A middletext distinguisher for full-round MISTY1

No Author Given

No Institute Given

Abstract. This paper presents the first successful attack against full MISTY1 under the known-key attack scenario. We apply existing higher order differentials to MISTY1, and adjust them to the scenario. Unfortunately, the simple concatenation of the higher order differentials, which is used in the attack against AES at Asiacrypt 2007 by Knudsen and Rijmen, does not work for full (8-round) MISTY1. We focus on the property of an FL function, and find that we can sometimes guess the output of the FL function from its input without knowing the value of subkey. Incorporating this analysis into the concatenation of higher order differentials, we successfully construct a distinguisher against full MISTY1. The number of queries, time complexity, memory requirement, and advantage of the attack are 2^{46}, 2^{46}, negligible, and 0.87, respectively.

Keywords: MISTY1, middletext distinguisher, known-key, higher order differential attack

1 Introduction

Since the standardization of the Data Encryption Standard (DES) [42], symmetric key cryptographers have been paying much more attention to the security of block ciphers. With modes of operation, e.g. [43, 45], a block cipher can be used for many purposes, including confidentiality and message authentication. This versatility enables block ciphers to be applied to many areas, and their long analysis history fosters a sense of confidence in security of block ciphers. MISTY1 [29] is one of the most popular block cipher algorithms.

MISTY was developed by Matsui of Mitsubishi Electric in 1997 [29], based on the theory of provable security [34, 33] against differential cryptanalysis [4] and linear cryptanalysis [27]. MISTY has a unique structure, the so-called *MISTY structure*, which is different from the Feistel structure used for DES. The MISTY structure enables parallel computation of two rounds and adopts the provable security theory [30]. Moreover, the provable security theory can also be applied to an unbalanced network. MISTY represents a family of block ciphers, and MISTY1 and MISTY2 are members of this family. Their block lengths are 64 bits and key lengths are 128 bits. MISTY1 uses the Feistel structure for its basic structure, while MISTY2 uses its own unique structure for the basic structure. Both ciphers achieve provable security against differential cryptanalysis and linear cryptanalysis. To achieve provable security, MISTY adopts a recursive construction, i.e., that is, their round functions are achieved using the MISTY structure. To strengthen the security against other attacks, MISTY1 and MISTY2 use an additional function, the FL function, where the FL function is non-linearly key-dependent and affine with a fixed key. MISTY1 has an FL layer every two rounds, and n-round MISTY1 has $1 + n/2$ FL layers. Additions in the FL function do not invalidate the provably secure property. During the development of MISTY, a higher order differential attack [18] turned out to be effective against ciphers whose s-boxes are based on a monomial of a Galois field and their algebraic degrees are relatively low [32]. The preliminary version [28] of the s-boxes in MISTY were replaced, and MISTY is expected to be more secure against a higher order differential attack.

MISTY1 was designed for practical use, and MISTY2 was designed for experimental use. MISTY1 was evaluated and standardized by many projects, including CRYPTREC (recommendations for Japanese e-Government use), NESSIE (New European Schemes for Signatures, Integrity, and Encryption), and ISO [16]. Moreover, its descendant, KASUMI, is used as a core primitive to secure 3G mobile communications.

Since MISTY1 has a long history, and many cryptanalytical studies are conducted. There were several studies on the pseudorandomness of the MISTY structure [35, 15, 10, 17, 14], which is similar to the Feistel structure [26]. Table 1 shows analytic results. Many analytic methods including cryptanalyses with impossible differentials, SQUARE attacks, and amplified boomerang attacks have been applied to MISTY1. Higher order differential attacks seem to be the most effective. MISTY1 reduced to 7 rounds with 4 FL layers can be attacked with $2^{54.1}$ chosen plaintexts and the time of $2^{120.8}$ encryptions [41], and MISTY1 reduced to 7 rounds without FL layers can be attacked with $2^{36.5}$ chosen plaintexts and the time of $2^{112.0}$ FO functions [13].

Table 1. MISTY1 attack results

Rounds	# of FL layers	Attack algorithm	Reference	Comments
4	2	collision	[22]	
4	2	impossible differential	[22]	
4	3	impossible differential	[23]	
4	3	slicing (+impossible differential)	[23]	
4	3	SQUARE	[20]	
5	0	higher order differential	[38]	
5	3	SQUARE	[20]	
5	4	higher order differential	[11]	
5	4	impossible differential	[9]	
6	0	impossible differential	[22]	
6	0	impossible differential	[25]	
6	4	higher order differential	[37]	weak key
6	4	higher order differential	[40]	
6	4	higher order differential	[39]	
6	4	impossible differential	[9]	
7	0	higher order differential	[37]	weak key
7	0	impossible differential	[9]	
7	0	higher order differential	[13]	
7	3	related-key amplified boomerang	[24]	weak key (rounds 2-8)
7	4	higher order differential	[40, 41]	
8	5	middletext higher order differential	This paper	
9	0	middletext higher order differential	This paper	

All of these attacks, which are listed in Table 1, are key recovery attacks. However, other vulnerabilities have recently been considered for block ciphers such as known-key attacks [19]. In a known-key attack, an attacker knows the key before the target of the cipher is distinguished. This scenario is not appropriate for the use of confidentiality, but it is sometimes appropriate for using hash functions. MISTY1 should be analyzed based on these new notions.

Knudsen and Rijmen proposed the known-key attacks [19], but they only reported their insights and examples. In Africacrypt 2009, Minier et al. formalized the known-key attack as a middletext distinguisher [31]. The middletext distinguisher does not cover all known-key distinguishers, but they are applicable to many existing known-key attacks, especially with higher order differential attacks [18], SQUARE attacks [7], and integral attacks [20]. These attacks combine two integrals to mount a middletext distinguisher, e.g. [19, 31].

This paper shows the first successful attack against full MISTY1 using a middletext distinguisher. We apply existing higher order differentials to MISTY1, and adjust them to the scenario in a manner similar to the attack in [19]. Unfortunately, the simple application of existing technique does not work against full MISTY1. To make a distinguisher against full MISTY1, we focus on an FL function. Each bit in 16-bit words is independent, and we can sometimes determine the output value of the FL function from its input without knowing the key value. Applying the analysis of the FL function to the concatenation of higher order differentials enables us to distinguish full (8-round) MISTY1 from random permutations.

This paper is organized as follows. Section 2 defines the specification of MISTY1 and some previous results. Section 3 shows a middletext distinguisher against 9-round MISTY1 without FL functions for better understanding of the next section. Section 4 shows a middletext distinguisher against full MISTY1. Section 5 concludes this paper.

2 Preliminaries

2.1 Specification of MISTY1

This section describes the specifications for MISTY1 used in this paper. Refer to [29] for details.

MISTY1 is a block cipher with a 64-bit block and a 128-bit key. Its structure is based on the Feistel structure with additional FL function layers. The round function is called an FO function. The number of rounds, n, is a multiple of four, and the recommended number of rounds is 8.

