Weak-Key Class of MISTY1 for Related-Key Differential Attack

Yi-bin Dai and Shao-zhen Chen

Zhengzhou Information Science and Technology Institute , Zhengzhou 450002, China
dybin321@163.com, chenshaozhen@vip.sina.com

Abstract. MISTY1 is a Feistel block cipher with presence in many cryptographic standards and applications. In this paper, according to analyzing the key schedule algorithm, a weak-key class encompassing $2^{102.57}$ weak keys of MISTY1 is found. Then we present 7-round related-key differential characteristics of MISTY1 under the weak-key class, which lead to the attacks on the 8-round MISTY1 without the first FL lay. The attack requires 2^{61} chosen ciphertexts, and the time complexities is $2^{84.6}$. To the best of our knowledge, the attack reported in this paper is the most powerful attack against MISTY1 with two related keys.

Keywords: MISTY1, weak-key, related-key, differential attack.

1 Introduction

The block cipher MISTY1 was proposed by M.Matsui [10], which was designed based on the principle of provable security against differential and linear cryptanalysis. MISTY1 is a 64-bit block cipher that has a key size of 128 bits. MISTY1 is used in many cryptographic standards and applications. For example, MISTY1 was selected to be in the final NESSIE portfolio of block ciphers, as well as an ISO standard.

Several cryptanalyses of MISTY1 have been reported. Slicing attack [7], collision search attack [6], integral attack [5], impossible differential attack [3,9], higher order differential attack [1,13,12,14,15] and the related-key amplified boomerang attack [8] can attack on reduced-round MISTY1. All of these attack can not attack on 8-round MISTY1. And the effective attack of these methods are higher order differential attack and related-key amplified boomerang attack, which lead to the attacks on 7-round MISTY1.

This paper concentrates on the key schedule algorithm since it is considered to be simple. According to our analysis of the key schedule, a weak-key class which has 2^{105} pairs related keys is found. Then combining the related-key attack [4,11] with the differential attack [2], we present a 7-round related-key differential characteristic of MISTY1, which lead to the attack on the 8-round MISTY1(without the first FL lay). Compared with the probability of 2^{-55} that the related keys exist in [8], the probability existing in this paper is 2^{-23}. Besides the attack requires two keys and can attack on the 8-round MISTY1(without the first FL lay).

C.-K. Wu, M. Yung, and D. Lin (Eds.): Inscrypt 2011, LNCS 7537, pp. 227–236, 2012.

We summarize our results along with previously known results on MISTY1 in Table 1.

This paper is organized as follows: In Section 2, we give a brief description of the structure of MISTY1. We describe the some Propositions of MISTY1 and introduce the related weak-key class in Section 3. In Section 4, we present the attack on 8-round MISTY1. Section 5 concludes the paper.

Table 1. Summary of the Attacks on MISTY1

Attack	Rounds	FL lays	Data	Time
Slice attack[7]	4	3	$2^{22.25}$CP	2^{45}
Collision attack[6]	4	3	2^{20}CP	2^{89}
Integral attack[5]	4	3	25CP	2^{27}
Integral attack[5]	5	3	2^{34}CP	2^{48}
Impossible differential attack[3]	$5^{\dagger}$	4	$2^{41.36}$CP	$2^{46.35}$
Higher order differential attack(weak key)[13]	6	4	$2^{18.9}$CP	$2^{80.6}$
Higher order differential attack[14]	6	4	$2^{53.7}$CP	$2^{64.4}$
Higher order differential attack[15]	6	4	$2^{53.7}$CP	$2^{53.7}$
Impossible differential attack[3]	6	4	2^{51}CP	$2^{123.4}$
Related-key amplified boomerang attack[8]$(2^{-55})^*$	7	3	2^{54}CP	$2^{55.3}$
Higher order differential attack[15]	7	4	$2^{54.1}$KP	$2^{120.7}$
Related-key differential attack$(2^{-23})^*$	7	4	2^{39}CC	$2^{39.5}$
Related-key differential attack(Sec[4])$(2^{-25.43})^*$	8	4	2^{61}CC	$2^{84.6}$

CP-Chosen plaintext; CC-Chosen ciphertext; KP-Known plaintext; $5^{\dagger}$-the attack retrieve 41.36 bits of information about the key; $(2^{-55})^*$ and $(2^{-25.43})^*$-the probability of the keys that exists in the attack.

2 The MISTY1 Cipher

In this section, we briefly describe the encryption and key schedule algorithm of MISTY1.

