Weak Keys of the Full MISTY1 Block Cipher for Related-Key Cryptanalysis*

Jiqiang Lu[1], Wun-She Yap[1,2], and Yongzhuang Wei[3,4]

[1] Institute for Infocomm Research,
Agency for Science, Technology and Research
1 Fusionopolis Way, #19-01 Connexis, Singapore 138632
lvjiqiang@hotmail.com, wsyap@i2r.a-star.edu.sg
[2] Faculty of Information Science and Technology, Multimedia University,
Melaka 75450, Malaysia
[3] Guilin University of Electronic Technology,
Guilin City, Guangxi Province 541004, P.R. China
[4] State Key Laboratory of Information Security, Institute of Software,
Chinese Academy of Sciences, Beijing 100190, P.R. China
walker_wei@msn.com

Abstract. The MISTY1 block cipher has a 64-bit block length, a 128-bit user key and a recommended number of 8 rounds. It is a Japanese CRYPTREC-recommended e-government cipher, an European NESSIE selected cipher, and an ISO international standard. Despite of considerable cryptanalytic efforts during the past fifteen years, there has been no published cryptanalytic attack on the full MISTY1 cipher algorithm. In this paper, we present related-key differential and related-key amplified boomerang attacks on the full MISTY1 under certain weak key assumptions: We describe $2^{103.57}$ weak keys and a related-key differential attack on the full MISTY1 with a data complexity of 2^{61} chosen ciphertexts and a time complexity of $2^{87.94}$ encryptions; and we also describe 2^{92} weak keys and a related-key amplified boomerang attack on the full MISTY1 with a data complexity of $2^{60.5}$ chosen plaintexts and a time complexity of $2^{80.18}$ encryptions. For the very first time, our results exhibit a cryptographic weakness in the full MISTY1 cipher (when used with the recommended 8 rounds), and show that the MISTY1 cipher is distinguishable from a random function and thus cannot be regarded to be an ideal cipher.

Key words: Block cipher, MISTY1, Differential cryptanalysis, Amplified boomerang attack, Related-key cryptanalysis, Weak key.

1 Introduction

The block cipher MISTY1 [33] was designed by Matsui and published in 1997. It has a 64-bit block length, a 128-bit user key, and a variable number of rounds; the officially recommended number of rounds is 8. We consider the version of MISTY1 that uses the recommended 8 rounds in this paper, which is also the most widely discussed version so far. MISTY1 has a Feistel structure with a total of ten key-dependent logical functions **FL** — two **FL** functions at the beginning plus two inserted after every two rounds. It became a CRYPTREC [10] e-government recommended cipher in 2002, and a NESSIE [35] selected block cipher in 2003, and was adopted as an ISO [15] international standard in 2005 and 2010.

MISTY1 has attracted extensive attention since its publication, and its security has been analysed against a wide range of cryptanalytic techniques [1,12,25,26,29,32,38–42]. In summary, the main previously published cryptanalytic results on MISTY1 are as follows. In 2008, Dunkelman and Keller [12] described impossible differential attacks [3, 23] on 6-round MISTY1 with FL functions and 7-round MISTY1 without FL functions. In the

* This work was partially supported by the Natural Science Foundation of China (No. 61100185).

Table 1. Main cryptanalytic results on MISTY1

#Rounds	FL	#Keys	Attack Type	Data	Time	Source
6 $(1-6)$	yes	2^{128}	Impossible differential	2^{51}CP	$2^{123.4}$Enc.	[12]
6 $(1-6)$	yes	2^{128}	Higer-order differential	$2^{53.7}$CP	$2^{64.4}$Enc.	[40,41]
6 $(3-8)$	yes	2^{128}	Integral	2^{32}CC	$2^{126.1}$Enc.	[38]
7 $(1-7)$	yes	2^{128}	Higer-order differential	$2^{54.1}$CP	$2^{120.7}$Enc.	[41,42]
$7^{\dagger}$ $(2-8)$	yes	2^{73}	Related-key amplified boomerang	2^{54}CP	$2^{55.3}$Enc.	[29]
$8^{\dagger}$ $(1-8)$	yes	2^{90}	Related-key amplified boomerang	2^{63}CP	2^{70}Enc.	[9]
$8^{\dagger}$ $(1-8)$	yes	$2^{105\ddagger}$	Related-key differential	2^{63}CC	$2^{86.6}$Enc.	[11]
full	yes	$2^{103.57}$	Related-key differential	2^{61}CC	$2^{87.94}$Enc.	Sect. 4
		2^{92}	Related-key amplified boomerang	$2^{60.5}$CP	$2^{80.18}$Enc.	Sect. 5

†: Exclude the first/last two FL functions, ‡: There is a flaw, see Section 5 for detail.

same year, Lee et al. [29] gave a related-key amplified boomerang attack [4, 14, 20] on 7-round MISTY1 with FL functions under a class of 2^{73} weak key[1], and Tsunoo et al. [41] presented a higher-order differential attack [22, 27] on 6 and 7-round MISTY1 with FL functions (without making a weak key assumption). In 2009, Sun and Lai [38] presented an integral attack on 6-round MISTY1 with FL functions, following Knudsen and Wagner's attack [24] on 5-round MISTY1. Most recently, following Lee et al.'s work, Chen and Dai [9] presented a 7-round related-key amplified boomerang distinguisher with probability 2^{-118} under a class of 2^{90} weak keys and gave a related-key amplified boomerang attack on the 8-round MISTY1 with only the first 8 FL functions; and in [11] they described a 7-round related-key differential characteristic with probability 2^{-60} under a class of 2^{105} weak keys and finally presented a related-key differential attack on the 8-round MISTY1 with only the last 8 FL functions. So far, there has been no published (non-generic) cryptanalytic attack on the full 8 rounds of MISTY1 yet.

Related-key cryptanalysis [2, 21] assumes that the attacker knows the relationship between one or more pairs of unknown keys; certain current real-world applications may allow for practical related-key attacks, for example, key-exchange protocols and hash functions [17]. Related-key differential cryptanalysis [17] takes advantage of how a specific difference in a pair of inputs of a cipher or function can affect a difference in the pair of outputs of the cipher or function, where the pair of outputs are obtained by encrypting the pair of inputs using two different keys with a specific difference. The related-key amplified boomerang attack [4, 14, 20] is a combination of related-key cryptanalysis and the amplified boomerang attack [18]; the amplified boomerang attack is a variant of the boomerang attack [43]. Remarkably, under certain weak key assumptions the related-key differential cryptanalysis technique was used in 2009 by Biryukov et al. [8] to obtain the the first cryptanalytic attack on the full version of the AES [36] block cipher with 256 key bits; and the related-key amplified boomerang attack technique was used to yield the first cryptanalytic attacks on the full versions of both AES with 192/256 key bits and KASUMI [16] — a variant of MISTY1, without using a weak key assumption, by Biham et al. [5, 13] and Biryukov et al. [7], respectively.

In this paper, for the very first time we show that the full MISTY1 cipher can be distinguished from a random function (in the related-key model): Building on Chen and Dai's work described in [9,11], we present related-key differential and amplified boomerang attacks on the full MISTY1 cipher under certain weak key assumptions. First, we spot some flaws in Dai and Chen's differential cryptanalytic results presented in [11], and find that there are only about $2^{102.57}$ weak keys in their weak key class such that their 7-round

[1] A weak key is defined as a key under which the concerned cipher is more vulnerable to be attacked.

related-key differential holds, but with probability 2^{-58}; and we observe that there are also a different class of $2^{102.57}$ weak keys under which there exists a 7-round related-key differential with probability 2^{-58}. We use the 7-round related-key differentials to break the full MISTY1. Finally, we find that under the class of 2^{90} weak keys described in [9], Chen and Dai's 7-round related-key amplified boomerang distinguisher actually has a probability of 2^{-116}, instead of 2^{-118}, which can be used to attack the full MISTY1; and similar results hold for three other classes of weak keys of the same size. Table 1 summarises our and previously published main cryptanalytic results on MISTY1, where CP and CC refer respectively to the numbers of chosen plaintexts and chosen ciphertexts, Enc. refers to the required number of encryption operations of the relevant version of MISTY1, and "yes" means "with FL functions".

The remainder of the paper is organised as follows. In the next section, we describe the notation, the MISTY1 cipher and the related-key amplified boomerang attack. In Sections 3 and 4 we review Chen and Dai's cryptanalytic results and give our differential and amplified boomerang cryptanalytic results on MISTY1, respectively. Section 5 concludes this paper.

2 Preliminaries

In this section we give the notation, and briefly describe the MISTY1 cipher and the related-key amplified boomerang attack.

2.1 Notation

The bits of a value are numbered from left to right, starting with 1. We use the following notation throughout this paper.

- $\oplus$ bitwise logical exclusive OR (XOR)
- $\cap$ bitwise logical AND
- $\cup$ bitwise logical OR
- $||$ bit string concatenation
- $\circ$ functional composition. When composing functions X and Y, $Y \circ X$ denotes the function obtained by first applying X and then Y

2.2 The MISTY1 Block Cipher

MISTY1 [33] employs a complex Feistel structure with a 64-bit block length and a 128-bit user key. It uses the following three functions **FL**, **FI**, **FO**, which are respectively depicted in Fig. 1-(a), Fig. 1-(b) and Fig. 1-(c) with their respective subkeys to be described below.

- **FL** : $\{0,1\}^{32} \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$ is a key-dependent linear function. If $X = (X_L||X_R)$ is a 32-bit block and $Y = (Y_1||Y_2)$ is a 32-bit block of two 16-bit words Y_1, Y_2, then

$$\mathbf{FL}(X, Y) = (X_L \oplus ((X_R \oplus (X_L \cap Y_1)) \cup Y_2), X_R \oplus (X_L \cap Y_1)).$$

- **FI** : $\{0,1\}^{16} \times \{0,1\}^{16} \rightarrow \{0,1\}^{16}$ is a non-linear function. If $X = (X_L(9 \text{ bits})||X_R(7 \text{ bits}))$ and $Y = (Y_1(7 \text{ bits})||Y_2(9 \text{ bits}))$ are 16-bit blocks, then $\mathbf{FI}(X, Y)$ is computed as follows, where $XL_0, XR_0, \cdots, XL_3, XR_3$ are 9 or 7-bit variables, S_9 is a 9×9-bit bijective S-box, S_7 is a 7×7-bit bijective S-box, the function Extnd extends from 7 bits to 9 bits by concatenating two zeros on the left side, and the function Trunc truncates two bits from the left side.

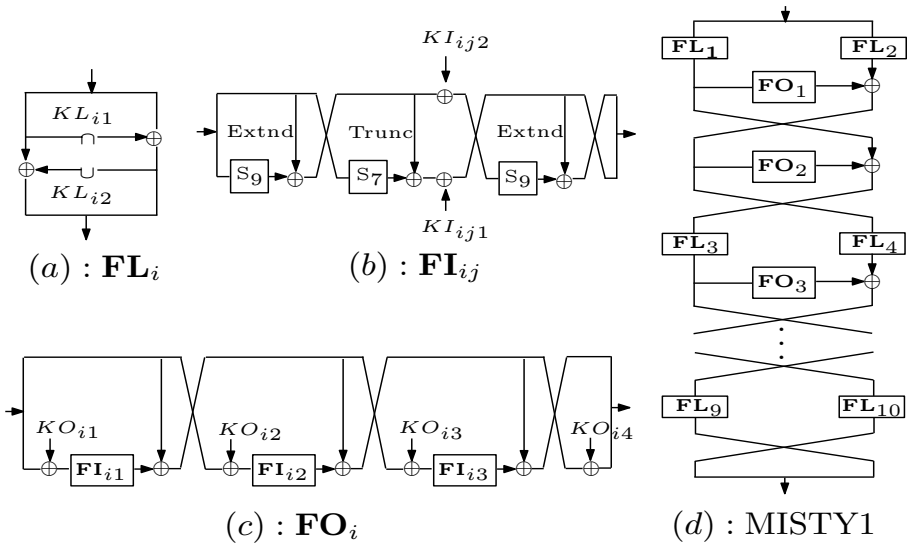


Fig. 1. MISTY1 and its components

1. $XL_0 = X_L, XR_0 = X_R$;
2. $XL_1 = XR_0$, $XR_1 = \mathrm{S}_9(XL_0) \oplus \mathrm{Extnd}(XR_0)$;
3. $XL_2 = XR_1 \oplus Y_2$, $XR_2 = \mathrm{S}_7(XL_1) \oplus \mathrm{Trunc}(XR_1) \oplus Y_1$;
4. $XL_3 = XR_2$, $XR_3 = \mathrm{S}_9(XL_2) \oplus \mathrm{Extnd}(XR_2)$;
5. $\mathbf{FI}(X, Y) = (XL_3||XR_3)$.