MISTY1 consists of two parts: a data randomizing part and a key scheduling part. The key scheduling part expands the secret key to subkeys KO_t, KI_t, and KL_t. In the data randomizing part, 64-bit plaintext P is divided into two 32-bit strings L_0 and R_0. The following is applied for $i = 0, 1, \dots, n-1$, where $\oplus$ is the bitwise XOR.

$$\begin{cases} i\text{: even} \begin{cases} L'_i \leftarrow FL_{KL_{i+1}}(L_i) \\ R'_i \leftarrow FL_{KL_{i+2}}(R_i) \end{cases} \quad i\text{: odd} \begin{cases} L'_i \leftarrow L_i \\ R'_i \leftarrow R_i \end{cases} \\ L_{i+1} \leftarrow FO_{KI_i,KO_i}(L'_i) \oplus R'_i \\ R_{i+1} \leftarrow L'_i \end{cases}$$

Before computing the ciphertext, one more FL layer is applied.

$$\begin{cases} L'_n \leftarrow FL_{KL_{n+1}}(L_n) \\ R'_n \leftarrow FL_{KL_{n+2}}(R_n) \end{cases}$$

Finally, ciphertext C is $R'_n \| L'_n$. Figure 1 illustrates the structure of MISTY1.

The FO function is a round function with a 32-bit input and output using two subkeys. The FO function consists of a 3-round MISTY structure, and its round function also consists of a 3-round unbalanced MISTY structure, where its round functions are based on 7-bit and 9-bit s-boxes. Note that we do not use the detailed property for the FO function other than the higher order differentials explained in Section 2.2.

The FL function is an additional simple function with a 32-bit input and output using a 32-bit subkey.

$$FL : \{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32}; \quad (x, k) \mapsto y$$

First, 32-bit input x is divided into two 16-bit strings, x_L and x_R, and 32-bit subkey input k is also divided into two 16-bit strings, k_1 and k_2. Then, the following computation is performed, where $\wedge$ and $\vee$ are the bitwise AND and OR, respectively. Figure 2 depicts the FL function.

$$\begin{cases} y_R \leftarrow x_R \oplus (x_L \wedge k_1) \\ y_L \leftarrow x_L \oplus (y_R \vee k_2) \end{cases}$$

Finally, the 32-bit output is the concatenation of y_L and y_R, that is, $y_L \| y_R$. Note that the FL function is an affine map with fixed key.

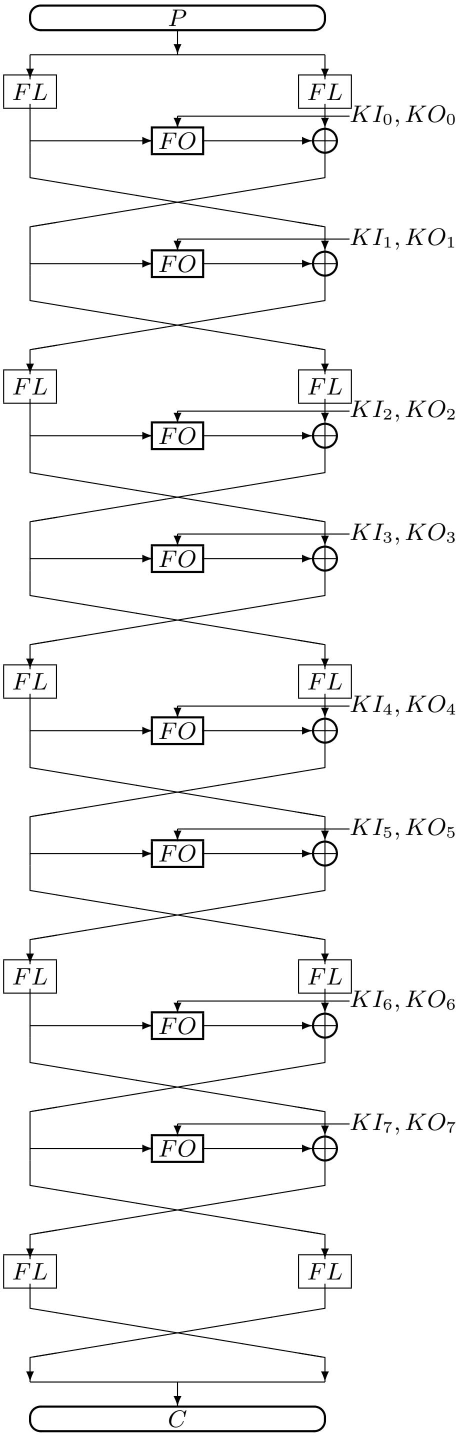


Fig. 1. Eight-round MISTY1

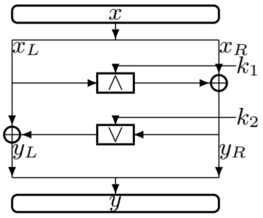


Fig. 2. FL function

2.2 Existing higher order differentials

Most of the higher order differentials in MISTY1 in previous work are based on the pioneering work by Tanaka et al. [38].

Property 1. Considering MISTY1 without FL functions, when the rightmost 7 bits of plaintext take all values and the other bits are fixed as constant,

$$\bigoplus L_3[31-25] = \texttt{0x6d},$$

where $x[i-j]$ represents that the bit-string from the jth bit to the ith bit of x and the rightmost bit is the 0th bit. Figure 3 illustrates this property.

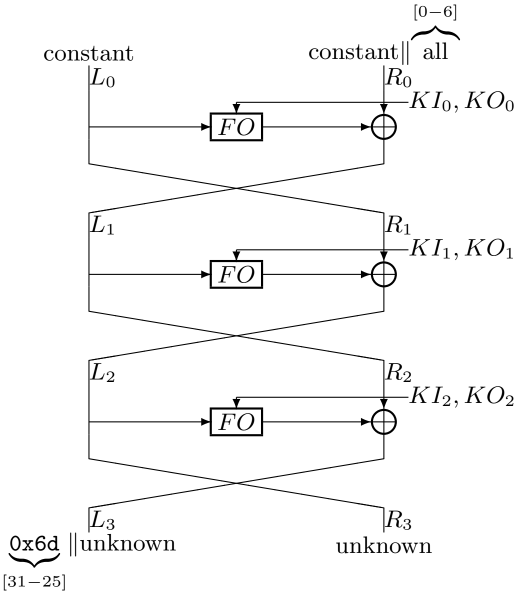


Fig. 3. Seventh order 3-round higher order differential of MISTY1 without FL functions

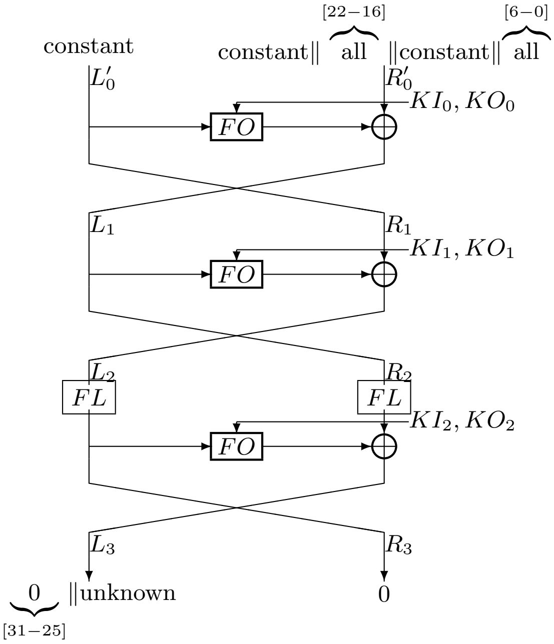


Fig. 4. Fourteenth order 3-round higher order differential for MISTY1

First, this property was found through computer experiments, and then analyzed by symbolic computation. After that, algebraic reasoning was shown in [2].

