FL in order to become secure against other attacks.

Figure 1 shows the main structure and components of the cipher. The round function FOi (1 ≤ i ≤ 8) is a variant of a 3-round Feistel construction which has 16-bit bijective function Fli (1 ≤ j ≤ 3) and 16-bit extended key KOi (1 ≤ j ≤ 4), KLj (1 ≤ j ≤ 3). Fli is a variant of a 3-round Feistel construction and its input is divided into left 9-bit data and right 7-bit data, which are transformed by bitwise XOR operations denoted by the symbol ⊕ and substitution tables S7 and S9. Klj1 and Klj2 are left 7-bit data and right 9-bit data of Fli, respectively. The key dependent linear function FLj are composed of bitwise AND operation denoted by the symbol ⊗, OR operation denoted by the symbol ∨, XOR operations and Klj (1 ≤ j ≤ 2).

The key schedule of MISTY1 takes the 128-bit secret key K to generate extended keys. Let Ki (1 ≤ i ≤ 8) be the i-th (from left) 16-bit data of the secret key K, and let KOi (1 ≤ i ≤ 8) be the output of Fli where the input of Fli is Ki and the key Klj is Ki+1. Also, identify K0 with K1. The correspondence between the

ICISSP 2016 - 2nd International Conference on Information Systems Security and Privacy

Table 1: Summary of single-key attacks on MISTY1.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>FL layers</th>
<th>Data</th>
<th>Time</th>
<th>Attack algorithm</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>4</td>
<td>22</td>
<td>228</td>
<td>Higher Order Differential</td>
<td>(Y. Hatano and Kaneko, 2004)</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>231</td>
<td>223.4</td>
<td>Impossible Differential</td>
<td>(Dunkelman and Keller, 2008)</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>233.7</td>
<td>253.7</td>
<td>Higher Order Differential</td>
<td>(Y. Tsunoo and Kawabata, 2008)</td>
</tr>
<tr>
<td>4</td>
<td>243</td>
<td>233.31</td>
<td>28</td>
<td>Higher Order Differential</td>
<td>Section5</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>220.2</td>
<td>214.4</td>
<td>Impossible Differential</td>
<td>(Dunkelman and Keller, 2008)</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>258</td>
<td>224.4</td>
<td>Impossible Differential</td>
<td>(Jia and Li, 2012)</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>262.9</td>
<td>2118</td>
<td>Multi-Zero Correlation</td>
<td>(Yi and Chen, 2014)</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>254.4</td>
<td>210.7</td>
<td>Higher Order Differential</td>
<td>(Y. Tsunoo and Kawabata, 2008)</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>251.45</td>
<td>2121</td>
<td>Higher Order Differential</td>
<td>(Bar-On, 2015b)</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>265.38</td>
<td>2121</td>
<td>Integral by division property</td>
<td>(Todo, 2015)</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>264</td>
<td>269.5</td>
<td>Integral by division property</td>
<td>(Bar-On, 2015a)</td>
</tr>
</tbody>
</table>

CP: Chosen Plaintexts, KP : Known Plaintexts.

Table 2: The Key Scheduling of MISTY1.

<table>
<thead>
<tr>
<th>KO1</th>
<th>KO2</th>
<th>KO3</th>
<th>KO4</th>
<th>KI1</th>
<th>KI2</th>
<th>KI3</th>
<th>KL1</th>
<th>KL2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ki</td>
<td>Ki+2</td>
<td>Ki+7</td>
<td>Ki+4</td>
<td>Kj+5</td>
<td>Kj+1</td>
<td>Kj+3</td>
<td>Kj+1</td>
<td>Kj+2</td>
</tr>
<tr>
<td>KI1</td>
<td>KI2</td>
<td>KI3</td>
<td>KL1</td>
<td>KL2</td>
<td>KL3</td>
<td>KL4</td>
<td>KL5</td>
<td>KL6</td>
</tr>
<tr>
<td>Kj+1 (odd i)</td>
<td>Kj+1 (odd i)</td>
<td>Kj+1 (even i)</td>
<td>Kj+1 (even i)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
symbols \( KO_{i,j}, KI_{i,j}, KL_{i,j} \) and the actual key is shown in Table 2. Here, \( K'_i \) is the output of \( FI_{i,j} \) where the input is \( K_i \) and the key is \( K_{i+1} \).