2.1 The Encryption Algorithm of MISTY1

MISTY1 [10] is a 64-bit block cipher with 128-bit keys. It has a recursive Feistel structure. The cipher has eight Feistel rounds. MISTY1 is composed of two functions: the non-linear function FO which is in itself close to a 3-round 32-bit Feistel construction and the function FL that mixes a 32-bit subkey with the data in a linear way.

The FO function also has a recursive structure: its round function called FI, is a three round Feistel construction. The FI function uses two non-linear S-boxes S7 and S9 (where S7 is a 7-bit to 7-bit permutation and S9 is a 9-bit to 9-bit permutation) . There is 112-bit subkey enters FO in each round 48 subkey bits are used in the FI functions and 64 subkey bits is used in the key mixing states.

The FL function is a simple linear transformation which accepts a 32-bit input and two 16-bit subkey words. One subkey word affects the data using the OR operation, while another subkey affects the data using the AND operation. We outline the structure of MISTY1 and its parts in Figure 1.

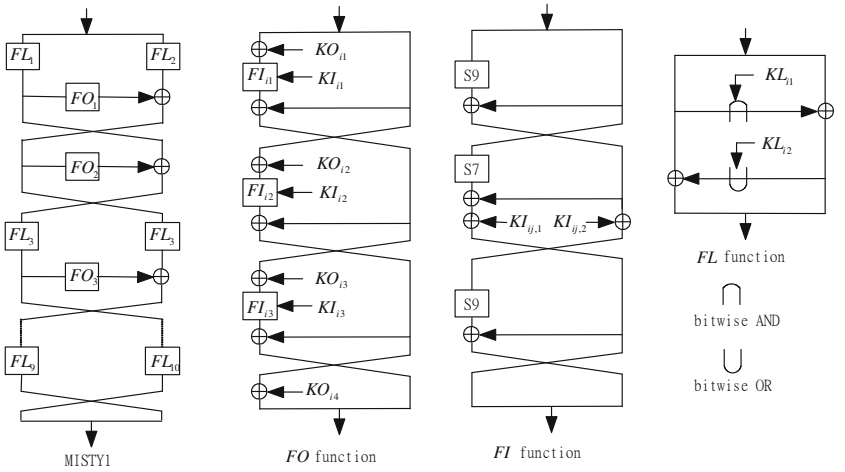

Fig. 1. Outline of MISTY1

2.2 The Key Schedule Algorithm of MISTY1

The key schedule of MISTY1 takes the 128-bit key, and treats it as eight 16-bit words:

$$K = K_1||K_2||K_3||K_4||K_5||K_6||K_7||K_8$$

From this set of subkeys, another eight 16-bit words are generated according to the non-linear FI function:

$$K'_i = FI_{K_{i+1}}(K_i), 1 \leq i \leq 8$$

Table 2. The Key Schedule Algorithm of MISTY1

KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	KL_{i1}	KL_{i2}
K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	$K_{\frac{i+1}{2}}(odd\ i)$	$K'_{\frac{i+1}{2}+6}(odd\ i)$
							$K'_{\frac{i}{2}+2}(even\ i)$	$K_{\frac{i}{2}+4}(even\ i)$

3 Preliminaries and Weak-Key Class of MISTY1

In this section, we will refer to some propositions of MISTY1. Then we find a weak-key class of MISTY1 for the 8-round related-key differential attack. Firstly, we give some denotations: $k = a^7 0^9$, $\beta = a^7 0^2 a^7$, where $a^7 = 0010000_2$ and $0^t = \overbrace{0 \cdots 0}^{t}$; $(K)_j$ shows the j-th bit of K (from the left side) , such as $K = 2000_x$, $(K)_3 = 1$.

3.1 Preliminaries

Here, we describe some propositions used in the related-key differential attack.

Observation 1. *Assume that the input difference of the function FI is 0^{16}, and the subkey difference of the function is k, then the output difference is β.*

Proposition 1. *Assume that the input difference of the FI function is k and the subkey difference is β, then the output difference of the FI function is 0^{16} with probability of 2^{-8}.*

Proof. The input difference of S9 is $a^7 0^2$, then the output difference of S9 is $0^2 a^7$ with probability of 2^{-8} which can kill the subkey difference, so that the output difference of the FI function is 0^{16} with probability of 2^{-8}.