Taking into account the effect of FL function, the higher order characteristic are extended to the following property [11, Section 4.2].

Property 2. Taking all values for $R'_0[6-0]$ and $R'_0[22-16]$ and fixed other bits as constant for L'_0 and R'_0, the following equations hold.

$$\begin{cases} \bigoplus L_3[31-25] = 0 \\ \qquad\quad \bigoplus R_3 = 0 \end{cases}$$

Figure 4 illustrates this property.

This property was extended, e.g. [39, Section 4.1].

Property 3. For MISTY1 with FL functions, when $L_0[6-0]$, $L_0[22-16]$, and R_0 take all values and the other bits of L_0 are fixed constant, we have

$$\bigoplus L_4[31-25] = 0, \qquad \bigoplus R_4 = 0.$$

Figure 5 illustrates this property.

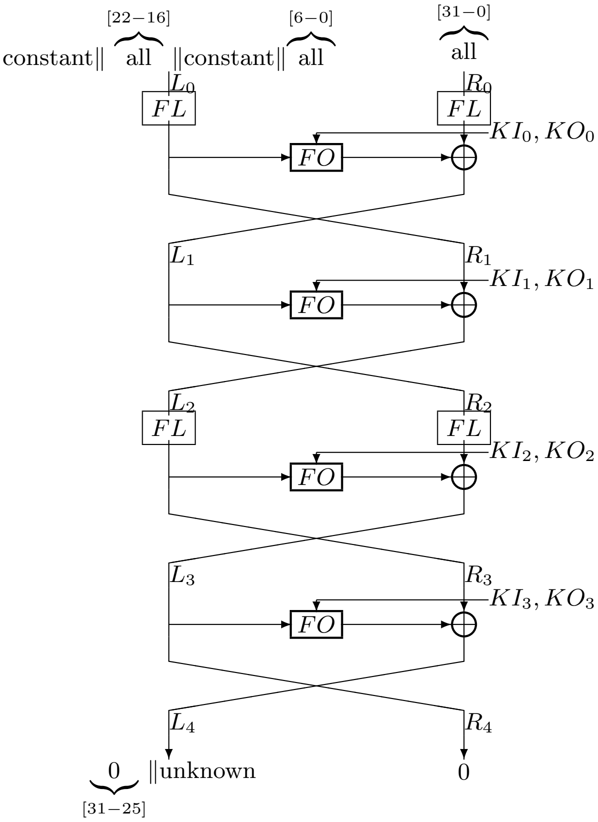


Fig. 5. Forty-sixth order 4-round higher order differential of MISTY1

For MISTY1 without FL functions, [13] shows another higher order differential.

Property 4. When R_0 takes all values and L_0 is fixed as constant, the following equation holds.

$$\bigoplus R_5[31-25] = 0.$$

Figure 6 illustrates this property.

2.3 Known-key attacks and middletext distinguisher

In the classical framework of the attack against block ciphers, an attacker does not know the secret key, while the secret key is given to the attacker in the framework of the known-key attack [19]. This framework sounds strange, but it became popular, because this framework relates the security of hash function constructions. Unfortunately, the formalization of the framework, which includes most non-ideal properties of a block cipher, has not yet been established. However, we believe that the scenario of the original proposal of the known-key attack [19] is worth considering to judge whether or not the cipher is secure. The proposal [19] considers the Square attack for AES [44]. The attacker chooses the intermediate states of AES and outputs a set of plaintexts and corresponding ciphertexts whose XORs are both 0. This distinguisher is called a *zero-sum distinguisher*. The details of the zero-sum distinguisher are discussed in the next section. This scenario can also be applied to higher order differential attacks in a similar way. Subsequently, at Africacrypt 2009, Minier et al. proposed an *NA-CMA* distinguisher [31]. We quote Algorithm 3 from the paper [31] as follows. We only consider Algorithm 3 for the known-key scenario.

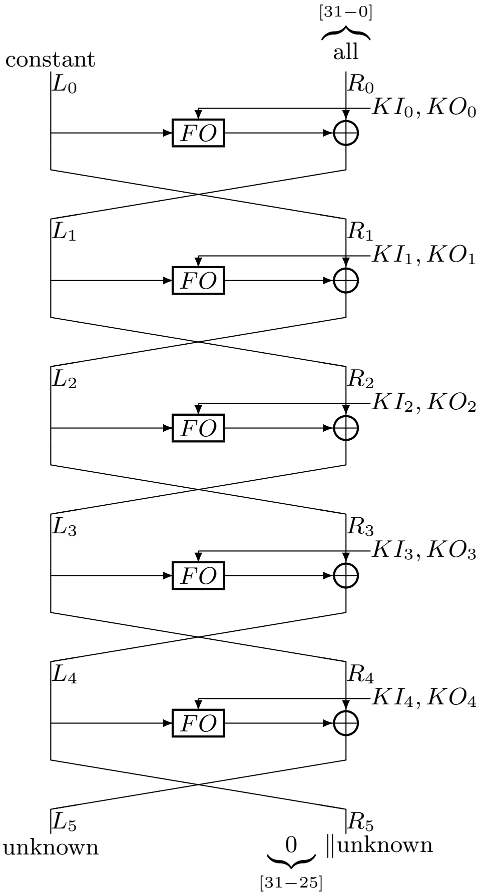


Fig. 6. Thirty-second order 5-round higher order differential of MISTY1 without FL functions

2.4 Zero-sum distinguishers

The zero-sum distinguisher, named by Aumasson [1], is already in use in the attack against AES [19] and other attacks such as the attacks against the internal block ciphers of the hash functions Keccak [3], *Luffa* [8], and Hamsi [21]. A zero-sum distinguisher finds a set of plaintexts such that the XOR of the plaintexts is zero and the XOR of the corresponding ciphertexts is also zero. When the number of queries is larger than the number of XORs, the zero-sum can sometimes easily be found and the advantage of the distinguisher is negligible. To be useful for the zero-sum distinguisher, Boura and Canteaut proposed a zero-sum partition problem [5] and applied it to Keccak and Hamsi, and their results are extended [6]. Sasaki and Aoki proposed a middletext distinguisher that restricts the number of queries to the same number of plaintexts to be XORed [36], and applied it to tweaked Lesamnta [12]. These papers also make *partial* zero-sum distinguishers meaningful, and this paper constructs a partial zero-sum distinguisher and its extension in the following sections.