2.1 Notations Used in This Paper

We use the following notations for intermediate values during the MISTY1 encryptions process.

- The plaintext and ciphertext are denoted by \( P \) and \( C \). The left 32-bit value of \( P \) is denoted by \( P_L \) and the right 32-bit value of \( P \) is denoted by \( P_R \). The left 32-bit value of \( C \) is denoted by \( C_L \) and the right 32-bit value of \( C \) is denoted by \( C_R \), respectively.
- The input of \( i \)-th round (\( 1 \leq i \leq 8 \)) are denoted by \( X_i \). We denote the intermediate value after appli-
cation of FL functions by $X'_i$.

- Let $Z$ be an intermediate variable. $Z[k]$ denotes $k$-th bit of $Z$ and $Z[k-l]$ denotes bits from $k$ to $l$ of $Z$ respectively.

3 HIGHER ORDER DIFFERENTIAL ATTACK

This section gives an overview of higher order differential attack.

3.1 Higher Order Differential (Lai, 1994)

Let $E(\cdot)$ be an encryption function as follows.

$$Y = E(X; K)$$

where $X \in GF(2)^n$, $K \in GF(2)^l$, $Y \in GF(2)^m$. For a block cipher, $X$, $K$ and $Y$ denote plaintext, key and ciphertext respectively. Let $\{a_1, a_2, \ldots, a_i\}$ be a set of linearly independent vectors in $GF(2)^n$ and $V(i)$ be a sub-space spanned by these vectors. We define $\Delta^{(i)}_{V(i)} E(X; K)$ as an $i$-th order differential of $E(X; K)$ with respect to $X$ as follows.

$$\Delta^{(i)}_{V(i)} E(X; K) = \bigoplus_{A \in V(i)} E(X \oplus A; K)$$

In the following, we abbreviate $\Delta^{(i)}_{V(i)}$ as $\Delta^{(i)}$, when it is clearly understood. In this paper, we use the following properties of the higher order differential.

Property 1. If the degree of $E(X; K)$ with respect to $X$ equals to $d$, then

$$\text{deg}_X \{E(X; K)\} = d \iff \begin{cases} 
\Delta^{(d+1)} E(X; K) = 0 \\
\Delta^{(d)} E(X; K) = \text{const}
\end{cases}$$

Property 2. Higher order differential has a linear property on XOR sum. That means $d$-th order differential of the sum of each function equals to the sum of $d$-th order differential of each function.

$$\Delta^{(d)} \{E(X_1; K_1) \oplus E(X_2; K_2)\} = \Delta^{(d)} E(X_1; K_1) \oplus \Delta^{(d)} E(X_2; K_2)$$

3.2 Attack Equation

Consider an $R$-round iterative block cipher. Let $H_{R-1}(X) \in GF(2)^m$ be a part of the $(R-1)$-th round output and $C(X) \in GF(2)^n$ be the ciphertext corresponding to the plaintext $X \in GF(2)^n$. $H_{R-1}(X)$ is expressed as follows.

$$H_{R-1}(X) = F_{R-1}(\cdots F_2((F_1(X; K_1); K_2), \cdots, K_{R-1})$$

where $K_i \in GF(2)^l$ be the $i$-th round key and $F(\cdot)$ be a function of $GF(2)^n \times GF(2)^l \rightarrow GF(2)^m$.

If the degree of $H_{R-1}(X)$ with respect to $X$ is $d$, we have the following equation from Property 1.

$$\Delta^{(d+1)} H_{R-1}(X) = 0$$

This equation holds with probability 1.