– $\mathbf{FO} : \{0,1\}^{32} \times \{0,1\}^{64} \times \{0,1\}^{48} \to \{0,1\}^{32}$ is a non-linear function. If $X = (X_L||X_R)$ is a 32-bit block, $Y = (Y_1||Y_2||Y_3||Y_4)$ is a 64-bit block of four 16-bit words Y_1, Y_2, Y_3, Y_4, and $Z = (Z_1||Z_2||Z_3)$ is a 48-bit block of three 16-bit words Z_1, Z_2, Z_3, then $\mathbf{FO}(X, Y, Z)$ is defined as follows, where $XL_0, XR_0, \cdots, XL_3, XR_3$ are 16-bit variables.

1. $XL_0 = X_L, XR_0 = X_R$;
2. For $j = 1, 2, 3$:
   $XL_j = XR_{j-1}$, $XR_j = \mathbf{FI}(XL_{j-1} \oplus Y_j, Z_j) \oplus XR_{j-1}$;
3. $\mathbf{FO}(X, Y, Z) = (XL_3 \oplus Y_4)||XR_3$.

MISTY1 uses a total of ten 32-bit subkeys $KL_1, KL_2, \cdots, KL_{10}$ for the **FL** functions, twenty-four 16-bit subkeys KI_{ij} for the **FI** functions, and thirty-two 16-bit subkeys KO_{il} for the **FO** functions, $(1 \leqslant i \leqslant 8, 1 \leqslant j \leqslant 3, 1 \leqslant l \leqslant 4)$, all derived from a 128-bit user key K. The key schedule is as follows.

1. Represent K as eight 16-bit words $K = (K_1, K_2, \cdots, K_8)$.
2. Generate a different set of eight 16-bit words $K'_1, K'_2, \cdots, K'_8$ by
$$K'_i = \mathbf{FI}(K_i, K_{i+1}), \text{ for } i = 1, 2, \cdots, 8,$$
where the subscript $i + 1$ is reduced by 8 when it is larger than 8, (similar for some subkeys in the following step).
3. The subkeys are as follows.
$$KO_{i1} = K_i, KO_{i2} = K_{i+2}, KO_{i3} = K_{i+7}, KO_{i4} = K_{i+4};$$
$$KI_{i1} = K'_{i+5}, KI_{i2} = K'_{i+1}, KI_{i3} = K'_{i+3};$$
$$KL_i = K_{\frac{i+1}{2}}||K'_{\frac{i+1}{2}+6}, \text{ for } i = 1, 3, 5, 7; \text{otherwise, } KL_i = K'_{\frac{i}{2}+2}||K_{\frac{i}{2}+4}.$$

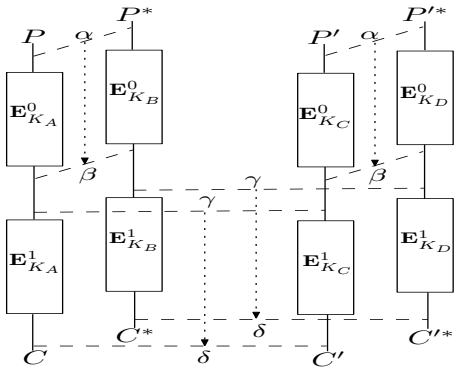


Fig. 2. A related-key amplified boomerang distinguisher

MISTY1 takes a 64-bit plaintext P as input, and has a variable number of rounds; the recommended number of rounds is 8. Its encryption procedure is as follows, where $L_0, R_0, \cdots, L_i, R_i$ are 32-bit variables, $KO_j = (KO_{j1}||KO_{j2}||KO_{j3}||KO_{j4})$, and $KI_j = (KI_{j1}||KI_{j2}||KI_{j3})$, $(j = 1, 2, \cdots, 8)$; see Fig. 1-(d).

1. $(L_0||R_0) = (P_L||P_R)$.
2. For $i = 1, 3, 5, 7$:
   $R_i = \mathbf{FL}(L_{i-1}, KL_i)$, $L_i = \mathbf{FL}(R_{i-1}, KL_{i+1}) \oplus \mathbf{FO}(R_i, KO_i, KI_i)$;
   $R_{i+1} = L_i$, $L_{i+1} = R_i \oplus \mathbf{FO}(L_i, KO_{i+1}, KI_{i+1})$.
3. Ciphertext $C = \mathbf{FL}(R_8, KL_{10})||\mathbf{FL}(L_8, KL_9)$.

We refer to the 8 rounds in the above description as Rounds $1, 2, \cdots, 8$, respectively.

2.3 The Related-Key Amplified Boomerang Attack

A related-key amplified boomerang attack is based on a related-key amplified boomerang distinguisher, which treats a block cipher $\mathbf{E} : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}^n$ as a cascade of two sub-ciphers $\mathbf{E} = \mathbf{E}^1 \circ \mathbf{E}^0$ and requires that there exists a related-key differential $\Delta\alpha \to \Delta\beta$ with probability p for $\mathbf{E}^0$: $\Pr_{X\in\{0,1\}^n}[\mathbf{E}^0_{K_A}(X) \oplus \mathbf{E}^0_{K_B}(X \oplus \alpha) = \beta] = \Pr_{X\in\{0,1\}^n}[\mathbf{E}^0_{K_C}(X) \oplus \mathbf{E}^0_{K_D}(X \oplus \alpha) = \beta] = p$, and a related-key differential $\Delta\gamma \to \Delta\delta$ with probability q for $\mathbf{E}^1$: $\Pr_{X\in\{0,1\}^n}[\mathbf{E}^1_{K_A}(X) \oplus \mathbf{E}^1_{K_C}(X \oplus \gamma) = \delta] = \Pr_{X\in\{0,1\}^n}[\mathbf{E}^1_{K_B}(X) \oplus \mathbf{E}^1_{K_D}(X \oplus \gamma) = \delta] = q$, where the four unknown user keys K_A, K_B, K_C, K_D satisfy $K_B = K_A \oplus \Delta K_0$, $K_C = K_A \oplus \Delta K_1$ and $K_D = K_C \oplus \Delta K_0$, with ΔK_0 and ΔK_1 being two known differences. See Fig. 2.

A quartet consisting of two randomly chosen pairs of plaintexts $(P, P^* = P \oplus \alpha)$ and $(P', P'^* = P' \oplus \alpha)$ satisfies $\mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_B}(P^*) = \mathbf{E}^0_{K_C}(P') \oplus \mathbf{E}^0_{K_D}(P'^*) = \beta$ with probability p^2. Assuming that the intermediate values after $\mathbf{E}^0$ distribute uniformly over all possible values, we get $\mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_C}(P') = \gamma$ with probability 2^{-n}. Once this occurs, then $\mathbf{E}^0_{K_B}(P^*) \oplus \mathbf{E}^0_{K_D}(P'^*) = \gamma$ holds with probability 1, for $\mathbf{E}^0_{K_B}(P^*) \oplus \mathbf{E}^0_{K_D}(P'^*) = (\mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_B}(P^*)) \oplus (\mathbf{E}^0_{K_C}(P') \oplus \mathbf{E}^0_{K_D}(P'^*)) \oplus (\mathbf{E}^0_{K_A}(P) \oplus \mathbf{E}^0_{K_C}(P')) = \beta \oplus \beta \oplus \gamma = \gamma$. As a result, the probability that the quartet satisfies $\mathbf{E}_{K_A}(P) \oplus \mathbf{E}_{K_C}(P') = \mathbf{E}_{K_B}(P^*) \oplus \mathbf{E}_{K_D}(P'^*) = \delta$ is expected to be about $(\Pr(\Delta\alpha \to \Delta\beta))^2 \cdot 2^{-n} \cdot (\Pr(\Delta\gamma \to \Delta\delta))^2 = 2^{-n} \cdot p^2 \cdot q^2$; while for a random cipher, the probability is about $2^{-n\times 2} = 2^{-2n}$.

Therefore, if $p \cdot q > 2^{-n/2}$, the related-key amplified boomerang distinguisher can distinguish between $\mathbf{E}$ and a random cipher given a sufficient number of plaintext pairs.

Note that in addition to those assumptions [28] used in differential cryptanalysis [6], the related-key amplified boomerang attack requires another assumption about independence, and we refer the reader to [19, 34] for a more formal discussion of the assumptions as well as the attack technique. These assumptions mean that, in some cases, the probability of a related-key amplified boomerang distinguisher may be overestimated or underestimated, and so is the success probability of the attack. Anyway, it seems reasonable to take the worst case assumption from the point of the user of a cipher. An application of such an attack was given by Dunkelman et al. [13] to break the full KASUMI cipher with a practical complexity, and its validity was experimentally verified.

3 $2^{103.57}$ Weak Keys of the Full MISTY1 for a Related-Key Differential Attack

In this section, we first review Dai and Chen's class of 2^{105} weak keys and their 7-round related-key differential characteristic with probability 2^{-60} under the class of weak keys. Then, we show that there are actually only $2^{102.57}$ weak keys such that the 7-round related-key differential characteristic holds, and it has a probability of 2^{-58}. Next we devise a related-key differential attack on the full MISTY1 when the user key used is a weak key from the class of $2^{102.57}$ weak keys. At last we describe another class of $2^{102.57}$ weak keys under which similar results hold.

3.1 A Class of 2^{105} Weak Keys due to Dai and Chen

First define three constants which will be used subsequently: A 7-bit constant $a = 0010000$, a 16-bit constant $b = 0010000000010000$, and another 16-bit constant $c = 0010000000000000$, all in binary notation. Observe that $b = (a||0^2||a)$ and $c = (a||0^9)$.

Let K_A, K_B be two 128-bit user keys defined as follows:

$$K_A = (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8),$$
$$K_B = (K_1, K_2, K_3, K_4, K_5, K_6^*, K_7, K_8).$$

By the key schedule of MISTY1 we can get the corresponding eight 16-bit words for K_A, K_B, which are denoted as follows.

$$K'_A = (K'_1, K'_2, K'_3, K'_4, K'_5, K'_6, K'_7, K'_8),$$
$$K'_B = (K'_1, K'_2, K'_3, K'_4, K'^*_5, K'^*_6, K'_7, K'_8).$$

Then, the class of weak keys is defined to be the set of all possible values for (K_A, K_B) that satisfy the following 10 conditions, where $K_{6,12}$ denotes the 12-th bit of K_6, and similar for $K_{7,3}, K_{7,12}, K_{8,3}, K'_{4,3}, K'_{4,12}, K'_{7,3}$.

$$K_6 \oplus K_6^* = c; \tag{1}$$
$$K'_5 \oplus K'^*_5 = b; \tag{2}$$
$$K'_6 \oplus K'^*_6 = c; \tag{3}$$
$$K_{6,12} = 0; \tag{4}$$
$$K_{7,3} = 1; \tag{5}$$
$$K_{7,12} = 0; \tag{6}$$
$$K_{8,3} = 1; \tag{7}$$
$$K'_{4,3} = 1; \tag{8}$$
$$K'_{4,12} = 1; \tag{9}$$
$$K'_{7,3} = 0. \tag{10}$$

Now let us analyse the number of the weak keys. First observe that when Condition (1) holds, then Condition (2) holds with certainty.