3 A middletext distinguisher against up to 9-round MISTY1 without FL functions

This section describes a middletext distinguisher against 9-round MISTY1 without FL functions. The result in this section can be derived only by combining the previous works, that is, the concatenation of two higher order differentials can be used for the middletext distinguisher as is in [19]. For better understanding of the following sections, we describe this example against MISTY1 without FL functions.

Algorithm 3 An n-limited generic non-adaptive chosen middletexts distinguisher (*NA-CMA*)

```
Parameters: a complexity $n$, an acceptable set $A^{(n)}$
Oracle: an oracle $\mathcal{O}$ implementing internal functions $f_1$ (resp. $f_2$) of permutation $c$ that process input middletexts
    to the plaintext (resp. ciphertext) end
Compute some middletexts $\mathbf{M} = (M_1, M_2 \ldots, M_n)$
Query $\mathbf{P} = (P_1, P_2, \ldots, P_n) = (f_1(M_1), f_1(M_2), \ldots, f_1(M_n))$ and $\mathbf{C} = (C_1, C_2, \ldots, C_n) = (f_2(M_1), f_2(M_2),$
    $\ldots, f_2(M_n))$ to $\mathcal{O}$
if $(\mathbf{P}, \mathbf{C}) \in A^{(n)}$ then
    Output 1
else
    Output 0
end if
```

We know 5-round higher order differential shown in Property 4 for MISTY1 without FL functions. We concatenate it with its reversely ordered higher order differential, which is similar to that shown in [19]. We explain this using Figure 7.

As shown in [19], two higher order differentials can be combined together for a known-key setting. Applying Property 4 from the 4th to 8th round, we can always obtain $\bigoplus R_9[31-25] = \bigoplus C[63-57] = 0$, when we make L_4 a fixed constant and R_4 takes all values as middletexts in Algorithm 3. For decryption, we consider using the round-reverse order of the higher order differential shown in Property 4. In Figure 6, R_1 is a fixed constant and L_1 takes all values once. Thus, we can construct the 32nd order higher order differential of 4-round MISTY1. Since MISTY1 is symmetric between encryption and decryption, the same higher order differential holds for the decryption. Applying this higher order differential from the 3rd to 0th round, we also obtain $\bigoplus P[63-57] = 0$.

Using the discussion above, we construct the 2^{32}-limited *NM-CMA* distinguisher shown in Algorithm 3. The middletext is (L_4, R_4), oracle f_1 is the decryption from (L_4, R_4) to P, oracle f_2 is the encryption from (L_4, R_4) to C, and the acceptable set $A^{(2^{32})}$ is

$$\{(\mathbf{P}, \mathbf{C}) \mid \bigoplus_{i=1}^{2^{32}} P_i[63-57] = \bigoplus_{i=1}^{2^{32}} C_i[63-57] = 0\}.$$

The distinguisher collects a set of 2^{32} plaintexts whose XOR is 0 at bit positions $[63-57]$, and the XOR of the corresponding ciphertexts is also 0 at bit positions $[63-57]$. On the other hand, on an ideal cipher, the best way to achieve these partial zero-sums with exactly 2^{32} queries is as follows. The distinguisher queries 2^{32} plaintexts whose XOR is zero at bit positions $[63-57]$, and confirms whether or not the XOR of ciphertexts at bit positions $[63-57]$ is zero. Since the ciphertexts are observed as truly random bit strings, the probability for satisfying $\bigoplus C[63-57] = 0$ is 2^{-7}, while the probability using the higher order differentials to make a partial zero-sum is 1. So, the distinguisher is expected to achieve a significant advantage, $1-2^{-7}$. This attack requires the number of queries, time complexity, and memory requirement of 2^{32}, 2^{32}, and negligible, respectively.

4 A middletext distinguisher against 8-round MISTY1 with *FL* functions

This section describes how to construct a middletext distinguisher against full-round MISTY1. Figure 9 shows an outline of the distinguisher. Firstly, we combine two higher order differentials similar to that in Section 3: the round-reverse actualization of Property 3 and the higher order differential of Property 3. Because FO_{KI_3,KO_3} is shared between two differentials to make the chosen middletexts consistent, we need to adjust the computational order of the FL function

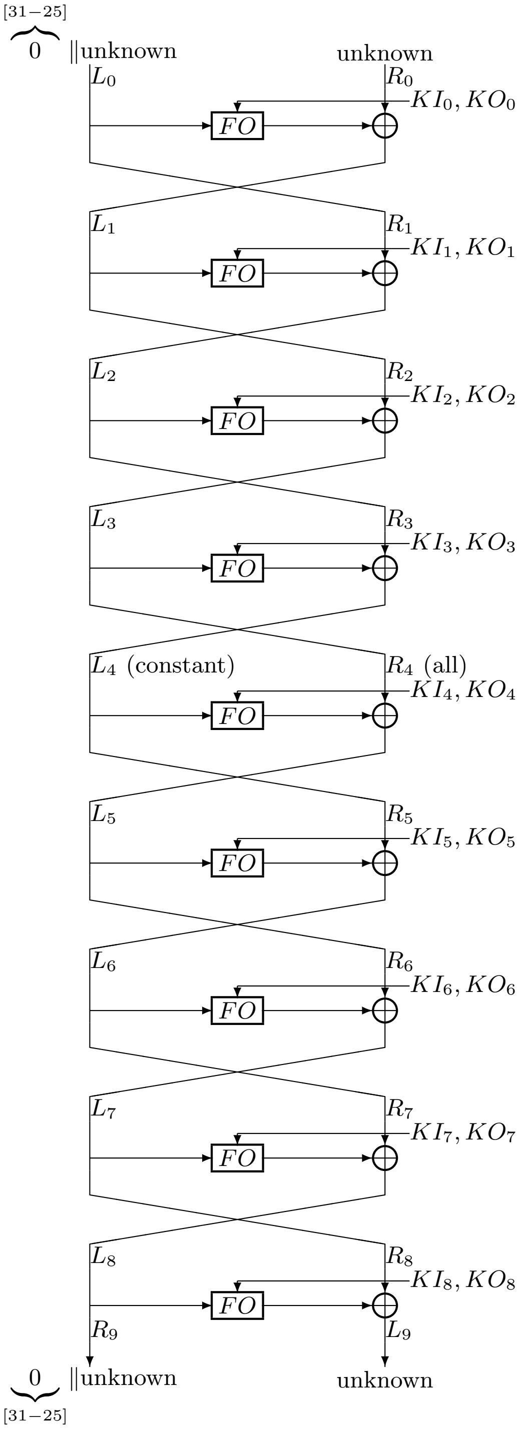


Fig. 7. A middletext distinguisher against 9-round MISTY1 without FL functions

in the latter higher order differential. However, the simple combination of two higher order differentials cannot include the last FL function, $R'_8 \leftarrow FL_{KL_{10}}(R_8)$. To solve this problem for constructing a full-round distinguisher, we analyze the FL function in detail, and derives some bias at R'_8 $(= C[63-32])$. Note that, on the plaintext side, Property 3 does not include the final FL layer which consists of two FL functions; however, we can achieve a zero-sum, because the FL functions are an affine function for a fixed key and one of their outputs L_0 $(= FL^{-1}_{KL_1}(L'_0))$ is a zero-sum.