Let $\tilde{F}(\cdot)$ be a decoding function that calculates $H_{R-1}(X)$ from a ciphertext $C(X) \in GF(2)^n$.

$$H_{R-1}(X) = \tilde{F}(C(X); K_R)$$

where $K_R \in GF(2)^l$ denotes the $R$-th round key to decode $H_{R-1}(X)$ from $C(X)$. From equation (6), (7) and (2), we can derive following equation.

$$\bigoplus_{A \in V^{(d+1)}} \tilde{F}(C(X \oplus A); K_R) = 0$$

We can determine $K_R$ by solving (8). In the following, we refer to equation (8) as an attack equation for key recovery.

3.3 Algebraic Method

Shimoyama et al. proposed an effective method of solving equation (8) (T. Shimoyama and Tsujii, 1999). This method, called algebraic method in this paper, expands equation (8) as boolean polynomials over GF(2), and linearizes by treating every higher order variables like $k_1 k_2$ with new independent variables like $k_{ij}$. In the following, we use the term linearized attack equation to refer to an attack equation that is regarded as a linear equation.

Let $L$ be the number of unknowns in the linearized attack equation (8). Since the equation (8) is derived by using an $m$-bit sub-block, we can rewrite equation (8) as follows.

$$A_k = b \cdot k = (k_1 k_2, \ldots, k_1 k_2, \ldots, k_1 k_2 k_3, \ldots)$$

where $A$, $b$, and $k$ are the $m \times L$ coefficient matrix, the $m$-dimensional vector, and the $L$-dimensional vector over GF(2). $k$ denotes linearized unknowns that are expressed as monomials of the $R$-th round key $K_R$.

We can obtain $m$ linearized attack equations from one $(d+1)$-th order differential because equation (8) is an $m$-bit equation. Therefore we need $[L/m]$ sets of the $(d+1)$-th order differential for the unique solution.

Since one set of $(d+1)$-th order differential requires $2^{d+1}$ chosen plaintexts, the necessary number
of plaintexts $D$ for the determination of a key is estimated as
\[
D = 2^{d+1} \times \left\lceil \frac{L}{m} \right\rceil
\] (10)

If we use the same technique shown in (T. Shimoyama and Tsuji, 1999), equation (9) requires $2^{d+1} \times (L+1)$ times of $\hat{F}(\cdot)$ calculations. Since we have to prepare $\lceil L/m \rceil$ sets of $(d+1)$-th order differentials to determine $k$, the computational cost\(^2\) is estimated as
\[
T = 2^{d+1} \times (L+1) \times \left\lceil \frac{L}{m} \right\rceil
\] (11)

Hatano et. al. proposed the optimization for algebraic method by analyzing the number of independent unknowns $I(\leq L)$ in equation (8) (Y. Hatano and Kaneko, 2004). If we can analyze the number of independent unknowns $I(\leq L)$ in equation (8), the $[l/m] \times l$ coefficient matrix $A_{op}$ and the $[l/m]$-dimensional vector $b_{op}$ is sufficient for solving the linearized attack equation.

4 HIGHER ORDER DIFFERENTIALS FOR REDUCED ROUND MISTY1

This section explains the previous results of higher order differential characteristic of MISTY1 and illustrates new higher order differential characteristics which we discovered. Here, $\alpha$ and $\beta$ denote fixed and variable sub-block respectively. For example, 64-bit variable $Y$ consisting of 3-bit variables $a$-th, $b$-th, and $c$-th bit of sub-block $\beta$ ($0 \leq a, b, c \leq 63, a \neq b \neq c$) can be denoted as $Y = \{Y[i] \in \alpha, Y[j] \in \beta | i \neq j, j = a, b, c, a \neq b \neq c\}$. A 3-rd order differential of intermediate variable $Z[k-l]$ by using $Y$ can be denoted as
\[
Y = \{Y[i] \in \alpha, Y[j] \in \beta | i \neq j, j = a, b, c, a \neq b \neq c\}
\]
\[
\Delta_{V(y)}^{(3)} Z[k-l]
\] (12)

where $0 \leq i, j, k, l \leq 63$ and $V^{(3)}$ is a subspace based on variable sub-block $Y[j]$.\(^4\)

4.1 Previous Results

Hatano et. al. proposed 14-th order differential of 3-round MISTY1 with FL functions (Y. Hatano and Kaneko, 2004).

\[
P = \{P[i] \in \alpha, P[j] \in \beta | i \neq j, 0 \leq j \leq 6, 16 \leq j \leq 22\}
\]
\[
\Delta_{V[i]}^{(14)} X_{\alpha}[63 - 57] = 0
\] (13)

where $V^{(14)}$ is the subspace based on variable sub-block $P[22 - 16, 6 - 0]$.