Note that $K'_4 = \mathbf{FI}(K_4, K_5), K'_6 = \mathbf{FI}(K_6, K_7)$, $K'^*_6 = \mathbf{FI}(K^*_6, K_7), K'_7 = \mathbf{FI}(K_7, K_8)$. By performing a computer search, we get

$$|\{(K_4, K_5)|\text{Conditions (8) and (9)}\}| = 2^{30};$$
$$|\{(K_6, K_7, K_8)|\text{Conditions (1), (3), (4), (5), (6), (7) and (10)}\}| = 2^{27}.$$

Therefore, Dai and Chen [11] concluded that there are a total of 2^{105} possible values for K_A satisfying the above 10 conditions, and thus there are 2^{105} weak keys.

3.2 Dai and Chen's 7-Round Related-Key Differential Characteristic

Under the class of 2^{105} weak keys (K_A, K_B) described in Section 3.1, Dai and Chen described the following 7-round related-key differential characteristic $\Delta\alpha \to \Delta\beta$: $(b||0^{32}||c) \to (0^{32}||c||0^{16})$ with probability 2^{-60} for Rounds 2–8, where 0^{32} represents a binary string of 32 zeros, and so on. In Fig. 5 in Appendix A we illustrate the related-key differential characteristic in detail, where $R_{4,3}$ denotes the 3-rd bit of R_4 (the right half of the output of Round 4), and $R_{4,12}$ denotes the 12-th bit of R_4.

As a result, Dai and Chen presented a related-key differential attack on 8-round MISTY1 without the first two FL functions, by conducting a key recovery on $\mathbf{FO}_1$ in a way similar to the early abort technique for impossible differential cryptanalysis introduced in [32]

3.3 A Corrected Class of Weak Keys and Improved 7-Round Related-Key Differential

We first focus on the $\mathbf{FI}_{73}$ function in Dai and Chen's 7-round related-key differential characteristic, where the probability is 2^{-16}. Observe that $KI_{73} = K'_2$. Dai and Chen assumed a random distribution when calculating the probability of the differential $\Delta c \to \Delta c$ for $\mathbf{FI}_{73}$, and thus obtained a probability value of 2^{-16}, (An alternative explanation is to consider the two S_9 S-boxes, each having a probability value of 2^{-8}). However, intuitively we should make sure that a weak key (K_A, K_B) should also satisfy the condition that the differential $\Delta c \to \Delta c$ is a possible differential for $\mathbf{FI}_{73}$; otherwise, the differential $\Delta c \to \Delta c$ would have a zero probability, and the 7-round differential characteristic would be flawed. Thus, we should put the following additional condition when defining a set of weak keys:

$$\Pr_{\mathbf{FI}(\cdot, K'_2)}(\Delta c \to \Delta c) > 0. \tag{11}$$

Motivated by this, we perform a computer programming to test the number of K'_2 satisfying Condition (11), and we find that the number of K'_2 satisfying Condition (11) is equal to 2^{15}. As a consequence, we know that the number of (K_2, K_3) satisfying Condition (11) is 2^{31}, thus not all 2^{32} possible values for (K_2, K_3) meet Condition (11), so this is really a flaw in Dai and Chen's results. Furthermore, we find that for each satisfying K'_2, there are exactly two pairs of inputs to $\mathbf{FI}_{73}$ which follow the differential $\Delta c \to \Delta c$, that is to say, the probability $\Pr_{\mathbf{FI}(\cdot, K'_2)}(\Delta c \to \Delta c) = 2^{-15}$, twice as large as the probability value 2^{-16} used by Dai and Chen.

Next we focus on the $\mathbf{FI}_{21}$ function in Dai and Chen's 7-round related-key differential characteristic, where the probability is 2^{-16}, and $KI_{21} = K'_7$. Likewise, we should make sure that a weak key (K_A, K_B) should also satisfy the condition that the differential $\Delta b \to \Delta c$ is a possible differential for $\mathbf{FI}_{21}$; otherwise, the differential $\Delta b \to \Delta c$ would have

a zero probability, and the 7-round differential characteristic would be flawed. Similarly, we should put another condition when defining a set of weak keys:

$$\Pr_{\mathbf{FI}(\cdot,K_7')}(\Delta b \to \Delta c) > 0. \tag{12}$$

By performing a computer programming we find that the number of K_7' satisfying Condition (12) is $24320 \approx 2^{14.57}$; on the other hand, the number of K_7' satisfying Conditions (1), (3), (4), (5), (6), (7) and (10) is 2^{15} (and for each satisfying K_7' there are 2^{12} possible values for (K_6', K_8)), so not all the possible values of K_7' satisfying Conditions (1), (3), (4), (5), (6), (7) and (10) satisfy Condition (12). After a further test, we get that the number of K_7' satisfying Conditions (1), (3), (4), (5), (6), (7), (10) and (12) is $12160 \approx 2^{13.57}$. As a result, we know that the number of (K_6, K_7, K_8) satisfying Conditions (1), (3), (4), (5), (6), (7), (10) and (12) is $2^{13.57} \times 2^{12} = 2^{25.57}$, so this is another flaw in Dai and Chen's results. Furthermore, we have that $\Pr_{\mathbf{FI}(\cdot,K_7')}(\Delta b \to \Delta c)$ is 2^{-15} for each of 9600 satisfying values for K_7', 2^{-14} for each of 2432 satisfying values for K_7', and $\frac{6}{2^{16}} \approx 2^{-13.42}$ for each of 128 satisfying values for K_7'.

In summary, there are approximately $2^{102.57}$ weak keys satisfying Conditions (1)–(12), and the 7-round related-key differential $\Delta\alpha \to \Delta\beta$ has a minimum probability of 2^{-58} under a weak key (K_A, K_B). In particular, we have the following result.

Proposition 1. *In the class of $2^{102.57}$ weak keys satisfying Conditions (1)–(12),*

1. *there are 2^{16} possible values for K_1, 2^{16} possible values for K_3, and 2^{16} possible values for K_5;*
2. *there are $2^{25.57}$ possible values for (K_6, K_7, K_8); in particular there are a total of $2^{13.57}$ possible values for K_7', and for every possible value of K_7' there are 2^{12} possible values for (K_6', K_8);*
3. *there are a total of 2^8 possible values for $K_{2,8-16}'$, 2^{16} possible values for K_3', and 2^8 possible values for $K_{4,8-16}'$, where $K_{2,8-16}'$ denotes bits $(8, \cdots, 16)$ of K_2' and $K_{4,8-16}'$ denotes bits $(8, \cdots, 16)$ of K_4';*
4. *$\Pr_{\mathbf{FI}(\cdot,\forall K_7')}(\Delta b \to \Delta c) \geq 2^{-15}, \Pr_{\mathbf{FI}(\cdot,\forall K_2')}(\Delta c \to \Delta c) = 2^{-15}$.*

3.4 Attacking the Full MISTY1 under the Class of $2^{102.57}$ Weak Keys

The 7-round related-key differential with probability 2^{-58} can be used to conduct a related-key differential attack on the full MISTY1 when the user key used is a weak key from the class of $2^{102.57}$ weak keys.

Preliminary Results. We first concentrate on the propagation of the input difference $\alpha(= b||0^{32}||c)$ of the 7-round differential through the preceding Round 1, including the $\mathbf{FL}_1$ and $\mathbf{FL}_2$ functions, under (K_A, K_B); see Fig. 3.

Under (K_A, K_B), by the key schedule of MISTY1 we have

$$\begin{aligned}
&\Delta KO_{11} = \Delta K_1 = 0, \Delta KO_{12} = \Delta K_3 = 0,\\
&\Delta KO_{13} = \Delta K_8 = 0, \Delta KO_{14} = \Delta K_5 = 0,\\
&\Delta KI_{11} = \Delta K_6' = c, \Delta KI_{12} = \Delta K_2' = 0, \Delta KI_{13} = \Delta K_4' = 0,\\
&\Delta KL_1 = \Delta(K_1||K_7') = 0, \Delta KL_2 = \Delta(K_3'||K_5) = 0.
\end{aligned}$$

As depicted in Fig. 3, the right half of α is $(0^{16}||c)$, so the $\mathbf{FI}_{11}$ function has a zero input difference; however since $\Delta KO_{11} = 0$ and $\Delta KI_{11} = c$, the output difference of $\mathbf{FI}_{11}$ is b with probability 1. The input difference of the $\mathbf{FI}_{12}$ function is c, thus the first S_9 function

in $\mathbf{FI}_{12}$ has an input difference $a||0^2$, and we assume its output difference is $A \in \{0,1\}^9$; the S_7 function in $\mathbf{FI}_{12}$ has a zero input and output difference. The second S_9 function in $\mathbf{FI}_{12}$ has an input difference A, and we assume its output difference is $B \in \{0,1\}^9$. As a result, the $\mathbf{FI}_{12}$ function has an output difference $X = (\text{Trunc}(A)||(B \oplus (0^2||\text{Trunc}(A))))$. A simple computer programming reveals that $\text{Trunc}(A)$ can take all 2^7 possible values, and thus we assume that X can take all values in $\{0,1\}^{16}$.

Since the input difference of the $\mathbf{FI}_{13}$ function is $0^9||a$, the first S_9 function in $\mathbf{FI}_{13}$ has a zero input difference. The S_7 function in $\mathbf{FI}_{13}$ has an input difference a, and we assume its output difference is $D \in \{0,1\}^7$, which can take only 2^6 possible values. The second S_9 function in $\mathbf{FI}_{13}$ has an input difference $0^2||a$, and we assume its output difference is $E \in \{0,1\}^9$. Consequently, the $\mathbf{FI}_{13}$ function has an output difference $Y = ((a \oplus D)||(E \oplus (0^2||(a \oplus D))))$, and it can take about 2^{15} values in $\{0,1\}^{16}$; we denote the set of 2^{15} values by $\mathcal{S}_d$.

The $\mathbf{FL}_1$ function has an output difference $(0^{16}||c)$, so its input difference can only be of the form $\overbrace{00?0000000000000}^{32\ bits}||00?0000000000000$, which will be denoted by $\eta = (\eta_L, \eta_R)$ in the following descriptions, where the question marker "?" represents an indeterminate bit; and when the first question marker takes a zero value, the second question marker can take only 1, that is η has only three possible values, (The specific form depends on the values of the two subkey bits $K_{1,3}$ and $K'_{7,3}$). The $\mathbf{FL}_2$ function has an output difference $(X \oplus c)||(X \oplus Y \oplus (0^9||a))$, so its input difference is indeterminate, denoted by "?" in Fig. 3.

From the above analysis we can see that the subkeys KI_{121} and KI_{131} do not affect the values of X and Y, and thus they are not required when checking whether a candidate plaintext pair generates the input difference $\alpha = (b||0^{32}||c)$ of the 7-round related-key differential. Further, as $K'_3 = \mathbf{FI}(K_3, K_4)$, $K'_4 = \mathbf{FI}(K_4, K_5)$, $K'_6 = \mathbf{FI}(K_6, K_7)$ and $K'_7 = \mathbf{FI}(K_7, K_8)$, we have the following result.

Proposition 2. *Only the subkeys $(K_1, K'_{2,8-16}, K_3, K_4, K_5, K_6, K_7, K_8)$ are required when checking whether a candidate plaintext pair produces the input difference $\alpha = (b||0^{32}||c)$ of the 7-round related-key differential.*

Attack Procedure. We first precompute two hash tables $\mathcal{T}_1$ and $\mathcal{T}_2$. Observe that from the left halves of a pair of plaintexts we only need $(K_1, K_3, K'_{2,8-16})$ when computing the output difference X of the $\mathbf{FI}_{12}$ function and only need $(K_1, K'_6, K'_7, K_8, K'_{4,8-16})$ when computing the output difference Y of the $\mathbf{FI}_{13}$ function. To generate $\mathcal{T}_1$ and $\mathcal{T}_2$, we do the following procedure under every 32-bit value $x = (x_L||x_R)$.