Proposition 2. *Assume that the input bit difference of AND(or OR) operation is 1, and the key bit difference is 0, then the output bit difference is 1(or 0) with probability of 2^{-1}.*

Proposition 3. *Assume that the input difference of the FI function is k and the subkey difference is 0, then the output difference of the FI function is k with probability of 2^{-16} (The proposition can be verified experimentally).*

All of the propositions and observation described above are effectively used in the construction of the weak-key class and the related-key differential characteristic.

3.2 Weak-Key Class of MISTY1

We define the two 128-bit master keys K_a and K_b of MISTY1 that satisfy the following assumptions:

$$K_a = K_1||K_2||K_3||K_4||K_5||K_6||K_7||K_8$$

$$K_b = K_1||K_2||K_3||K_4||K_5||K_6^*||K_7||K_8,$$

where $K_6 \oplus K_6^* = k$.

According to the function FI, another two keys are generated:

$$K'_a = K'_1||K'_2||K'_3||K'_4||K'_5||K'_6||K'_7||K'_8$$

$$K'_b = K'_1||K'_2||K'_3||K'_4||K'^*_5||K'^*_6||K'_7||K'_8,$$

where $K'_i = FI_{K_{i+1}}(K_i)$, $1 \leq i \leq 8$, especially $K'^*_5 = FI_{K^*_6}(K_5)$, $K'^*_6 = FI_{K_7}(K'^*_6)$. Besides $K'_6 \oplus K'^*_6 = k$, $K'_5 \oplus K'^*_5 = \beta$. Obversely, the two keys K_a and K_b satisfy the following conditions:

$$\Delta K_{ab} = (0,0,0,0,0,k,0,0), \Delta K'_{ab} = (0,0,0,0,\beta,k,0,0)$$

Then assume that we give the following 7-bit keys:

$$(K_7)_3 = 1,\ (K_7)_{12} = 0,\ (K_8)_3 = 1,\ (K'_4)_3 = 1,\ (K'_4)_{12} = 1,\ (K_6)_{12} = 0,\ (K'_7)_3 = 0,$$

i.e. we know the following 7-bit key:
$(KL_{62})_3 = 1$, $(KL_{62})_{12} = 0$, $(KL_{82})_3 = 1$, $(KL_{41})_3 = 1$, $(KL_{41})_{12} = 1$, $(KL_{42})_{12} = 0$, $(KL_{10\ 1})_3 = 0$.
Besides, in order to construct the related-key differential characteristics, the following conditions should be ensure:

$$Pr[FI_{(\bullet,K_2\prime)}(k \longrightarrow k)] > 0$$

$$Pr[FI_{(\bullet,K_7\prime)}(\beta \longrightarrow k)] > 0$$

[1] Consequently, the number of the keys (K_6, K_7, K_8) and (K_2, K_3) which satisfy the conditions are $2^{29.57}$, that is to say, the probability is $2^{-2.43}$.

The set of all the key pairs satisfied the conditions above is called a weak-key class. The probability of the weak-key class is 2^{-23} $(= 2^{-16} \cdot 2^{-7})$, since

$$Pr[K'_6 \oplus K'^*_6 = k | K_6 \oplus K^*_6 = k] = 2^{-16}$$

$$Pr[K'_5 \oplus K'^*_5 = \beta | K_6 \oplus K^*_6 = k] = 1,$$

according to the Proposition.3, and $Pr[(K_7)_3 = 1, (K_7)_{12} = 0, (K_8)_3 = 1, (K'_4)_3 = 1, (K'_4)_{12} = 1, (K_6)_{12} = 0, (K'_7)_3 = 0] = 2^{-7}$, which can be verified experimentally. Hence, the number of the weak keys of the weak-key class is about $2^{102.57}$($= 2^{128} \cdot 2^{-23} \cdot 2^{-2.43}$).

4 Related-Key Differential Attack on 8-Round MISTY1 without the First FL Lay

In this section, we present a 7-round related-key differential characteristic of MISTY1 under the weak-key class. Then we attack on the 8-round MISTY1 without the first FL lay. The attack requires 2^{61} chosen ciphertexts and the time complexity is $2^{84.6}$.

[1] Thanks Jiqiang Lu presents the conditions.