The following describes the distinguisher in detail.

4.1 A middletext distinguisher against 8-round MISTY1 without one *FL* function

Similar to the distinguisher constructed in Section 3, we use Property 3 to construct the distinguisher. However, since MISTY1 with the FL functions is not symmetrical in terms of encryption and decryption, we need to establish the following property.

Property 5. Taking all values for L'_4, $R'_4[6-0]$, and $R'_4[22-16]$, and fixing other bits as constant for R'_4, the following equations hold.

$$\begin{cases} \bigoplus L'_0 = 0 \\ \bigoplus R'_0[31-25] = 0 \end{cases}$$

Figure 8 illustrates this property. Moreover, we have

$$\bigoplus L_0 = 0,$$

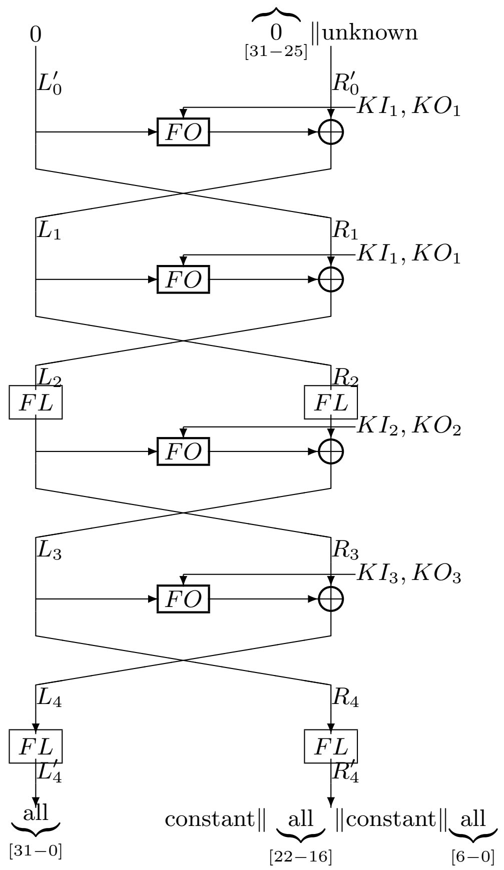
since (an inverse of) the FL function $(L_0 \leftarrow FL^{-1}_{KL_1}(L'_0))$ is an affine map and the number of XORs is even.

Proof. We can prove the above equations in the same way as in the proof of Property 3. However, since the inverse of the FL function is not an FL function, we need to confirm the same requirement as is used to prove Property 3 is applicable for FL^{-1}. When Property 3 was proved, we only used the following requirement: On the FL function, each bit in 16-bitwise words are independent and an affine map. This also holds for FL^{-1}.

Using Properties 5 and 2, we can mount a distinguisher against MISTY1 without one FL function that computes $R'_8 \leftarrow FL_{KL_{10}}(R_8)$. When we assume that $R'_4[6-0]$, $R'_4[22-16]$, and L'_4 take all values and other bits of R'_4 are fixed as constant, $\bigoplus C[63-57] = 0$ and $\bigoplus P[63-32] = 0$, because $P[63-32] = R_8[32-25] = L_7[32-25]$ and $\bigoplus L'_0 = 0$ hold. We can make this a partial zero-sum with probability 1, while we can make this a partial zero-sum for an ideal cipher with probability 2^{-7} using exactly 2^{46} queries. Note that we can attack MISTY1 even when $FL_{KL_{10}}(R_8)$ is replaced with $R_8 \oplus KL_{10}$. This fact implies that the XOR whitening cannot protect this distinguishing attack.

4.2 A middletext distinguisher against full MISTY1

This section extends the distinguisher described in the previous section. The previous section shows that we can find a zero-sum of $R_8[31-25]$, when we choose the following middletexts: L'_4, $R'_4[6-0]$, and $R'_4[22-16]$ take all values and other bits of R'_4 are fixed as constant. We try to confirm this zero-sum of $R_8[31-25]$ using R'_8, where $R_8 = FL^{-1}(R'_8)$ and $R'_8 = C[63-32]$. Unfortunately, we cannot confirm whether or not $\bigoplus R_8[31-25] = 0$ holds only using R'_8. However, we can sometimes guess the partial bits of $\bigoplus R_8[31-25]$. We can decide that the



0
$\overbrace{0}_{[31-25]}$||unknown
L'_0
R'_0
KI_1, KO_1
FO
L_1
R_1
KI_1, KO_1
FO
L_2
R_2
FL
FL
KI_2, KO_2
FO
L_3
R_3
KI_3, KO_3
FO
L_4
R_4
FL
FL
L'_4
R'_4
$\underbrace{\text{all}}_{[31-0]}$
constant|| $\underbrace{\text{all}}_{[22-16]}$ ||constant|| $\underbrace{\text{all}}_{[6-0]}$

Fig. 8. Forty-sixth order 4-round higher order differential for MISTY1 decryption

oracle implements an ideal permutation, when we know a bit of $\bigoplus R_8[31-25]$ is 1. With this guess, we construct a "partial" zero-sum distinguisher for full MISTY1.

First, we focus on the simple structure of the FL function, whose one input bit only depends on four bits of the subkey and output bits at most. Moreover, the upper 16-bit words of the input bits depends on 3 bits. We analyze this relation bit-by-bit between the input, output, and key in detail, and we find that several bits of the input R_8 of the FL function can be guessed from the output bits R'_8 without knowing the key. Figure 10 shows a graphical representation of the FL function to be analyzed. For each bit position j $(25 \leq j \leq 31)$, the input bits can be written as

$$\begin{aligned} R_8[j] &= R'_8[j] \oplus (R'_8[j-16] \vee KL_{10}[j-16]) \\ &= \begin{cases} KL_{10}[j-16] & \text{for } R'_8[j] = 0 \text{ and } R'_8[j-16] = 0 \\ 1 & \text{for } R'_8[j] = 0 \text{ and } R'_8[j-16] = 1 \\ \overline{KL_{10}[j-16]} & \text{for } R'_8[j] = 1 \text{ and } R'_8[j-16] = 0 \\ 0 & \text{for } R'_8[j] = 1 \text{ and } R'_8[j-16] = 1 \end{cases}, \end{aligned}$$

where $\overline{x}$ is the bitwise complement of x and $\overline{x} = x \oplus 1$.