1. For every possible K_1:
   (a) Compute $Z = (x_L \cap K_1) \oplus ((x_L \oplus \eta_L) \cap K_1) \oplus \eta_R$, and proceed to the following steps only when $Z = c$.
   (b) For every possible $(K_3, K'_{2,8-16})$, compute the output difference of $\mathbf{FI}_{12}$ as X.
2. Store all satisfying $(K_1, K_3, K'_{2,8-16})$ into Table $\mathcal{T}_1$ indexed by (x, η, X).
3. For every possible K'_7:
   (a) Compute $W = \eta_L \oplus (((x_L \cap K_1) \oplus x_R) \cup K'_7) \oplus (((x_L \cap K_1) \oplus x_R \oplus c) \cup K'_7)$, and proceed to the following steps only when $W = 0$.
   (b) For every possible $(K'_6, K_8, K'_{4,8-16})$, compute the output difference of $\mathbf{FI}_{13}$ as Y.
4. Store the values of (K_6, K_7, K_8) corresponding to all satisfying (K'_6, K'_7, K_8) into Table $\mathcal{T}_2$ indexed by $(x, \eta, Y, K_1, K'_{4,8-16})$.

There are 2^{16} possible values for K_1, 2^{16} possible values for K_3, 2^8 possible values for $K'_{2,8-16}$, and 3 possible values for η. For a fixed (x, η, X), on average there are $2^{16} \times 2^{-1} \times$

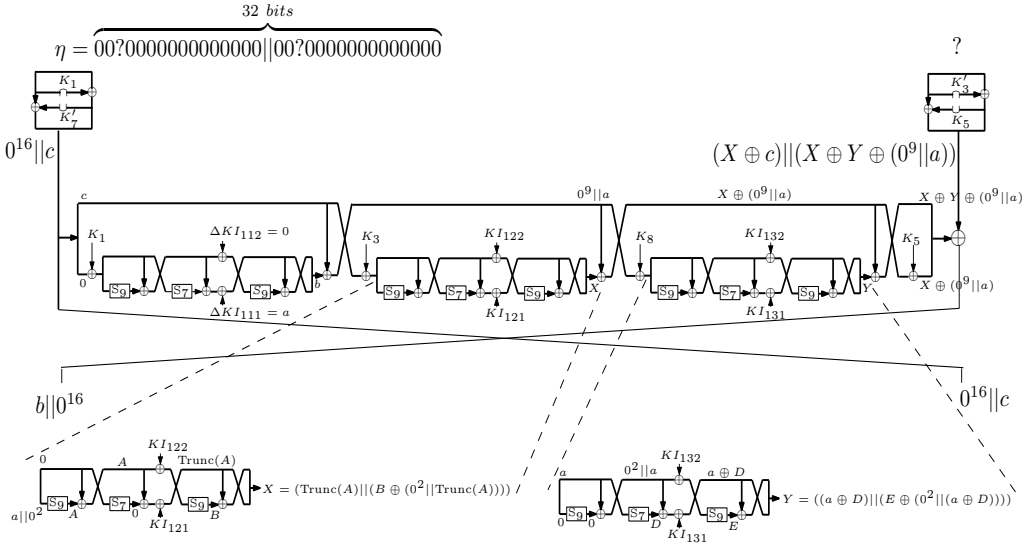


Fig. 3. Propagation of α through the inverse of Round 1 with $\mathbf{FL}_1$ and $\mathbf{FL}_2$

$2^{16} \times 2^8 \times 2^{-16} = 2^{23}$ satisfying values for $(K_1, K_3, K'_{2,8-16})$ in $\mathcal{T}_1$. The precomputation for $\mathcal{T}_1$ takes about $2^{32} \times 3 \times 2^{16} \times 2^{16} \times 2^8 \approx 2^{73.59}$ **FI** computations, and $\mathcal{T}_1$ requires a memory of about $2^{24} \times 2^{32} \times 3 \times 2^{16} \times \frac{16+16+8}{8} \approx 2^{75.91}$ bytes. There are $2^{13.57}$ possible values for K'_7, 2^{12} possible values for (K'_6, K_8), 2^8 possible values for $K'_{4,8-16}$, and 2^{15} possible values for Y. For a fixed $(x, \eta, Y, K_1, K'_{4,8-16})$, on average there are $2^{13.57} \times 2^{-1} \times 2^{12} \times 2^{-15} = 2^{9.57}$ satisfying values for (K'_6, K'_7, K_8) in $\mathcal{T}_2$. The precomputation for $\mathcal{T}_2$ takes about $2^{32} \times 3 \times 2^{16} \times 2^{13.57} \times 2^{12} \times 2^8 \times 2 \approx 2^{84.16}$ **FI** computations, and $\mathcal{T}_2$ requires a memory of about $2^{9.57} \times 2^{32} \times 3 \times 2^{15} \times 2^{16} \times 2^8 \times 6 \approx 2^{84.74}$ bytes. Note that we can use several tricks to optimise the procedure to reduce the computational complexity for generating the two tables, but anyway it is negligible compared with the computational complexity of the following online attack procedure.

We devise the following attack procedure to break the full MISTY1 when a weak key is used.

1. Initialize zero to an array of $2^{95.57}$ counters corresponding to all the $2^{95.57}$ possible values for $(K_1, K'_{2,8-16}, K_3, K_4, K_5, K_6, K_7, K_8)$.
2. Choose 2^{60} ciphertext pairs $(C, C^* = C \oplus (0^{32}||c||0^{16}))$. In a chosen-ciphertext attack scenario, obtain the plaintexts for the ciphertexts C, C^* under K_A, K_B, respectively, and we denote by $P = (PL_L||PL_R, PR_L||PR_R)$ the plaintext for ciphertext C encrypted under K_A, by $P^* = (PL^*_L||PL^*_R, PR^*_L||PR^*_R)$ the plaintext for ciphertext C^* encrypted under K_B.
3. Check whether a plaintext pair (P, P^*) meets the condition $(PL_L||PL_R) \oplus (PL^*_L||PL^*_R) = \eta$ by first checking the 30 bit positions with a zero difference and then checking the remaining two bit positions. Keep only the satisfying plaintext pairs.
4. For every remaining plaintext pair (P, P^*), do the following sub-steps.
   (a) Guess a possible value for (K'_3, K_5), and compute (X, Y) such that

$$(X \oplus c)||(X \oplus Y \oplus (0^9||a)) = \mathbf{FL}(PR_L||PR_R, K'_3||K_5) \oplus \mathbf{FL}(PR^*_L||PR^*_R, K'_3||K_5).$$

   Execute the next steps only if $Y \in \mathcal{S}_d$; otherwise, repeat this step with another subkey guess.

(b) Access Table $\mathcal{T}_1$ at entry $(PL_L||PL_R, \eta, X)$ to get the satisfying values for $(K_1, K_3, K'_{2,8-16})$.

(c) For each satisfying value for $(K_1, K_3, K'_{2,8-16})$, retrieve K_4 from the equation $K'_3 = \mathbf{FI}(K_3, K_4)$, compute $K'_4 = \mathbf{FI}(K_4, K_5)$, and access Table $\mathcal{T}_2$ at entry $(PL_L||PL_R, \eta, Y, K_1, K'_{4,8-16})$ to get the satisfying values for (K_6, K_7, K_8).

(d) Increase 1 to each of the counters corresponding to the obtained values for $(K_1, K'_{2,8-16}, K_3, K_4, K_5, K_6, K_7, K_8)$.

5. For a value of $(K_1, K'_{2,8-16}, K_3, K_4, K_5, K_6, K_7, K_8)$ whose counter number is equal to or larger than 3, exhaustively search the remaining 7 key bits with two known plaintext-ciphertext pairs. If a value of $(K_1, K_2, \cdots, K_8)$ is suggested, output it as the user key of the full MISTY1.

Attack Complexity. The attack requires $2^{60} \times 2 = 2^{61}$ chosen ciphertexts. In Step 3, only $2^{60} \times 2^{-30} \times \frac{3}{4} \approx 2^{29.58}$ palintext pairs are expected to satisfy the condition, and it takes about 2^{60} memory accesses to obtain the satisfying palintext pairs. Step 4(a) has a time complexity of about $2^{29.58} \times 2^{16} \times 2^{16} \times 2 = 2^{62.58}$ **FL** computations. In Step 4(b), for a plaintext pair and a possible value for (K'_3, K_5), on average we obtain 2^{23} possible values for $(K_1, K_3, K'_{2,8-16})$, as discussed in the procomputation phase; due to the filtering condition in Step 4(a), Step 4(b) has a time complexity of about $2^{29.58} \times \frac{2^{15}}{2^{16}} \times 2^{32} \times 2^{23} = 2^{83.58}$ memory accesses (if conducted on a 64-bit computer). In Step 4(c), for a plaintext pair and a possible value for $(K_1, K_3, K_5, K'_{2,8-16}, K'_3)$, on average we obtain $2^{9.57}$ possible values for (K_6, K_7, K_8), (as discussed in the procomputation phase), thus Step 4(c) has a time complexity of about $2^{28.58} \times 2^{32} \times 2^{23} \times 2^{9.57} = 2^{93.15}$ memory accesses. Step 4(d) has a time complexity of about $2^{93.15} \times 2 = 2^{94.15}$ memory accesses, where the factor "2" represents that a single operation requires two memory accesses when conducted on a 64-bit computer.

The probability that the counter for a wrong $(K_1, K'_{2,8-16}, K_3, K_4, K_5, K_6, K_7, K_8)$ has a number equal to or larger than 3 is approximately $\sum_{i=3}^{2^{60}} [\binom{2^{60}}{i} \cdot (2^{-64})^i \cdot (1-2^{-64})^{2^{60}-i}] \approx 2^{-14.67}$. Thus, it is expected that there are a total of $2^{95.57} \times 2^{-14.67} = 2^{80.9}$ wrong values of $(K_1, K'_{2,8-16}, K_3, K_4, K_5, K_6, K_7, K_8)$ whose counters have a number equal to or larger than 3. Thus it requires $2^{80.9} \times 2^7 + 2^{80.9} \times 2^7 \times 2^{-64} \approx 2^{87.9}$ trial encryptions to check them in Step 5. In Step 5, a wrong value of $(K_1, K_2, \cdots, K_8)$ is suggested with probability $2^{-64\times 2} = 2^{-128}$, so the number of suggested values for $(K_1, K_2, \cdots, K_8)$ is expected to be $2^{87.9} \times 2^{-128} = 2^{-40.1}$, which is rather low. Thus, the time complexity of the attack is dominated by Steps 4(c), 4(d) and 5. On a general 64-bit personal computer (with Intel Xeon Processor E5630 running on Ubuntu 10.04), we check that a full encryption using an optimised MISTY1 implementation twice as fast as the one given in [37] by the cipher designer equals about 2^{12} memory accesses in terms of time. Therefore, the attack has a total time complexity of about $2^{93.15} \times 2^{-12} + 2^{94.15} \times 2^{-12} + 2^{87.9} \approx 2^{87.94}$ MISTY1 encryptions.

The counter for the correct key has an expected number of $2^{60} \times 2^{-58} = 4$, and the probability that the counter for the correct key has a number equal to or larger than 3 is approximately $\sum_{i=3}^{2^{60}} [\binom{2^{60}}{i} \cdot (2^{-58})^i \cdot (1-2^{-58})^{2^{60}-i}] \approx 0.76$. Therefore, the related-key differential attack has a success probability of 76%.

The memory complexity of the attack is dominated by the space for the array of $2^{95.57}$ counters, which is $2^{95.57} \times \frac{95.57}{8} \approx 2^{99.2}$ bytes. It is worthy to note that there exist time-memory tradeoff versions to the above attack.