Table 3. The Subkeys Difference of MISTY1

Round	ΔKO_{i1}	ΔKO_{i2}	ΔKO_{i3}	ΔKO_{i4}	ΔKI_{i1}	ΔKI_{i2}	ΔKI_{i3}	ΔKL_{i1}	ΔKL_{i2}
1	0	0	0	0	k	0	0	0	0
2	0	0	0	k	0	0	β	0	0
3	0	0	0	0	0	0	k	0	0
4	0	k	0	0	0	β	0	0	k
5	0	0	0	0	0	k	0	0	0
6	k	0	0	0	0	0	0	β	0
7	0	0	k	0	0	0	0	0	0
8	0	0	0	0	β	0	0	k	0
9	–	–	–	–	–	–	–	0	0
10	–	–	–	–	–	–	–	0	0

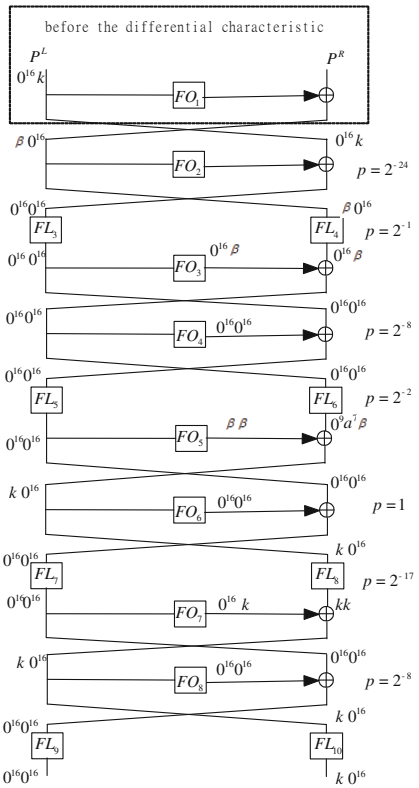

Fig. 2. 8-Round Related-key Differential Characteristics

4.1 The 7-Round Related-Key Differential Characteristic

Let the key pair (K_a, K_b) satisfies the following conditions:

$$\Delta K_{ab} = (0,0,0,0,0,k,0,0), \Delta K'_{ab} = (0,0,0,0,\beta,k,0,0)$$

and $(KL_{62})_3 = 1$, $(KL_{62})_{12} = 0$, $(KL_{82})_3 = 1$, $(KL_{41})_3 = 1$, $(KL_{41})_{12} = 1$, $(KL_{42})_{12} = 0$, $(KL_{10\ 1})_3 = 0$, $Pr[FI_{(\bullet,K_{2'})}(k \longrightarrow k)] > 0$, $Pr[FI_{(\bullet,K_{7'})}(\beta \longrightarrow k)] > 0$ i.e. the pair (K_a, K_b) is in the weak-key class. Then we can construct a 7-round related-key differential characteristic of MISTY1: $(\beta 0^{16}, 0^{16}k) \longrightarrow (0^{16}0^{16}, k0^{16})$ (See Figure 2) with probability of 2^{-58}, and the Table 3 gives the subkey difference of MISTY1.

Figure 2 and Table 4 illustrate the family and the probabilities of about 7-round differential characteristics in detail. The Proposition 1, 2, 3 are effectively used in the differential characteristics. Moreover, the given seven bits $(KL_{62})_3 = 1$, $(KL_{62})_{12} = 0$, $(KL_{82})_3 = 1$, $(KL_{41})_3 = 1$, $(KL_{41})_{12} = 1$, $(KL_{42})_{12} = 0$, $(KL_{10\ 1})_3 = 0$ ensure the following equations right: $FL_4(\beta 0^{16}) = 0^{16}\beta$, $FL_6(0^{16}0^{16}) = 0^9a^7\beta$, $FL_8(k0^{16}) = kk$, $FL_{10}(k0^{16}) = k0^{16}$. These elements correspond to some 7-round differential characteristics with probability of 2^{-58}, which is better than the random permutation, so that, the characteristic can lead to an attack on the full MISTY1 without the first FL lay.

Table 4. The 7-Round Related-Key Differential Characteristic

Round(i)	Difference	Probability
1	($\beta 0^{16}$, $0^{16}k$)	-
2	($0^{16}0^{16}$, $\beta 0^{16}$)	2^{-23}(Prop.1 and experiment)
3	($0^{16}0^{16}$, $0^{16}0^{16}$)	2^{-1}(Prop.2)
4	($0^{16}0^{16}$, $0^{16}0^{16}$)	2^{-8}(Prop.1)
5	($k0^{16}$, $0^{16}0^{16}$)	2^{-2}(Prop.2, 2 bits)
6	($0^{16}0^{16}$, $k0^{16}$)	1
7	($k0^{16}$, $0^{16}0^{16}$)	2^{-16}(Prop.1 and experiment)
8	($0^{16}0^{16}$, $k0^{16}$)	2^{-8}(Prop.1)
output†	($0^{16}0^{16}$, $k0^{16}$)	1

†: the output difference of the last FL lay.