Tsunoo et. al. proposed 46-th order differential which was a 1-round extension of the 14-th order differential to the direction to plaintext. Due to the Feistel structure of MISTY1, the 3-round 14-th order differential can be extended to a 4-round 46-th order differential by taking all the $2^{32}$ possible values in the previous round. Thus, the following theorem could be derived.

**Theorem.** For four consecutive rounds of MISTY1 with FL functions that starts at 1-st round, the following equation independently holds under any fixed value of the key, constant value of the $P[i]$ ($39 \leq i \leq 47, 55 \leq i \leq 63$) and $V^{(46)}$ is the subspace based on variable sub-block $P_R$, $P[j]$ ($32 \leq j \leq 38, 48 \leq j \leq 54$).

\[
P = \{P[i] \in \alpha, P[j] \in \beta | 39 \leq i \leq 47, 55 \leq i \leq 63, 32 \leq j \leq 38, 48 \leq j \leq 54\}
\]
\[
\Delta_{V^{(46)}}^{(46)} X_{\beta}[63 - 57] = 0
\] (14)

4.2 New Higher Order Differential for MISTY1

In this subsection, we describe the new higher order differential characteristics for MISTY1 which were discovered by computer experiment.

46-th Order Differential Characteristic. We implemented 46-th order differential described in equation (14) on a computer which mounts Graphics Processing Unit (GPU) co-processors and found the following 46-th order differential characteristic.

\[
\Delta_{V^{(46)}}^{(46)} X_{\beta}[63 - 48] = 0
\] (15)

Although we verified equation (15) with 10 different keys and fixed sub-blocks, equation (15) always held. Since the provability of 10 sets 16-bit random variables incidentally becomes 0 is $2^{-160}$, we don’t think equation (15) accidentally holds.

38-th Order Differential Characteristic. We gradually reduced the order of differentials in equation (15) and discovered the new higher order
β shown in 32-bit state (α, β, α, β) are 3-bits variables out of 7-bits sub-blocks, respectively.

Figure 2: A new 38th order differential of MISTY1.

Differential characteristics as follows.

\[ P = \{ P'_i \in \alpha, P'_j \in \beta \mid i \neq j, i \neq k, 32 \leq i \leq 63, j = k + 16, k = h_1, h_2, h_3 (32 \leq h_1 < h_2 < h_3 \leq 38) \} \]  

\[ \Delta_{V^{(38)}, X_5[63 - 57]} = 0 \]

where \( h_1, h_2 \) and \( h_3 \) are bit patterns of variable sub-block. The variations of 38-th order differential illustrated in equation (16) exist \( _5^7 = 35 \) patterns.

Other Characteristics. We searched for the new higher order differential characteristics on 3-round, 4-round and 5-round MISTY1 respectively. The results are presented in Table 3.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>i-th order diff.</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>14 [^{[1]}]</td>
<td>( X_6[63 - 57] = 0 )</td>
</tr>
<tr>
<td>3</td>
<td>18</td>
<td>( X_4[63 - 48] = 0 )</td>
</tr>
<tr>
<td>3</td>
<td>N/A</td>
<td>( X_4[63 - 41] = 0 )</td>
</tr>
<tr>
<td>3</td>
<td>32</td>
<td>( X_4[63 - 32] = 0 )</td>
</tr>
<tr>
<td>4</td>
<td>38</td>
<td>( X_5[63 - 57] = 0 )</td>
</tr>
<tr>
<td>4</td>
<td>44</td>
<td>( X_5[63 - 48] = 0 )</td>
</tr>
<tr>
<td>4</td>
<td>50</td>
<td>( X_5[63 - 41] = 0 )</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>( X_5[63 - 32] = 0 )</td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

Table 3: The results of higher order differential characteristics on MISTY1.