3.5 Another Class of $2^{102.57}$ Weak Keys

In the above sub-sections we have described a class of $2^{102.57}$ weak keys and a related-key differential attack on the full MISTY1 under a weak key. However, we observe that there exists another class of $2^{102.57}$ weak keys under which similar results hold. The new weak key class is obtained by setting $K'_{7,3} = 1$, which is further classified into two sub-classes by the possible values of the subkey bit $K_{1,3}$. This will affect only the $\mathbf{FL}_{10}$ function in the 7-round related-key differential, but the output difference of $\mathbf{FL}_{10}$ will be fixed once $K_{1,3}$ is given, that is, the right half of the output difference of the resulting 7-round related-key differential will be $c||c$ when $K_{1,3} = 1$, and $0^{16}||c$ when $K_{1,3} = 0$. Thus, by choosing a number of ciphertext pairs with a corresponding difference we can conduct a similar attack on the full MISTY1 under every sub-class of weak keys. In total, we have $2^{103.57}$ weak keys under which a related-key differential attack can break the full MISTY1.

4 2^{92} Weak Keys of the Full MISTY1 for a Related-Key Amplified Boomerang Attack

In this section, we first review Chen and Dai's class of 2^{90} weak keys and their 7-round related-key amplified boomerang distinguisher with probability 2^{-118}. Next, we describe a slight improvement to Chen and Dai's 7-round related-key amplified boomerang distinguisher, which has a probability of 2^{-116}, and then present a related-key amplified boomerang attack on the full MISTY1 under the class of 2^{90} weak keys. Finally, we describe three other classes of 2^{90} weak keys under which there exist similar results.

4.1 A Class of 2^{90} Weak Keys due to Chen and Dai

First define the same three constants a, b, c as used in Section 3.1, that is a 7-bit constant $a = 0010000$, a 16-bit constant $b = 0010000000010000$, and another 16-bit constant $c = 0010000000000000$, all in binary notation.

Let K_A, K_B, K_C, K_D be four 128-bit user keys defined as follows:

$$\begin{aligned}
K_A &= (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8),\\
K_B &= (K_1, K_2^*, K_3, K_4, K_5, K_6, K_7, K_8),\\
K_C &= (K_1, K_2, K_3, K_4, K_5, K_6^*, K_7, K_8),\\
K_D &= (K_1, K_2^*, K_3, K_4, K_5, K_6^*, K_7, K_8).
\end{aligned}$$

By the key schedule of MISTY1 we can get the corresponding eight 16-bit words for K_A, K_B, K_C, K_D, which are denoted as follows.

$$\begin{aligned}
K'_A &= (K'_1, K'_2, K'_3, K'_4, K'_5, K'_6, K'_7, K'_8),\\
K'_B &= (K'^*_1, K'^*_2, K'_3, K'_4, K'_5, K'_6, K'_7, K'_8),\\
K'_C &= (K'_1, K'_2, K'_3, K'_4, K'^*_5, K'^*_6, K'_7, K'_8),\\
K'_D &= (K'^*_1, K'^*_2, K'_3, K'_4, K'^*_5, K'^*_6, K'_7, K'_8).
\end{aligned}$$

Then, the class of weak keys is defined to be the set of all possible values for (K_A, K_B, K_C, K_D) that satisfy the following 12 conditions, where $K_{5,3}$ denotes the 3-rd bit of K_5, and similar for $K_{5,12}, K'_{4,3}, K_{7,3}, K_{7,12}, K_{8,3}$.

$$K_2 \oplus K_2^* = c; \tag{13}$$

$$K_6 \oplus K_6^* = c; \tag{14}$$

$$K'_1 \oplus K'^*_1 = b; \tag{15}$$
$$K'_5 \oplus K'^*_5 = b; \tag{16}$$
$$K'_2 \oplus K'^*_2 = c; \tag{17}$$
$$K'_6 \oplus K'^*_6 = c; \tag{18}$$
$$K_{5,3} = 1; \tag{19}$$
$$K_{5,12} = 0; \tag{20}$$
$$K'_{4,3} = 0; \tag{21}$$
$$K_{7,3} = 1; \tag{22}$$
$$K_{7,12} = 0; \tag{23}$$
$$K_{8,3} = 0. \tag{24}$$

Now let us analyse the number of the weak keys. First observe that when Condition (13) holds, then Condition (15) holds with certainty; when Condition (14) holds, Condition (16) holds with certainty.

Note that $K'_2 = \mathbf{FI}(K_2, K_3), K'^*_2 = \mathbf{FI}(K^*_2, K_3), K'_4 = \mathbf{FI}(K_4, K_5), K'_6 = \mathbf{FI}(K_6, K_7)$, $K'^*_6 = \mathbf{FI}(K^*_6, K_7)$. By performing a computer search, we get

$$|\{(K_2, K_3)|\text{Conditions (13) and (17)}\}| = 2^{16};$$
$$|\{(K_4, K_5)|\text{Conditions (19), (20) and (21)}\}| = 2^{29};$$
$$|\{(K_6, K_7)|\text{Conditions (14), (18), (22) and (23)}\}| = 2^{14}.$$

Therefore, Chen and Dai [9] got that there are a total of 2^{90} possible values for K_A satisfying the above 12 conditions, and thus there are 2^{90} weak keys.

4.2 Chen and Dai's 7-Round Related-Key Amplified Boomerang Distinguisher

We now describe Chen and Dai's related-key amplified boomerang distinguisher for Rounds 1–7 under the class of 2^{90} weak keys (K_A, K_B, K_C, K_D) described in Section 4.1.

The first related-key differential $\Delta\alpha \to \Delta\beta$ for this distinguisher is the 2-round related-key differential $(0^{48}||b) \to (0^{32}||c||0^{16})$ with probability 1 for Rounds 1–2 under (K_A, K_B) or under (K_C, K_D), where 0^{48} represents a binary string of 48 zeros and so on. The second related-key differential $\Delta\gamma \to \Delta\delta$ for this distinguisher is the 5-round related-key differential $(0^{48}||b) \to 0$ with probability 2^{-27} for Rounds 3–7 under (K_A, K_C) or under (K_B, K_D). In Fig. 6 in Appendix A we illustrate the two related-key differentials in detail, where $R_{4,3}$ denotes the 3-rd bit of R_4 (the right half of the output of Round 4), and $R_{4,12}$ denotes the 12-th bit of R_4.

Consequently, Chen and Dai obtained a 7-round related-key amplified boomerang distinguisher with probability $1^2 \times (2^{-27})^2 \times 2^{-64} = 2^{-118}$ under a weak key (K_A, K_B, K_C, K_D). As a result, they presented an attack on 8-round MISTY1 without the last two FL functions, by conducting a key recovery on $\mathbf{FO}_8$ (in a way similar to the early abort technique used in [32]).

4.3 An Improved 7-Round Related-Key Amplified Boomerang Distinguisher

First focus on the $\mathbf{FI}_{73}$ function in the second related-key differential $\Delta\gamma \to \Delta\delta$ used in Chen and Dai's 7-round distinguisher, where the probability is 2^{-16}. Observe that $KI_{73} = K'_2$ or K'^*_2, depending on which pair from a quartet is considered. Chen and Dai used a probability value of 2^{-16} for the differential $\Delta c \to \Delta c$ operating on $\mathbf{FI}_{73}$. Similar to

what we mention in Section 3.3, we should make sure that a weak key (K_A, K_B, K_C, K_D) should also satisfy the condition that the differential $\Delta c \to \Delta c$ is a possible differential for $\mathbf{FI}_{73}$; otherwise, the differential $\Delta c \to \Delta c$ would have a zero probability, and the 7-round distinguisher would be flawed. Thus, we should put the following two additional conditions when defining a set of weak keys:

$$\Pr_{\mathbf{FI}(\cdot,K_2')}(\Delta c \to \Delta c) > 0; \tag{25}$$
$$\Pr_{\mathbf{FI}(\cdot,K_2'^*)}(\Delta c \to \Delta c) > 0. \tag{26}$$

After performing a computer programming, we surprisingly find that the number of (K_2, K_3) satisfying Conditions (13),(17),(25) and (26) is equal to the number of (K_2, K_3) satisfying Conditions (13) and (17), that is $|\{(K_2, K_3)|\text{Conditions (13), (17), (25) and (26)}\}| = 2^{16}$. This means that the class of weak keys satisfying Conditions (13)–(26) is the same as the class of weak keys satisfying Conditions (13)–(24) due to Chen and Dai. But nevertheless we find something valuable: For each possible K_2' or $K_2'^*$, there are exactly two pairs of inputs to $\mathbf{FI}_{73}$ which follow the differential $\Delta c \to \Delta c$, that is to say, the differential $\Delta c \to \Delta c$ for $\mathbf{FI}_{73}$ has a probability of 2^{-15}, twice as large as the probability value used by Chen and Dai.

Therefore, the second related-key differential $\Delta\gamma \to \Delta\delta$ used in Chen and Dai's 7-round distinguisher actually has a probability of 2^{-26}, and the resulting 7-round distinguisher has probability $1^2 \times (2^{-26})^2 \times 2^{-64} = 2^{-116}$ under a weak key (K_A, K_B, K_C, K_D).

Particularly we have the following result.

Proposition 3. *In the class of 2^{90} weak keys satisfying Conditions (13)–(26),*

1. *there are 2^{16} possible values for K_1, 2^{14} possible values for K_5, and 2^{15} possible values for K_8;*
2. *there are 2^{14} possible values for (K_6, K_7); in particular there are a total of 2^{13} possible values for K_7, and for every possible value of K_7 there are 2 possible values for K_6;*
3. *there are a total of 2^{16} possible values for K_3';*
4. $\Pr_{\mathbf{FI}(\cdot,\forall K_2')}(\Delta c \to \Delta c) = \Pr_{\mathbf{FI}(\cdot,\forall K_2'^*)}(\Delta c \to \Delta c) = 2^{-15}$.

4.4 Attacking the Full MISTY1 under the Class of 2^{90} Weak Keys

We devise a related-key amplified boomerang attack on the full MISTY1 under a weak key from the weak key class, basing it on the 7-round related-key amplified boomerang distinguisher with probability 2^{-116}.

Preliminary Results. First concentrate on the propagation of the output difference $\delta(=0)$ of the 7-round distinguisher through the following Round 8, including the $\mathbf{FL}_9$ and $\mathbf{FL}_{10}$ functions, under (K_A, K_C) or under (K_B, K_D); see Fig. 4.

Under (K_A, K_C), by the key schedule of MISTY1 we have

$$\begin{aligned}
&\Delta KO_{81} = \Delta K_8 = 0, \Delta KO_{82} = \Delta K_2 = 0,\\
&\Delta KO_{83} = \Delta K_7 = 0, \Delta KO_{84} = \Delta K_4 = 0,\\
&\Delta KI_{81} = \Delta K_5' = b, \Delta KI_{82} = \Delta K_1' = 0, \Delta KI_{83} = \Delta K_3' = 0,\\
&\Delta KL_9 = \Delta(K_5||K_3') = 0, \Delta KL_{10} = \Delta(K_7'||K_1) = 0.
\end{aligned}$$

Since $\delta = 0$, the $\mathbf{FI}_{81}$ and $\mathbf{FI}_{82}$ functions both have a zero input difference. The first S_9 and S_7 in $\mathbf{FI}_{81}$ both have a zero input difference, however, as $\Delta KI_{81} = b$ we know the second S_9 in $\mathbf{FI}_{81}$ has an input difference $0^2||a$, thus the output difference of the $\mathbf{FI}_{81}$

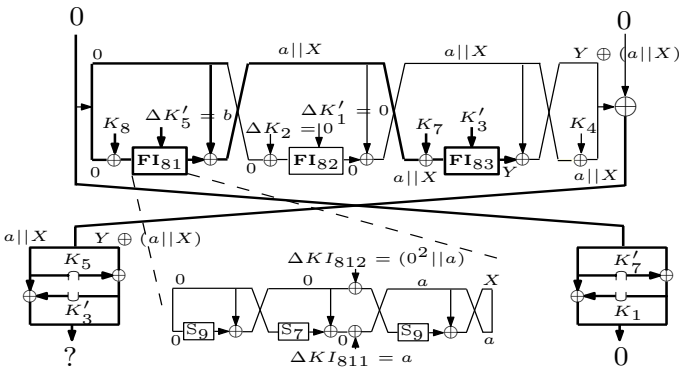


Fig. 4. Propagation of δ through Round 8 with $\mathbf{FL}_9$ and $\mathbf{FL}_{10}$

function has a form of $a||X$, where $X \in \{0,1\}^9$ can take only 2^8 possible values, and we denote by $\mathcal{S}_a$ the set of the 2^8 possible values for X. Since $\Delta KO_{82} = 0$ and $\Delta KI_{82} = 0$, the $\mathbf{FI}_{82}$ function has a zero output difference. Since $\Delta KO_{83} = 0$, the $\mathbf{FI}_{83}$ function has an input difference $a||X$. We assume the output difference for $\mathbf{FI}_{83}$ is Y. Then, the $\mathbf{FO}_8$ function has an output difference $(a||X)||(Y \oplus (a||X))$, so the $\mathbf{FL}_9$ function has an input difference $(a||X)||(Y \oplus (a||X))$, but its output difference is indeterminate (Denoted by the question marker in Fig. 4). The $\mathbf{FL}_{10}$ function has a zero input and output difference.