Second, we analyze $\bigoplus R_8$ using the above analysis. We reorder the computation of the XOR $\bigoplus R_8[j]$ $(25 \leq j \leq 31)$ by the values of $(R'_8[j], R'_8[j-16])$.

$$\bigoplus R_8[j] = \bigoplus_{(R'_8[j],R'_8[j-16])=(0,0)} KL_{10}[j-16] \oplus \bigoplus_{(R'_8[j],R'_8[j-16])=(0,1)} 1$$

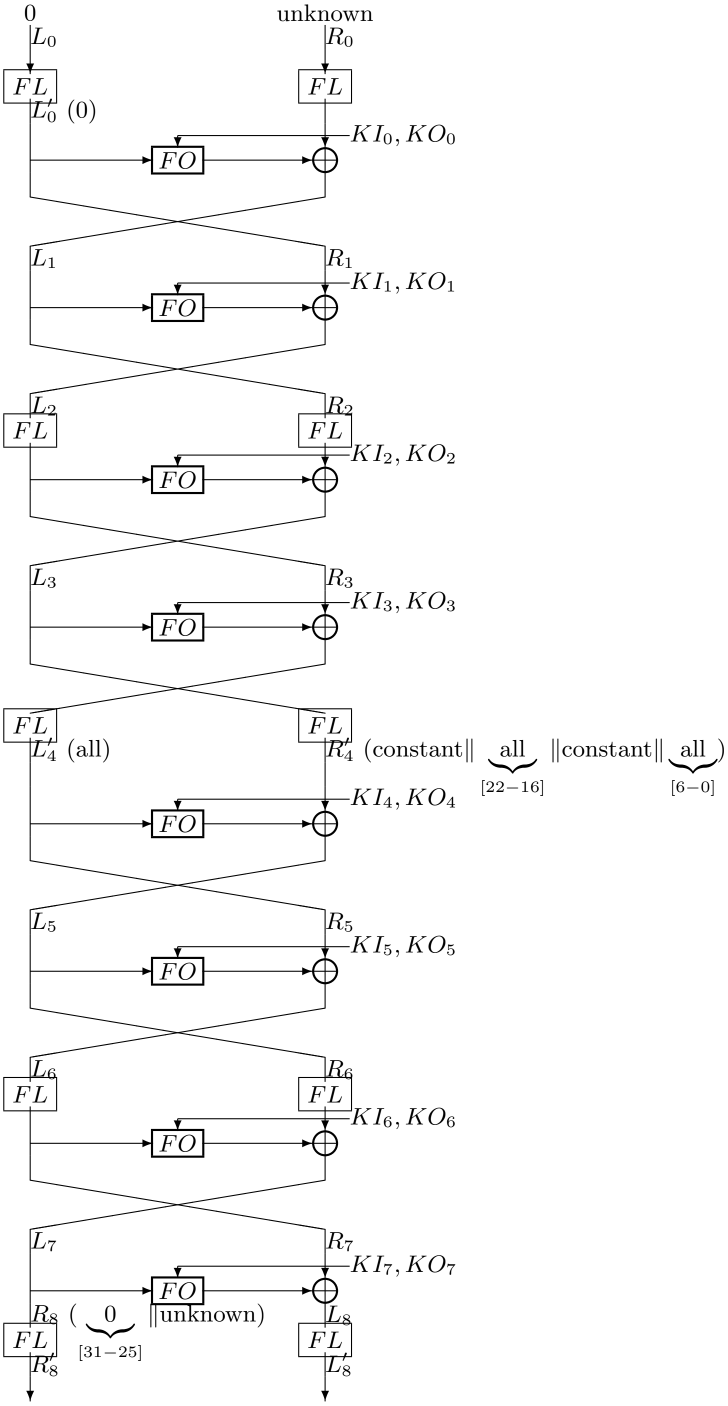


Fig. 9. A distinguisher against 8-round MISTY1

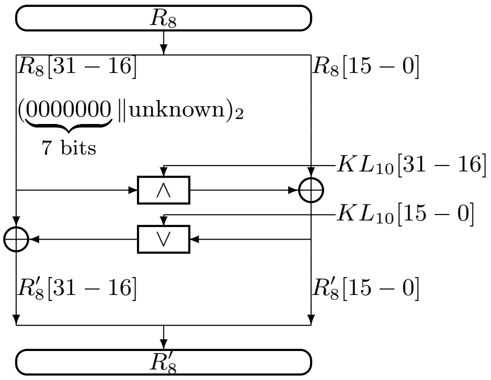


Fig. 10. $R'_8 \leftarrow FL_{KL_{10}}(R_8)$

$$\oplus \bigoplus_{(R'_8[j],R'_8[j-16])=(1,0)} \overline{KL_{10}[j-16]} \oplus \bigoplus_{(R'_8[j],R'_8[j-16])=(1,1)} 0$$

The XOR of each term can be determined by the parity of the occurrence of the value of $(R'_8[j], R'_8[j-16])$, since the XOR of the same two value makes zero. Table 2 summarizes the value $\bigoplus R_8[j]$ for all patterns of $(R'_8[j], R'_8[j-16])$. For example, the last row shows the case that $p_{(0,0)}[j] = p_{(0,1)}[j] = p_{(1,0)}[j] = p_{(1,1)}[j] = 1$, where $p_{(l,r)}[j] = \#\{(R'_8[j], R'_8[j-16]) \mid R'_8[j] = l,\ R'_8[j-16] = r\}$ mod 2. In this case, $\bigoplus R_8[j]$ can be computed as $KL_{10}[j-16] \oplus 1 \oplus \overline{KL_{10}[j-16]} \oplus 0$. Note that we do not need to consider the case that the total number of occurrences is odd, because we use an even number of queries, 2^{46}.

Table 2. Relation between R_8 and R'_8 based on the number of occurrence of $(R'_8[j], R'_8[j-16])$

$R'_8[j]$	0	0	1	1	
$R'_8[j-16]$	0	1	0	1	$\bigoplus R_8[j]$
	even	even	even	even	0
	even	even	odd	odd	$\overline{KL_{10}[j-16]}$
	even	odd	even	odd	1
	even	odd	odd	even	$KL_{10}[j-16]$
	odd	even	even	odd	$KL_{10}[j-16]$
	odd	even	odd	even	1
	odd	odd	even	even	$\overline{KL_{10}[j-16]}$
	odd	odd	odd	odd	0

Observing Table 2, $\bigoplus R_8[j]$ can sometimes be determined only by $p_{(l,r)}[j]$ without knowing the value of KL_{10}. Moreover, $\bigoplus R_8[j]$ may happen to be 1, but we know that $\bigoplus R_8[j]$ is always 0 when we choose the appropriate set of middletexts which is used in Section 4.1. We can distinguish full MISTY1 using this fact. Thus, the acceptable set for the middletext distinguisher is

$$\begin{aligned}&\{(\mathbf{P},\mathbf{C}) \mid \bigoplus_{i=1}^{2^{46}} P_i[63-32] = 0 \\ &\quad \text{and } ((p_{(0,0)}[j], p_{(0,1)}[j], p_{(1,0)}[j], p_{(1,1)}[j]) \neq (0,1,0,1) \text{ or } (1,0,1,0)) \text{ for } 25 \leq j \leq 31\},\end{aligned}$$

where $R'^{(i)}_8[j] \leftarrow C_i[32+j]$ and $p_{(h,l)}[j]$ is defined as above. After the distinguisher queries the chosen middletexts to the oracle and receives the set $(P_i, C_i)_{i=1}^{2^{46}}$, the distinguisher can confirm whether or not the set belongs to the acceptable set as follows. First, confirmation of $\bigoplus P_i[63-32]=0$ is performed. If it does not hold, the set does not belong to the acceptable set. Then, for each j $(25 \leq j \leq 31)$ and $(r,l) \in \{(0,0),(0,1),(1,0),(1,1)\}$, to count the parity of occurrences of the pattern $(C_i[j+32], C_i[j+16])$ to construct $p_{(h,l)}[j]$. If $(p_{(0,0)}[j], p_{(0,1)}[j], p_{(1,0)}[j], p_{(1,1)}[j]) = (0,1,0,1)$ or $(1,0,1,0)$ holds, the set does not belong to the acceptable set. This confirmation can efficiently be done, since the confirmation can be performed by XOR and the count of the occurrence of the simple patterns.