We abbreviate \( \Delta_{V^{(i)}, X_i[63 - 57]} = 0 \) \((i = 7, 14)\) as \( X_i[63 - 57] = 0 \) in the table. This abbreviation is same other characteristics. The symbol ‘N/A’ means that we couldn’t find a higher order differential characteristic which satisfied \( \Delta_{V^{(i)}, X_i[63 - 41]} = 0 \) \((1 \leq i \leq 31)\). (*1) is discovered by Hatano (Y. Hatano and Kaneko, 2004). (*2) is discovered by Tanaka (H. Tanaka and Kaneko, 1999). (*3) is discovered by Igarashi (Igarashi and Kaneko, 2008).

We estimate the complexity for an attack by means of same procedure described in (Y. Tsunoo and Kawabata, 2008). Using the chosen plaintext denoted in equation (16), we have the following attack equation by assuming \( KL_{52}[15 - 9] = 0 \) \( t_f \). (See figure 3.)

\[ \bigoplus_{A \in V^{(38)}} \{ FO_8(X_6[63 - 32]; KO_{61}, KO_{62})[31 - 25] \} \bigoplus_{A \in V^{(38)}} FL_7^{-1}(C_i(X \oplus A); KL_{72})[31 - 25] = 0, X_6[63 - 32] = FL_8^{-1}(C_i(X \oplus A); KL_{81}, KL_{82}) \]

where \( FL^{-1} \) means an inverse function of FL. We divide the attack equation into seven kinds of 1-bit attack equations in order to increase the success probability. Assuming \( KL_{52}[15 - 9] = 0 \) \( t_f \), the seven kinds of 1-bit attack equations are written as

\[ \bigoplus_{A \in V^{(38)}} \{ FO_8(X_6[63 - 32]; KO_{61}, KO_{62})[i] \} \bigoplus_{A \in V^{(38)}} FL_7^{-1}(C_i(X \oplus A); KL_{72})[i] = 0, X_6[63 - 32] = FL_8^{-1}(C_i(X \oplus A); KL_{81}, KL_{82}) \]

where \( 25 \leq i \leq 31 \). Each 1-bit attack equation holds with probability \( 2^{-1} \). Using those equations, we can determine the key with probability \( 1 - 2^{-7} \), which means \( KL_{52}[15 - 9] \neq 0 \). Otherwise we can determine \( KL_{52}[15 - 9] = 0 \).

After linearization of the attack equation which consists of 7-bits width, we obtain the total number of unknown variables \( L = 1665 \) in a system of linear equations. If any of the unknown variables have linear sum relations, the complexity for attack can be reduced. In this paper, we chose independent un-
known variables as worst-case. Because every linearized attack equation was derived by 1-bit key assumption, additional 10 linear equations are needed to remove all false keys. From equation (10), the necessary number of chosen plaintexts  is estimated as

\[ D = 2^{38} \times \left\lceil \frac{189 + 10}{m} \right\rceil \]

where \( m = 1 \) since the attack solves equation (17) for each bit. Namely, \( D = 2^{38} \times 199 \approx 2^{55.7} \). Here, we can reduce the number of plaintexts \( D \) as follows. Let us consider a 43-rd order differential denoted equation (18).

\[ P = \{ P[i] \in \alpha, P[j, k, l], P_R \in \beta | i \neq j, k, l, j = k + 16 \} \]

\[ k = h_1, \sim, h_5 \text{ (} 32 \leq h_1 < h_2 < h_3 < h_4 < h_5 \leq 38 \) \]

\[ l = h_6 \text{ (} 32 \leq h_6 \leq 38, \text{ or } 48 \leq h_6 \leq 54 \) \]

(18)