The same results hold for the propagation of δ under (K_B, K_D); note that X and Y under this case may take a different value from that case under (K_A, K_C).

Finally, since the $\mathbf{FI}_{82}$ function has a zero input and output difference, by the structure of the $\mathbf{FO}$ function we observe that only the subkeys $(K_1, K'_3, K_5, K'_5, K'^*_5, K_7, K'_7, K_8)$ are required when checking whether a candidate quartet consisting of two ciphertext pairs produces the output difference $\delta = 0$ of the 7-round distinguisher. Since $K'_5 = \mathbf{FI}(K_5, K_6)$, $K'^*_5 = K'_5 \oplus b$ and $K'_7 = \mathbf{FI}(K_7, K_8)$, we have the following result.

Proposition 4. *Only the subkeys $(K_1, K'_3, K_5, K_6, K_7, K_8)$ are required when checking whether a candidate quartet consisting of two ciphertext pairs satisfies the output difference $\delta = 0$ of the 7-round distinguisher.*

Attack Procedure. First we precompute two hash tables $\mathcal{T}_1$ and $\mathcal{T}_2$, as follows.

Table $\mathcal{T}_1$. Note that $KI_{81} = K'_5$ or $K'^*_5 (= K'_5 \oplus b)$, $KO_{83} = K_7$, and $KI_{83} = K'_3$. Under every possible (K'_3, K'_5, K_7), we compute $(\Delta\mu, \Delta\nu)$ for every $x = (x_L||x_R) \in \{0,1\}^{32}$, as follows.

$$\begin{aligned}\mu = &\ \mathbf{FI}_{81}(x_L, K'_5) \oplus \mathbf{FI}_{81}(x_L, K'_5 \oplus b),\\ \nu = &\ \mathbf{FI}_{83}(\mathbf{FI}_{81}(x_L, K'_5) \oplus X_R \oplus K_7, K'_3) \oplus\\ &\ \mathbf{FI}_{83}(\mathbf{FI}_{81}(x_L, K'_5 \oplus b) \oplus X_R \oplus K_7, K'_3).\end{aligned}$$

By the structure of $\mathbf{FI}$, we know the left 7 bits of μ must be a, and μ has the form $a||X$, that is $\mu = (a||X)$, where $X \in \mathcal{S}_a$, where $\mathcal{S}_a$ is defined above. For a fixed $(K'_3, K'_5, K_7, \mu, \nu)$, on average there are $2^{32} \times 2^{-8} \times 2^{-16} = 2^8$ satisfying values for x. We store the satisfying values of x into table $\mathcal{T}_1$ indexed by the value $(K'_3, K'_5, K_7, X, \nu)$. There are 2^{16} possible values for K'_3, at most 2^{16} possible values for K'_5, 2^{13} possible values for K_7, 2^8 possible values for μ, and 2^{16} possible values for ν, thus this precomputation takes about $2^{16} \times 2^{16} \times 2^{13} \times 2^8 \times 2^{16} \times 4 = 2^{71}$ $\mathbf{FI}$ computations, and $\mathcal{T}_1$ requires a memory of about $2^{16} \times 2^{16} \times 2^{13} \times 2^8 \times 2^{16} \times 2^8 \times 4 = 2^{79}$ bytes.

Table $\mathcal{T}_2$. Under every possible (K_1, K_7', K_8), we compute $\lambda = (K_8||0^{16}) \oplus \mathbf{FL}_{10}^{-1}(x, K_7'||K_1)$ for each $x \in \{0,1\}^{32}$. There are 2^{16} possible values for K_1, 2^{13} possible values for K_7, 2^{15} possible values for K_8, and 2^{16} possible values for K_7'. Note that $K_7 = \mathbf{FI}^{-1}(K_7', K_8)$. For a fixed (x, λ, K_7), on average there are $2^{16} \times 2^{15} \times 2^{-32} = 0.5$ satisfying values for (K_1, K_7', K_8); for a fixed (K_1, K_7, K_8), there are 2^{32} satisfying (x, λ). We make table $\mathcal{T}_2$ in the following manner:

For every possible K_7:

For every possible (K_1, K_8):

- Compute $K_7' = \mathbf{FI}(K_7, K_8)$.
- Find all the 2^{32} possible (x, λ) such that $\lambda = (K_8||0^{16}) \oplus \mathbf{FL}_{10}^{-1}(x, K_7'||K_1)$.
- Store (K_1, K_8) into Table $\mathcal{T}_2$ indexed first by K_7 and then by (x, λ).
- Set a binary marker with two possible statuses, "up" and "down", to the set of 2^{32} tuples $(K_7, K_1, K_8, x, \lambda)$. The marker's initial status is down.

That is, for a K_7, there are 2^{31} markers corresponding to the 2^{31} possible values of (K_1, K_8); and 2^{32} different (x, λ) that work under the same (K_7, K_1, K_8) share the same marker. $\mathcal{T}_2$ requires a memory of about $2^{13} \times 2^{16} \times 2^{15} \times 2^{32} \times 4 = 2^{78}$ bytes. This precomputation has a time complexity of about $2^{13} \times 2^{16} \times 2^{15} \times 2^{32} = 2^{76}$ $\mathbf{FL}^{-1}$ computations.

Now we can give the following attack procedure to break the full MISTY1.

1. Initialize zero to an array of 2^{75} counters corresponding to all the 2^{75} possible values for $(K_1, K_3', K_5, K_6, K_7, K_8)$.
2. Choose a set of $2^{58.5}$ plaintext pairs $(P, P^* = P \oplus (0^{48}||b))$, and another set of $2^{58.5}$ plaintext pairs $(P', P'^* = P' \oplus (0^{48}||b))$. In a chosen-plaintext attack scenario, obtain the ciphertexts for the plaintexts P, P^*, P', P'^* under K_A, K_B, K_C, K_D, respectively, and we denote by $C = (CL_L||CL_R, CR_L||CR_R)$ the ciphertext for plaintext P encrypted under K_A, by $C^* = (CL_L^*||CL_R^*, CR_L^*||CR_R^*)$ the ciphertext for plaintext P^* encrypted under K_B, by $C' = (CL_L'||CL_R', CR_L'||CR_R')$ the ciphertext for plaintext P' encrypted under K_C, and by $C'^* = (CL_L'^*||CL_R'^*, CR_L'^*||CR_R'^*)$ the ciphertext for plaintext P'^* encrypted under K_D.
3. Check whether a candidate quartet (C, C^*, C', C'^*) meets both the following conditions by storing the ciphertext pairs (C, C^*) and (C', C'^*) into a hash table indexed by the values $CR_L||CR_R||CR_L^*||CR_R^*$ and $CR_L'||CR_R'||CR_L'^*||CR_R'^*$.

$$(CR_L||CR_R) \oplus (CR_L'||CR_R') = 0, (CR_L^*||CR_R^*) \oplus (CR_L'^*||CR_R'^*) = 0.$$

Keep only the satisfying quartets.

4. For every remaining quartet (C, C^*, C', C'^*), do the following sub-steps.
   (a) Choose all the possible K_3' satisfying the following conditions:

$$(CL_R \cup K_3') \oplus CL_L \oplus (CL_R' \cup K_3') \oplus CL_L' = a||X',$$
$$(CL_R^* \cup K_3') \oplus CL_L^* \oplus (CL_R'^* \cup K_3') \oplus CL_L'^* = a||X^*,$$

   where X', X^* represents two indeterminate 9-bit values, (X', X^* can be different for different quartets, but obviously their values are fixed for a given quartet and K_3').
   (b) For every satisfying K_3', do as follows.
      i. Guess K_5, and compute the difference just before the $\mathbf{FL}_9^{-1}$ function between C and C', and the difference just before the $\mathbf{FL}_9^{-1}$ function between C^* and

C'^*. Let

$$\begin{aligned} & \mathbf{FL}_9^{-1}(CL_L||CL_R, K_5||K'_3) \oplus \mathbf{FL}_9^{-1}(CL'_L||CL'_R, K_5||K'_3) \\ = \; & a||X'||(Y' \oplus (a||X')), \\ & \mathbf{FL}_9^{-1}(CL^*_L||CL^*_R, K_5||K'_3) \oplus \mathbf{FL}_9^{-1}(CL'^*_L||CL'^*_R, K_5||K'_3) \\ = \; & a||X^*||(Y^* \oplus (a||X^*)), \end{aligned}$$

where Y', Y^* represent specific 16-bit values.

ii. Guess K_7; by Proposition 3-(2) we know there are two corresponding values for K_6 (for each guessed K_7), and we denote them by $\widetilde{K}_6$ and $\overline{K}_6$. Then, do the following four sub-steps.

A. Compute

$$\widetilde{K}'_5 = \mathbf{FI}(K_5, \widetilde{K}_6); \overline{K}'_5 = \mathbf{FI}(K_5, \overline{K}_6).$$

B. For (C, C'), access Table $\mathcal{T}_1$ at entry $(K'_3, \widetilde{K}'_5, K_7, X', Y')$ to get the possible 32-bit inputs to the $\mathbf{FO}_8$ function excluding the XOR operation with KO_{81}. As discussed earlier, when $X' \in \mathcal{S}_a$, on average there are 2^8 possible inputs, and we denote them by $\widetilde{x}_1, \widetilde{x}_2, \cdots, \widetilde{x}_{256}$; when X' does not belong to $\mathcal{S}_a$ we get no input and go to execute Step 4(b)(ii)(D). Similarly, for (C^*, C'^*), access Table $\mathcal{T}_1$ at entry $(K'_3, \widetilde{K}'_5, K_7, X^*, Y^*)$ to get the possible 32-bit inputs to the $\mathbf{FO}_8$ function excluding the XOR operation with KO_{81}, and we denote them by $\widetilde{x}^*_1, \widetilde{x}^*_2, \cdots, \widetilde{x}^*_{256}$ when $X^* \in \mathcal{S}_a$; when X' does not belong to $\mathcal{S}_a$ there is no input and we execute Step 4(b)(ii)(D).

C. For $i = 1, 2, \cdots, 256$, access Table $\mathcal{T}_2$ at entry $(K_7, CL_L||\ CL_R, \widetilde{x}_i)$ and flip the corresponding marker up. For $i = 1, 2, \cdots, 256$, access Table $\mathcal{T}_2$ at entry $(K_7, CL^*_L||CL^*_R, \widetilde{x}^*_i)$ and check whether the corresponding marker is up or down; if it is up, get the corresponding (K_1, K_8) and increase 1 to the counter corresponding to the guessed $(K_1, K'_3, K_5, \widetilde{K}_6,\ K_7, K_8)$, otherwise execute the next iteration (Initialize the markers in $\mathcal{T}_2$ to be down after finishing all the 256 iterations).