We evaluate the advantage of the distinguisher. When the oracle implements MISTY1, the received $(\mathbf{P},\mathbf{C})$ is an element of the acceptable set with probability 1. When the oracle implements an ideal permutation, an adversary can choose appropriate plaintexts that satisfy $\bigoplus P_i[63-32]=0$. However, because the adversary cannot control the ciphertext, $(p_{(0,0)}[j], p_{(0,1)}[j], p_{(1,0)}[j], p_{(1,1)}[j]) = (0,1,0,1)$ or $(1,0,1,0)$ holds with probability $2/8$ for each j $(25 \leq j \leq 31)$. That is, the adversary succeeds to cheat that the oracle behaves as MISTY1 with probability $6/8$ for each j $(25 \leq j \leq 31)$. In summary, the advantage of the attack is 0.87 $(\approx 1-(6/8)^7)$. The distinguisher requires the number of queries, time complexity, and memory requirement of 2^{46}, 2^{46}, and negligible, respectively.

Remark. We have 18 constant bits for the chosen middletexts. By using these constant bits, we expect to have a higher advantage using more middletexts. When t $(t < 18)$ bits are used, the advantage will be $1-(6/8)^{7t}$, and it is approximately $1-2^{-49.4}$ when $t=17$.

5 Conclusion

This paper presented a middletext distinguisher for full MISTY1. We analyzed the detailed property of the FL function and used the existing higher order differentials to construct the distinguisher. The query complexity of the attack is 2^{46}, the time complexity is 2^{46}, the memory requirement is negligible, and the advantage of the attack is 0.87. The proposed middletext distinguisher shows a non-ideal property, but they can be used for a very specific environment. It is hard to imagine that an actual application of MISTY1 is affected by this middletext distinguisher.

References

1. Jean-Philippe Aumasson. Zero-sum distinguishers. (Rump session talk at CHES 2009 `http://131002.net/data/talks/zerosum_rump.pdf`), 2009.
2. Steve Babbage and Laurent Frisch. On MISTY1 higher order differential cryptanalysis. In Dongho Won, editor, *Information Security and Cryptology — ICISC 2000, Third International Conference*, volume 2015 of *Lecture Notes in Computer Science*, pages 22–36. Springer-Verlag, Berlin, Heidelberg, New York, 2001.
3. Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. KECCAK *specifications — Version 2.* STMicroelectronics and NXP Semiconductors, 2009. (`http://keccak.noekeon.org/files.html`).
4. Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer-Verlag, Berlin, Heidelberg, New York, 1993.
5. Christina Boura and Anne Canteaut. Zero-sum distinguishers for iterated permutations and application to KECCAK-f and Hamsi-256. In Alex Biryukov, Guang Gong, and Douglas Stinson, editors, *Selected Areas in Cryptography, 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers*, volume 6544 of *Lecture Notes in Computer Science*, pages 1–17, Berlin, Heidelberg, 2011. Springer-Verlag.
6. Christina Boura, Anne Canteaut, and Christophe De Cannière. Higher-order differential properties of KECCAK and *Luffa*. In Antoine Joux, editor, *Fast Software Encryption — 18th International Workshop, FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 252–269, Berlin, Heidelberg, New York, 2011. Springer-Verlag.
7. Joan Daemen, Lars Ramkilde Knudsen, and Vincent Rijmen. The block cipher SQUARE. In Eli Biham, editor, *Fast Software Encryption — 4th International Workshop, FSE'97*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68, Berlin, Heidelberg, New York, 1997. Springer-Verlag.