4.2 Attack on 8-Round MISTY1 without the First FL Lay

According to the 7-round related-key differential characteristics of MISTY1, we attack the 7-round MISTY1.

The attack algorithm is as follows:

1. Choose m ciphertext pairs (C_a, C_b) that satisfy $C_a \oplus C_b = (0^{16}0^{16}, k0^{16})$. Ask for the decryption of all the ciphertexts under the keys K_a and K_b respectively and denote the plaintexts corresponding to (P_a, P_b);

2. For each plaintext pair (P_a, P_b), check $P_a^L \oplus P_b^L = 0^{16}k$. If this is not the case, discard the pair. After this test, about $m \cdot 2^{-32}$ pairs are expected remain;
3. For every guess KO_{11}, KO_{12}, KO_{13}, KI_{11}, $KI_{12,2}$ and $KI_{13,2}$, partially encrypt the FO_1, we can get the output difference of the FO_1. Then if the output difference does not match the corresponding bits of $P_a^R \oplus P_b^R \oplus 0^{32}$, discard the pairs. Do as follow :
   (a) Guess KO_{11} and KO_{12}, we get the left 7-bit output difference of the FI_{11} and FI_{12} respectively, then we can compute the 7-bit output difference of the FO_1. Compared with the corresponding bits of $(P_a^R \oplus P_b^R)$[2] . Discard all pairs if they do not pass the test. After the test, about $m \cdot 2^{-32} \cdot 2^{-7} = m \cdot 2^{-39}$ pairs are expected to remain.
   (b) Guess $KI_{11,2}$ and $KI_{12,2}$, we get the right 9-bit output difference of the FI_{11} and FI_{12} respectively, then we can compute the 9-bit output difference of the FO_1. Compared with the corresponding bits of $(P_a^R \oplus P_b^R)$. Discard all pairs if they do not pass the test. After the test, about $m \cdot 2^{-39} \cdot 2^{-9} = m \cdot 2^{-48}$ pairs are expected to remain.
   (c) Guess $KI_{11,1}$ and KO_{13}(only guess 15 bits, since $(KO_{13})_3 = (K_8)_3 = 1$), we get two output values of the FI_{13}. Then we can compute the 7-bit output difference of the FI_{13}, according to (a), we get the 7-bit output difference of the FO_1. Compared with the corresponding bits of $P_a^R \oplus P_b^R$. Discard all pairs if they do not pass the test. After the test, about $m \cdot 2^{-48} \cdot 2^{-7} = m \cdot 2^{-55}$ pairs are expected to remain.
   (d) Guess $KI_{13,2}$, we compute the right 9-bit output difference of the FI_{13}. According to (b), we can get the 9-bit output difference of the FO_1. Compared with the corresponding bits of $P_a^R \oplus P_b^R$. Discard all pairs if they do not pass the test; After the test, about $m \cdot 2^{-55} \cdot 2^{-9} = m \cdot 2^{-64}$ pairs are expected to remain. If $m = 2^{60}$, thus the expectation of the remaining plaintext pairs for the wrong key guess is about $2^{60} \cdot 2^{-64} = 2^{-4}$; the expectation of the remaining plaintext pairs for the right key guess is about $2^{60} \cdot 2^{-58} = 2^2$;
   (e) Output the subkey guess KO_{11}, KO_{12}, KO_{13}, KI_{11}, $KI_{12,2}$ and $KI_{13,2}$ as the correct subkey, if the number of the remaining pairs is bigger than 2. Otherwise, go to Step (3).

The attack requires about $2 \cdot 2^{60} = 2^{61}$ chosen ciphertexts.

We analyze the time complexity of the attack. There remains $2^{60} \cdot 2^{-32} = 2^{28}$ pairs after the step (2). In Step (a), the remaining pairs are treated with 2^{32} subkey candidates for KO_{11} and KO_{12}, so the time complexity is about $2 \cdot 2^{28} \cdot 2^{32} \cdot 1/8 = 2^{58}$ and about $2^{28} \cdot 2^{-7} = 2^{21}$ pairs remain; In Step (b), the remaining pairs are treated with 2^{18} subkey candidates for $KI_{11,2}$ and $KI_{12,2}$, so the time complexity is about $2 \cdot 2^{32} \cdot 2^{21} \cdot 2^{18} \cdot 1/8 = 2^{69}$ and about $2^{21} \cdot 2^{-9} = 2^{12}$ pairs remain; In Step (c), the remaining pairs are treated with 2^{22} subkey candidates for $KI_{11,1}$ and KO_{13}, so the time complexity is about $2 \cdot 2^{50} \cdot 2^{12} \cdot 2^{22} \cdot 1/8 = 2^{82}$ and about $2^{12} \cdot 2^{-7} = 2^5$ pairs remain; In Step (d), the remaining pairs are