D. Repeat the above two sub-steps (B) and (C) similarly for the case $\overline{K}'_5$. When X' or X^* does not belong to $\mathcal{S}_a$, there is no input, and we execute Step 4(b)(ii) with another guess for K_7. (If this sub-step is done, go to Step 4(b)(ii), etc.)

5. For a value of $(K_1, K'_3, K_5, K_6, K_7, K_8)$ whose counter has a non-zero number, exhaustively search the remaining key bits with two known plaintext-ciphertext pairs. If a value of $(K_1, K_2, \cdots, K_8)$ is suggested, output it as the user key of the full MISTY1.

Note that in Step 4(b)(ii) we check the two pairs from a candidate quartet one after the other, instead of checking them simultaneously. This is the early abort technique for the (related-key) rectangle attack, described in [31] as well as in Chapter 4.4 of [30].

Attack Complexity. The attack requires $2^{58.5} \times 4 = 2^{60.5}$ chosen plaintexts. There are a total of $2^{58.5} \times 2^{58.5} = 2^{117}$ candidate quartets (C, C^*, C', C'^*), of which only $2^{117} \times (2^{-32})^2 = 2^{53}$ quartets are expected to satisfy the two conditions in Step 3. It takes about $2^{59.5}$ memory accesses to obtain the satisfying quartets. For every remaining quartet, on average there exist $2^{16} \times (2^{-7})^2 = 2^2$ possible values for K'_3 satisfying the two conditions in Step 4(a). Step 4(a) has a time complexity of about $2^{53} \times 2^{16} \times 4 \times \frac{1}{2} = 2^{70}$ **FL** computations. There are a total of 2^{14} possible values for K_5, thus Step 4(b)(i) has a time complexity

of $2^{53} \times 2^2 \times 2^{14} \times 4 \times \frac{1}{2} = 2^{70}$ **FL** computations (Note that some required intermediate values have been computed in Step 4(a)). There are a total of 2^{13} possible values for K_7, so Step 4(b)(ii)(A) has a time complexity of $2^{53} \times 2^2 \times 2^{14} \times 2^{13} \times 2 = 2^{83}$ **FI** computations. Step 4(b)(ii)(B) has a time complexity of about $2^{53} \times 2^2 \times 2^{14} \times 2^{13} \times \frac{256 \times 32}{64} + 2^{53} \times 2^2 \times 2^{14} \times 2^{13} \times 2^{-1} \times \frac{256 \times 32}{64} = 3 \cdot 2^{88}$ memory accesses (if conducted on a 64-bit computer), due to one-bit filtering condition on X'. Because of one-bit filtering condition on X^*, Step 4(b)(ii)(C) has a time complexity of about $2^{53} \times 2^2 \times 2^{14} \times 2^{13} \times 2^{-2} \times 256 \times 2 = 2^{89}$ memory accesses. Step 4(b)(ii)(D) has a time complexity of about $3 \cdot 2^{88} + 2^{89} = 5 \cdot 2^{88}$ memory accesses.

The probability that the counter for a wrong $(K_1, K_3', K_5, K_6, K_7, K_8)$ has a non-zero number is approximately $\sum_{i=1}^{2^{117}} [\binom{2^{117}}{i} \cdot (2^{-128})^i \cdot (1 - 2^{-128})^{2^{117}-i}] \approx 2^{-11}$. Thus, it is expected that there are a total of $2^{75} \times 2^{-11} = 2^{64}$ wrong values of $(K_1, K_3', K_5, K_6, K_7, K_8)$ whose counters are non-zero, so in total we need to access the array of counters only 2^{64} times in Steps 4(b)(ii)(C) and 4(b)(ii)(D). The 2^{64} wrong values of $(K_1, K_3', K_5, K_6, K_7, K_8)$ make at most 2^{79} possible values for $(K_1, K_2, \cdots, K_8)$, and thus it requires $2^{79} + 2^{79} \times 2^{-64} \approx 2^{79}$ trial encryptions to check them in Step 5. In Step 5, a wrong value of $(K_1, K_2, \cdots, K_8)$ is suggested with probability $2^{-64 \times 2} = 2^{-128}$, so it is expected that there remain $2^{79} \times 2^{-128} = 2^{-49}$ values for $(K_1, K_2, \cdots, K_8)$; that is to say, the number of suggested wrong user keys is rather low. Hence, the time complexity of the attack is dominated by Steps 4(b)(ii)(B), 4(b)(ii)(C) and 4(b)(ii)(D), which is $3 \cdot 2^{88} + 2^{89} + 5 \cdot 2^{88} \approx 2^{91.33}$ memory accesses, plus Step 5. Therefore, by the evaluation used in Section 3.4, the attack has a total time complexity of about $2^{91.33} \times 2^{-12} + 2^{79} \approx 2^{80.18}$ MISTY1 encryptions.

The counter for the correct key has an expected number of $2^{117} \times 2^{-116} = 2$, and the probability that the counter for the correct key has a non-zero number is approximately $\sum_{i=1}^{2^{117}} [\binom{2^{117}}{i} \cdot (2^{-116})^i \cdot (1 - 2^{-116})^{2^{117}-i}] \approx 0.86$. Therefore, the related-key impossible boomerang attack has a success probability of 86%.

The memory complexity of the attack is dominated by the space for the array of 2^{75} counters, which is $2^{75} \times \frac{75}{8} \approx 2^{78.23}$ bytes. Taking the storage space for $\mathcal{T}_1$ and $\mathcal{T}_2$ into consideration, we need a total memory space of $2^{79} + 2^{78} + 2^{78.23} \approx 2^{80.07}$ bytes.

It is very worthy to note that we can slightly reduce the memory space by splitting $\mathcal{T}_1$ into two smaller tables which mainly correspond to $\mathbf{FI}_{81}$ and $\mathbf{FI}_{83}$ respectively, but at the cost of a few more memory accesses in the attack procedure.

4.5 Three Other Classes of 2^{90} Weak Keys

The above sub-sections have shown a class of 2^{90} weak keys and a related-key amplified boomerang attack on the full MISTY1 under a weak key. Nevertheless, there exist three other classes of 2^{90} weak keys under which there are similar results. The new weak key classes are obtained by setting other possible values for the two subkey bits $(K_{5,3}, K_{5,12})$, which are further classified into several sub-classes by the possible values of the two subkey bits combination $(K'_{3,3}, K'_{3,12})$. This will affect only the $\mathbf{FL}_2$ function of the first related-key differential, and the input difference of $\mathbf{FL}_2$ will be fixed once the setting is given, provided that the output difference of $\mathbf{FL}_2$ is $0^9||a||b$. Likewise, by choosing a number of plaintext pairs with a corresponding difference we can conduct a similar attack on the full MISTY1 under every sub-class of weak keys. In total, we have 2^{92} weak keys under which a related-key amplified boomerang attack can break the full MISTY1.

One might consider obtaining more weak keys by setting $K'_{4,3} = 1$, instead of $K'_{4,3} = 0$ used in our results. This case will affect only the output difference of the $\mathbf{FL}_4$ function of the first related-key differential, and it seems that we can further classify the resulting class of weak keys into two sub-classes according to the possible values of the subkey bit

$K_{6,3}$, as we did before. However, this case is not possible, because $K_{6,3} \oplus K^*_{6,3} = 1$, and a detailed analysis reveals that under the condition that the input difference of $\mathbf{FL}_4$ is $c||0^{16}$, the output difference of $\mathbf{FL}_4$ under one plaintext pair from a candidate quartet is definitely not equal to the output difference of $\mathbf{FL}_4$ under the other plaintext pair from the candidate quartet. Consequently, the XOR of the four differences concerned between the two sub-ciphers when constructing an amplified boomerang distinguisher is definitely non-zero, so the four related-key differentials cannot form an amplified boomerang distinguisher.

5 Conclusions

The MISTY1 block cipher has received considerable attention and its security has been thoroughly analysed since its publication, particularly the European NESSIE project announced that "no weaknesses were found in the selected designs" when making the portfolio of selected cryptographic algorithms including MISTY1. In this paper, we have described $2^{103.57}$ weak keys for a related-key differential attack on the full MISTY1 and 2^{92} weak keys for a related-key amplified boomerang attack on the full MISTY1.

For the very first time, our results exhibit a cryptographic weakness in the full MISTY1 cipher algorithm , particularly from an academic point of view: The cipher does not behave like a random function (in the related-key model); thus it cannot be regarded to be an ideal cipher. From a practical point of view, our results do not pose a significant threat to the security of MISTY1, for the presented attacks work under the assumptions of weak-key and related-key scenarios and their complexity is beyond the power of a general computer of today. But nevertheless the weak key classes mean that a large fraction of all possible 2^{128} keys in the whole key space of MISTY1 is weak in the sense of related-key cryptanalysis, roughly, one of every twenty million keys in the larger set of $2^{103.57}$ weak keys, and thus the chance of picking such a weak key at random is not trivial; in this sense, the presence of these weak keys has an impact on the security of the full MISTY1 cipher.

Acknowledgments

The authors are very grateful to Prof. Wenling Wu for her help, and to Yibin Dai for providing the post-proceedings version of their paper at INSCRYPT 2011.

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 attacks using related keys. In: Helleseth, T. (ed.), EUROCRYPT 1993. LNCS, vol. 765, pp. 398–409. Springer, Heidelberg (1993)
3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999)
4. Biham, E., Dunkelman, O., Keller, N.: Related-key boomerang and rectangle attacks. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 507–525. Springer, Heidelberg (2005).
5. Biham, E., Dunkelman, O., Keller, N.: A related-key rectangle attack on the full KASUMI. In: Roy, B.K. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 443–461. Springer, Heidelberg (2005).
6. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4(1), 3–72. Springer (1991)
7. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 1–18. Springer, Heidelberg (2009).
8. Biryukov, A., Khovratovich, D., Nikolić, I.: Distinguisher and related-key attack on the full AES-256. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 231–249. Springer, Heidelberg (2009).

9. Chen, S., Dai, Y.: Related-key amplified boomerang attack on 8-round MISTY1. In: Li, C., Wang, H. (eds.) CHINACRYPT 2011, pp. 7–14. Science Press USA Inc. (2011)
10. CRYPTREC — Cryptography Research and Evaluatin Committees, report 2002.
11. Dai, Y., Chen, S.: Weak key class of MISTY1 for related-key differential attack. In: Moti, Y., Wu, C.K. (eds.) INSCRYPT 2011, to appear in LNCS.
12. 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)
13. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In: Rabin, T. (ed.): CRYPTO 2010. LNCS, vol. 6223, pp. 393–410. Springer, Heidelberg (2010)
14. Hong, S., Kim, J., Lee, S., Preneel, B.: Related-key rectangle attacks on reduced versions of SHACAL-1 and AES-192. In: Gilbert, H., Handschuh, H. (eds.) FSE 2005. LNCS, vol. 3557, pp. 368–383. Springer, Heidelberg (2005).
15. International Standardization of Organization (ISO), International Standard – ISO/IEC 18033-3, Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, 2005/2010.
16. 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification, V3.1.1 (2001)
17. Kelsey, J., Schneier, B., Wagner, D.: Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 237–251. Springer, Heidelberg (1996)
18. 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)
19. Kim, J., Hong, S., Preneel, B., Biham, E., Dunkelman, O., Keller, N.: Related-Key Boomerang and Rectangle Attacks. IACR ePrint report 2010/019, accepted to IEEE Transactions on Information Theory, to appear.
20. Kim, J., Kim, G., Hong, S., Lee, S., Hong, D.: The related-key rectangle attack — application to SHACAL-1. In: Wang, H., Pieprzyk, J., Varadharajan, V. (Eds.) ACISP 2004. LNCS, vol. 3108, pp. 123–136. Springer, Heidelberg (2004).
21. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Seberry, J., Zheng, Y. (eds.) ASIACRYPT 1992. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg (1993)
22. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995)
23. Knudsen, L.R.: DEAL — a 128-bit block cipher. Technical report, Department of Informatics, University of Bergen, Norway (1998).
24. Knudsen, L.R., Wagner, D.: Integral cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
25. Kühn, U.: Cryptanalysis of reduced-round MISTY. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 325–339. Springer, Heidelberg (2001)
26. Kühn, U.: Improved cryptanalysis of MISTY1. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 61–75. Springer, Heidelberg (2002)
27. Lai, X.: Higher order derivatives and differential cryptanalysis. In: Communications and Cryptography, pages 227–233, 1994. Academic Publishers.
28. Lai, X., Massey, J.L., Murphy, S: Markov ciphers and differential cryptanalysis. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 17–38. Springer, Heidelberg (1991)
29. Lee, S., Kim, J., Hong, D., Lee, C., Sung, J., Hong, S., Lim, J.: Weak key classes of 7-round MISTY 1 and 2 for related-key amplied boomerang attacks. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 91-A(2), 642–649 (2008)
30. Lu, J.: Cryptanalysis of block ciphers. PhD thesis, University of London, UK (2008)
31. Lu, J., Kim, J.: Attacking 44 rounds of the SHACAL-2 block cipher using related-key rectangle cryptanalysis. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E91-A(9), 2588-2596 (2008).
32. 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)
33. Matsui, M.: New block encryption algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)
34. Murphy, S.: The return of the cryptographic boomerang. IEEE Transactions on Information Theory 57(4), 2517-2521 (2011)
35. NESSIE — New European Schemes for Signatures, Integrity, and Encryption, final report of European project IST-1999-12324.