8. Christophe De Cannière, Hisayoshi Sato, and Dai Watanabe. *Hash Function Luffa — Specification Ver 2.0.1.* Hitachi, Ltd., 2009. (`http://www.sdl.hitachi.co.jp/crypto/luffa/`).
9. Orr Dunkelman and Nathan Keller. An improved impossible differential attack on MISTY1. In Josef Pieprzyk, editor, *Advances in Cryptology — ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 441–454. Springer-Verlag, Berlin, Heidelberg, New York, 2008.
10. Henri Gilbert and Marine Minier. New results on the pseudorandomness of some blockcipher constructions. In Mitsuru Matsui, editor, *Fast Software Encryption — 8th International Workshop, FSE 2001*, volume 2355 of *Lecture Notes in Computer Science*, pages 248–266, Berlin, Heidelberg, New York, 2002. Springer-Verlag.
11. Yasuo Hatano, Hidema Tanaka, and Toshinobu Kaneko. Optimization for the algebraic method and its application to an attack of MISTY1. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, E87-A(1):18–27, 2004.
12. Shoichi Hirose, Hidenori Kuwakado, and Hirotaka Yoshida. *SHA-3 Proposal: Lesamnta.* Hitachi Ltd., 2008. (`http://www.hitachi.com/rd/yrl/crypto/lesamnta/`).
13. Yasutaka Igarashi and Toshinobu Kaneko. The 32nd-order differential attack on MISTY1 without FL functions. In *International Symposium on Information Theory and Its Applications*, ISITA2008, pages W–TI–4–4, Auckland, New Zealand, 2008.
14. Tetsu Iwata, Tohru Yagi, and Kaoru Kurosawa. On the pseudorandomness of KASUMI type permutations. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, E87-A(5):1098–1109, 2004.
15. Tetsu Iwata, Tomonobu Yoshino, Tomohiro Yuasa, and Kaoru Kurosawa. Round security and super-pseudorandomness of MISTY type structure. In Mitsuru Matsui, editor, *Fast Software Encryption — 8th International Workshop, FSE 2001*, volume 2355 of *Lecture Notes in Computer Science*, pages 233–247, Berlin, Heidelberg, New York, 2002. Springer-Verlag.
16. JTC1. *ISO/IEC 18033: Security techniques — Encryption algorithms — Part 3: Block ciphers*, 2005.
17. Ju-Sung Kang, Okyeon Yi, Dowon Hong, and Hyunsook Cho. Pseudorandomness of MISTY-type transformations and the block cipher KASUMI. In Vijay Varadharajan and Yi Mu, editors, *Information Security and Privacy, 6th Australasian Conference, ACISP 2001*, volume 2119 of *Lecture Notes in Computer Science*, pages 60–73, Berlin, Heidelberg, New York, 2001. Springer-Verlag.
18. Lars Ramkilde Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, *Fast Software Encryption — Second International Workshop*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer-Verlag, Berlin, Heidelberg, New York, 1995.
19. Lars Ramkilde Knudsen and Vincent Rijmen. Known-key distinguishers for some block ciphers. In Kaoru Kurosawa, editor, *Advances in Cryptology — ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 315–324. Springer-Verlag, Berlin, Heidelberg, New York, 2007.
20. Lars Ramkilde Knudsen and David Wagner. Integral cryptanalysis. In Joan Daemen and Vincent Rijmen, editors, *Fast Software Encryption — 9th International Workshop, FSE 2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 112–127, Berlin, Heidelberg, 2002. Springer-Verlag.
21. Özgül Küçük. *The Hash Function Hamsi (2nd Round Updates)*, 2009. (`http://homes.esat.kuleuven.be/~okucuk/hamsi/specification.html`).
22. Ulrich Kühn. Cryptanalysis of reduced-round MISTY. In Birgit Pfitzmann, editor, *Advances in Cryptology — EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 325–339. Springer-Verlag, Berlin, Heidelberg, New York, 2001.
23. Ulrich Kühn. Improved cryptanalysis of MISTY1. In Joan Daemen and Vincent Rijmen, editors, *Fast Software Encryption — 9th International Workshop, FSE 2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 61–75, Berlin, Heidelberg, 2002. Springer-Verlag.
24. Eunjin Lee, Jongsung Kim, Deukjo Hong, Changhoon Lee, Jaechul Sung, Seokhie Hong, and Jongin Lim. Weak-key classes of 7-round MISTY 1 and 2 for related-key amplified boomerang attacks. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, E91-A(2):642–649, 2008.
25. Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In Tal Malkin, editor, *Topics in Cryptology - CT-RSA 2008: The Cryptographers' Track at the RSA Conference 2008*, volume 4964 of *Lecture Notes in Computer Science*, pages 370–386, Berlin, Heidelberg, New York, 2008. Springer-Verlag.
26. Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *Journal of Computing (Society for Industrial and Applied Mathematics)*, 17(2):373–386, 1988.
27. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, Heidelberg, New York, 1994. (A preliminary version written in Japanese was presented at SCIS93-3C).
28. Mitsuru Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In Dieter Gollmann, editor, *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 1996, Proceedings*, volume 1039 of *Lecture Notes in Computer Science*, pages 205–218. Springer-Verlag, Berlin, Heidelberg, New York, 1996. (Japanese version was presented at SCIS96-4C).

29. Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *Fast Software Encryption — 4th International Workshop, FSE'97*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68, Berlin, Heidelberg, New York, 1997. Springer-Verlag. (A preliminary version written in Japanese was presented at ISEC96-11).
30. Mitsuru Matsui. On a structure of block ciphers with provable security against differential and linear cryptanalysis. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, E82-A(1):117–122, 1999. (Preliminary version was presented at SCIS96-4C in Japanese and FSE'96 in English).
31. Marine Minier, Raphael Chung-Wei Phan, and Benjamin Pousse. Distinguishers for ciphers and known key attack against Rijndael with large blocks. In Bart Preneel, editor, *Progress in Cryptology - AFRICACRYPT 2009, Second International Conference on Cryptology in Africa*, volume 5580 of *Lecture Notes in Computer Science*, pages 60–76, Berlin, Heidelberg, New York, 2009. Springer-Verlag.
32. Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer-Verlag, Berlin, Heidelberg, New York, 1994.
33. Kaisa Nyberg. Linear approximation of block ciphers. In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 439–444. Springer-Verlag, Berlin, Heidelberg, New York, 1995.
34. Kaisa Nyberg and Lars Ramkilde Knudsen. Provable security against a differential attack. *Journal of Cryptology*, 8(1):27–37, 1995. (A preliminary version was presented at CRYPTO'92 rump session).
35. Kouichi Sakurai and Yuliang Zheng. On non-pseudorandomness from block ciphers with provable immunity against linear cryptanalysis. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, E80-A(1):19–24, 1997.
36. Yu Sasaki and Kazumaro Aoki. Improved integral analysis on tweaked lesamnta. In Howon Kim, editor, *Information Security and Cryptology — ICISC 2011*, Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York, 2012. *to appear*.
37. Hidema Tanaka, Yasuo Hatano, Nobuyuki Sugio, and Toshinobu Kaneko. Security analysis of MISTY1. In Sehun Kim, Moti Yung, and Hyung-Woo Lee, editors, *Information Security Applications — 8th International Workshop, WISA 2007, Revised Selected Papers*, volume 4867 of *Lecture Notes in Computer Science*, pages 215–226, Berlin, Heidelberg, 2007. Springer-Verlag.
38. Hidema Tanaka, Kazuyuki Hisamatsu, and Toshinobu Kaneko. Strength of MISTY1 without FL function for higher order differential attack. In Marc Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes — 13th International Symposium, AAECC-13 Proceedings*, volume 1719 of *Lecture Notes in Computer Science*, pages 221–230, Berlin, Heidelberg, New York, 1999. Springer-Verlag.
39. Yukiyasu Tsunoo, Teruo Saito, Hiroki Nakashima, and Maki Shigeri. Higher order differential attack on 6-round MISTY1. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, E92-A(1):3–10, 2009.
40. Yukiyasu Tsunoo, Teruo Saito, Maki Shigeri, and Takeshi Kawabata. Higher order differential attacks on reduced-round MISTY1. In Pil Joong Lee and Jung Hee Cheon, editors, *Information Security and Cryptology - ICISC 2008, 11th International Conference*, volume 5461 of *Lecture Notes in Computer Science*, pages 415–431. Springer-Verlag, Berlin, Heidelberg, New York, 2009.
41. Yukiyasu Tsunoo, Teruo Saito, Maki Shigeri, and Takeshi Kawabata. Security analysis of 7-round MISTY1 against higher order differential attacks. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, E93-A(1):144–152, 2010.
42. U.S. Department of Commerce, National Bureau of Standards. *Data Encryption Standard (Federal Information Processing Standards Publication 46)*, 1977.
43. U.S. Department of Commerce, National Institute of Standards and Technology. *NIST Special Publication 800-38, Recommendation for Block Cipher Modes of Operation*, 2001. (`http://csrc.nist.gov/publications/PubsSPs.html#SP-800-38-A`).
44. U.S. Department of Commerce, National Institute of Standards and Technology. *Specification for the ADVANCED ENCRYPTION STANDARD (AES) (Federal Information Processing Standards Publication 197)*, 2001. (`http://csrc.nist.gov/encryption/aes/index.html#fips`).
45. U.S. Department of Commerce, National Institute of Standards and Technology. *The Keyed-Hash Message Authentication Code (HMAC) (Federal Information Processing Standards Publication 198-1)*, 2008. (`http://csrc.nist.gov/publications/PubsFIPS.html#FIPS-198--1`).