[2] We replace $P_a^R \oplus P_b^R$ with $(P_a^R \oplus P_b^R \oplus 0^{32})$ for short.

treated with 2^9 subkey candidates for $KI_{13,2}$, so the time complexity is about $2 \cdot 2^{72} \cdot 2^5 \cdot 2^9 \cdot 1/8 = 2^{84}$ and about $2^5 \cdot 2^{-9} = 2^{-4}$ pairs remain.

Hence, the attack requires 2^{63} chosen ciphertexts and the complexity is $2^{58} + 2^{69} + 2^{82} + 2^{84} + 2 \cdot 2^{60} \approx 2^{84.6}$. Besides, by the *Possion* distribution, the success rate of the attack is 0.76.

Remark 1. The related-key differential characteristic can be used to attack on the 7-round MISTY1. The attack requires 2^{38} chosen ciphertexts, the time complexity is $2^{38.5}$ encryption.

5 Summary

In this paper, we analyze the key schedule algorithm of MISTY1 and describe a weak-key class. Then we present a 7-round related-key differential distinguisher of MISTY1 under the weak-key class. According to the distinguisher, we attack the 8-round MISTY1 which requires 2^{61} chosen ciphertexts and the time complexity is about $2^{84.6}$. Since our target, reduce round MISTY1, has FL function, this algorithm is more realistic and powerful than existing methods. We require the least number of chosen ciphertexts and the time complexity is smallest. Moreover, the attack requires two related keys and can attack on 8-round MISTY1 without the first FL lay.

Acknowledgement. This paper is supported by the National Natural Science Foundation of China (NO. 60673081), the opening Foundation of Key Laboratory of Information Security of China and the postgraduate subject of the strategics.

References

1. Babbage, S., Frisch, L.: On MISTY1 Higher Order Differential Cryptanalysis. In: Won, D. (ed.) ICISC 2000. LNCS, vol. 2015, pp. 22–36. Springer, Heidelberg (2001)
2. Biham, E.: New types of Cryptanalytic Attack Using Related Keys. J. Cryptology 7(4), 229–246 (1994)
3. Dunkelman, O., Keller, N.: An Improved Impossible Differential Attack on MISTY1. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 441–454. Springer, Heidelberg (2008)
4. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Zheng, Y., Seberry, J. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg (1993)
5. Knudsen, L.R., Wagner, D.: Integral Cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
6. Kühn, U.: Cryptanalysis of Reduced-Round MISTY. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 325–339. Springer, Heidelberg (2001)
7. Kühn, U.: Improved Cryptanalysis of MISTY1. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 61–75. Springer, Heidelberg (2002)
8. Lee, E., Kim, J., Hong, D., Lee, C., Sung, J., Lim, J.: Weak-key Classes of 7-Round MISTY1 and 2 for Related-Key Amplified Boomerang Attack. IEICE Transactions 91-A(2), 642–649 (2008)

9. Lu, J., Kim, J., Keller, N., Dunkelman, O.: Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. In: Malkin, T. (ed.) CT-RSA 2008. LNCS, vol. 4964, pp. 370–386. Springer, Heidelberg (2008)
10. Matsui, M.: New Block Encryption Algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)
11. Kelsey, J., Kohno, T., Schneier, B.: Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 75–93. Springer, Heidelberg (2001)
12. Sugita, M.: Higher Order Differential Attack of Block Cipher MISTY1, 2. In: ISEC 1998, IEICE (1998)
13. Tanaka, H., Hatano, Y., Sugio, N., Kaneko, T.: Security Analysis of MISTY1. In: Kim, S., Yung, M., Lee, H.-W. (eds.) WISA 2007. LNCS, vol. 4867, pp. 215–226. Springer, Heidelberg (2008)
14. Tsunoo, Y., Saito, T., Nakashima, H., Shigeri, M.: Higher Order Differential Attack on 6-Round MISTY1. IEICE Transactions 92-A(2) (2009)
15. Tsunoo, Y., Saito, T., Shigeri, M., Kawabata, T.: Higher Order Differential Attacks on Reduced-Round MISTY1. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 415–431. Springer, Heidelberg (2009)