A 43-rd order differential described in equation (18) can be used to construct \( 25 \times \binom{5}{3} = 320 \) sets of 38-th order differential. The explanation is as follows. The combination of choosing variable bit sub-blocks of 38-th order differential in equation (18) is \( \binom{5}{3} \), because we have to choose 3-bits from \( \{ h_1, \sim, h_5 \} \) as variable bit sub-blocks. When we regard one set of 43-rd order differential as some sets of 38-th order differential, the number of fixed bit sub-blocks in 43-rd order differential is five. 5-bits pattern includes \( 2^5 \) possible values. Thus, a 43-rd order differential illustrated in equation (18) generates \( 2^5 \times \binom{5}{3} = 320 > 199 \) sets of 38-th order differential. Therefore, the necessary number of chosen plaintexts \( D \) for key recovery is estimated as \( 2^{33} \).

Now, we consider the time complexity for this attack. The necessary computational cost for an attack can be estimated as sum of the following 2-steps.

1. Preparation of ciphertexts
2. Key recovery

The time complexity for a preparation of ciphertexts \( T_C \) is estimated as \( 2^{33} \) 6-round MISTY1 encryptions. From equation (11), the complexity for key recovery is estimated as follows.

\[ T_M = 2^{38} \times (1665 + 1) \times \left\lceil \frac{189 + 10}{1} \right\rceil \]

We can reduce the complexity by using a modulo 2 frequency distribution table. This table counts ciphertext values appearing an odd number of times since performing an XOR operation on the same value an even number of times results in a value of 0. We prepare 2 kinds of tables whose size are \( 2^{18} \) with respect to 18-bits \( C_L[32 \sim 23, 15 \sim 7] \) for 2 S9-boxes and \( 2^{14} \) with respect to 14-bits \( C_L[22 \sim 16, 6 \sim 0] \) for 2 S7-boxes respectively. The cost for generating these tables is \( T_t = 2^{38} \times 2 \times 199 \) table look-ups. If the computational cost for one table look-up equals to the cost for a S7, S9 look-up, \( T_t \) is estimated as

\[ T_t = 2^{38} \times 2 \times 199 \times 6 \times 9 \approx 2^{40.9} \]

encryptions because 6-round MISTY1 has \( 6 \times 9 \) S-boxes. The computational cost from equation (11) by using these tables is estimated as

\[ T_M = (2 \times 2^{18} + 2 \times 2^{14}) \times (1665 + 1) \times \left\lceil \frac{189 + 10}{1} \right\rceil \approx 2^{57.5} \]

S-box look-ups. \( T_M' \) is estimated as \( 2^{37.5} \) \( \frac{5}{3} \times 2^{57.5} \approx 2^{31.8} \) encryptions. The complexity for solving a system of equations resulting from linearization is negligible. The overall time complexity \( T \) is estimated as

\[ T = T_C + T_t + T_M' = 2^{43} + 2^{40.9} + 2^{31.8} \approx 2^{43.31} \]

times of 6-round MISTY1 encryptions. The time complexity \( T \) is dominated by the encryption of plaintexts.
6 CONCLUSIONS

In this paper, we focused on evaluating the security of MISTY1 in terms of practical-time complexity. We implemented the 46th-order differential characteristic for 4-round MISTY1 introduced in (Y. Tsunoo and Kawabata, 2008) on a computer which mounts GPU co-processors. We found 16-bits of 46-th order differential characteristic was 0. We discovered the new 38-th order differential characteristic for 4-round MISTY1 whose characteristic is equal to the characteristic estimated in (Y. Tsunoo and Kawabata, 2008). We applied the 38-th order differential characteristic to attack 6-round MISTY1 with 4 FL layers. The complexity for attack needs $2^{193}$ chosen plaintexts and $2^{193.31}$ encryptions. By using 38-th order differential, we can reduce the necessary number of data and time complexity for an attack on 6-round MISTY1 with 4 FL layers by a factor of $2^{10}$. This is the best practical-time attack on 6-round MISTY1.

REFERENCES