36. National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES), FIPS-197 (2001).
37. RFC 2994 — a description of the MISTY1 encryption algorithm. The Internet Engineering Task Force (IETF), 2000. http://tools.ietf.org/html/rfc2994
38. Sun, X., Lai, X.: Improved integral attacks on MISTY1. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 266–280. Springer, Heidelberg (2009)
39. Tanaka, H., Hatano, Yasuo., 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 (2007)
40. Tsunoo, Y., Saito, T., Nakashima, H., Shigeri, M.: Higher order differential attack on 6-round MISTY1. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 92-A(1), 3–10 (2009)
41. 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)
42. Tsunoo, Y., Saito, T., Shigeri, M., Kawabata, T.: Security analysis of 7-round MISTY1 against higher order differential attacks. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 93-A(1), 144–152 (2010)
43. Wagner, D.: The boomerang attack. In: Knudsen, L.R. (ed.) FSE 1999. LNCS, vol. 1636, pp. 156–170. Springer, Heidelberg (1999)

Appendix A

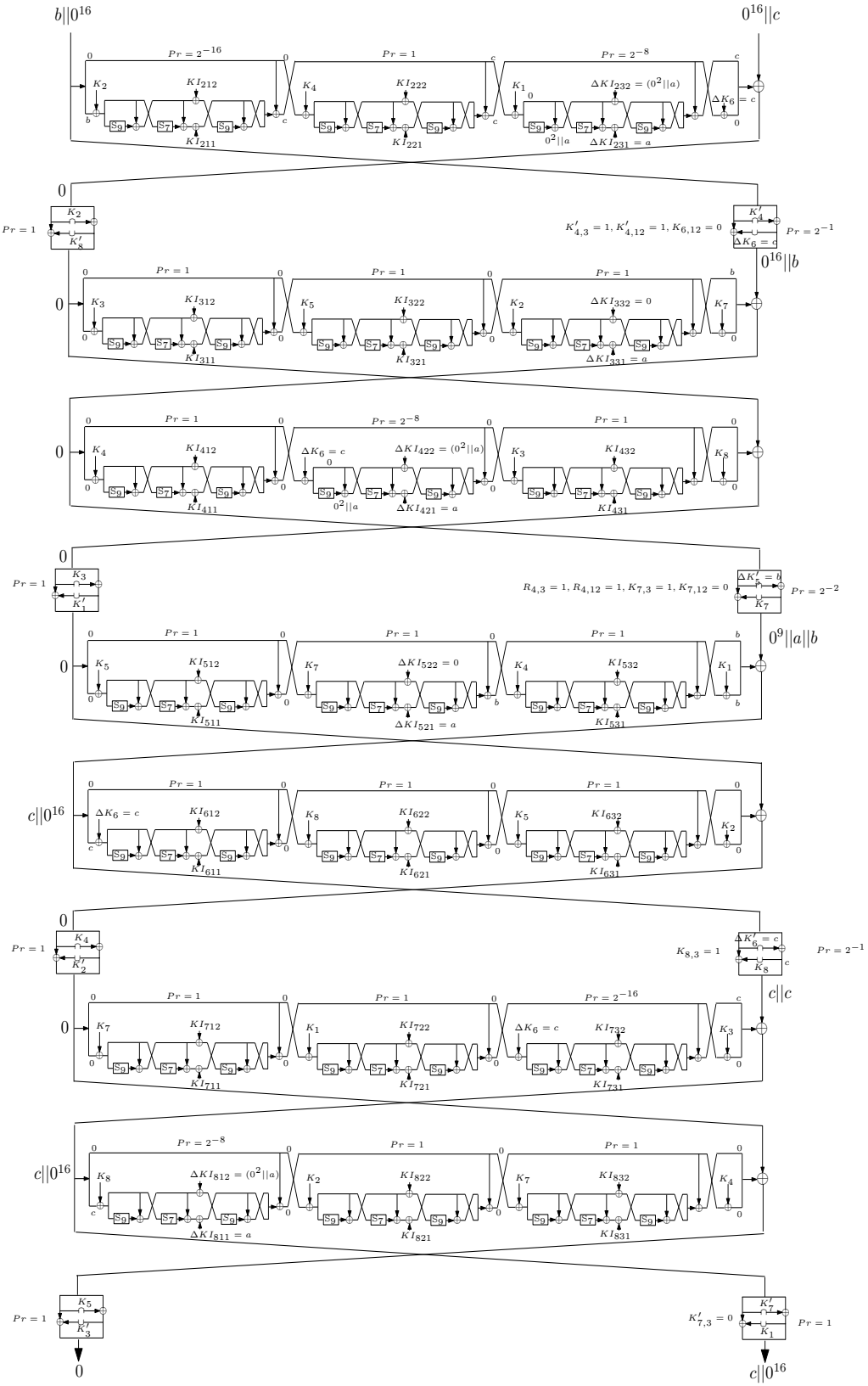
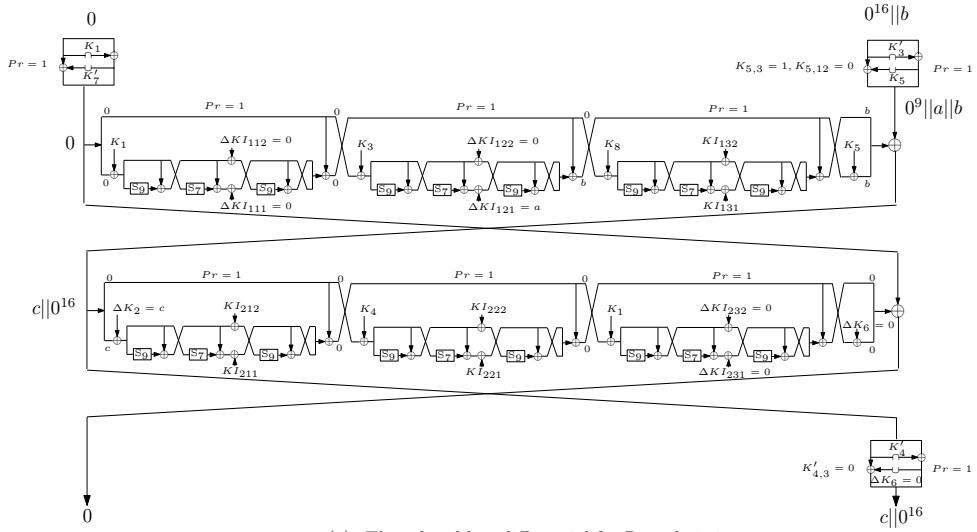
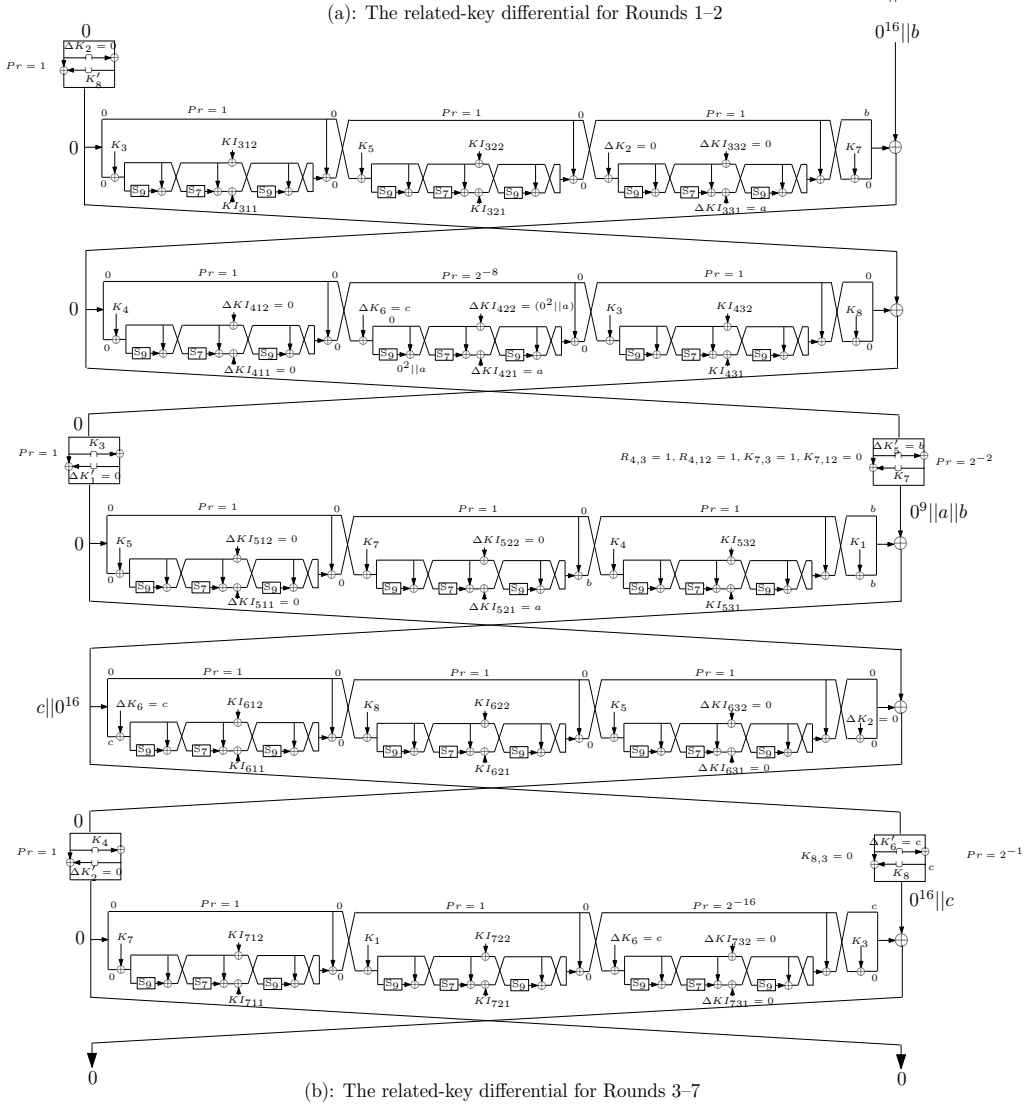


Fig. 5. Chen and Dai's related-key differential characteristic for Rounds 2–8



(a): The related-key differential for Rounds 1–2



(b): The related-key differential for Rounds 3–7

Fig. 6. The two related-key differentials used in Chen and Dai's 7-round distinguisher