Weak Keys of the Full MISTY1 Block Cipher for Related-Key Differential 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, Singapore 138632
lvjiqiang@hotmail.com, {jlu,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, a 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 a related-key differential attack 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 $2^{90.93}$ encryptions. For the first time, our result exhibits a cryptographic weakness in the full MISTY1 cipher (when used with the recommended 8 rounds), and shows that the MISTY1 cipher is distinguishable from an ideal cipher and thus cannot be regarded to be an ideal cipher.

Keywords: Block cipher, MISTY1, Differential cryptanalysis, Related-key cryptanalysis, Weak key.

1 Introduction

The MISTY1 block cipher was designed by Matsui [26] and published in 1997. It has a 64-bit block length, a 128-bit user key, and a variable number of rounds;

* An earlier version of this work appeared in 2012 as part of Cryptology ePrint Archive Report 2012/066 [25]. This work was partially supported by the Natural Science Foundation of China (No. 61100185), Guangxi Natural Science Foundation (No. 2011GXNSFB018071), the Foundation of Guangxi Key Lab of Wireless Wideband Communication and Signal Processing (No. 11101), and China Postdoctoral Science Foundation Funded Project.

E. Dawson (Ed.): RSA 2013, LNCS 7779, pp. 389–404, 2013.

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 [7] e-government recommended cipher in 2002, and a NESSIE [27] selected block cipher in 2003, and was adopted as an ISO [11] 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, 6, 9, 10,18,19,22,24,29–31]. In summary, the main previously published cryptanalytic results on MISTY1 are as follows. In 2008, Dunkelman and Keller [10] described impossible differential attacks [3, 16] on 6-round MISTY1 with FL functions and 7-round MISTY1 without FL functions. In the same year, Lee et al. [22] gave a related-key amplified boomerang attack [13] on 7-round MISTY1 with FL functions under a class of 2^{73} weak keys[1], and Tsunoo et al. [30] presented a higher-order differential attack [15, 20] on 6 and 7-round MISTY1 with FL functions (without making a weak key assumption). In 2009, Sun and Lai [29] presented an integral attack on 6-round MISTY1 with FL functions, building on Knudsen and Wagner's integral attack [17] on 5-round MISTY1. Following Lee et al.'s work, in 2011 Chen and Dai [6] 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 subsequently Dai and Chen [8, 9] 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.[2] By now, there has been no published (non-generic) cryptanalytic attack on the full 8 rounds of MISTY1 yet.

Related-key cryptanalysis [2, 14] 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 [12]. Related-key differential cryptanalysis [12] is a combination of differential cryptanalysis [4] and related-key cryptanalysis; it 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. Remarkably, under certain weak key assumptions the related-key differential cryptanalysis technique was used in 2009 by Biryukov et al. [5] to yield

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

[2] Our work is based on the version of Dai and Chen's paper that we requested from Dai in February 2012 [8]. However, we note that the post-proceedings version [9] of their paper appeared in the LNCS website a few days ago, acknowledging us, where the results were modified as given in Table 1.

Table 1. Main cryptanalytic results on MISTY1 with FL functions

#Rounds	#Keys	Attack Type	Data	Memory	Time	Source
6 (1 – 6)	2^{128}	Impossible differential	2^{51} CP	not specified	$2^{123.4}$ Enc.	[10]
6 (1 – 6)	2^{128}	Higher-order differential	$2^{53.7}$ CP	not specified	$2^{64.4}$ Enc.	[30]
6 (3 – 8)	2^{128}	Integral	2^{32} CC	not specified	$2^{126.1}$ Enc.	[29]
7 (1 – 7)	2^{128}	Higher-order differential	$2^{54.1}$ CP	not specified	$2^{120.7}$ Enc.	[30, 31]
7† (2 – 8)	2^{73}	Related-key amplified boo.	2^{54} CP	2^{59} Bytes	$2^{55.3}$ Enc.	[22]
8† (1 – 8)	2^{90}	Related-key amplified boo.	2^{63} CP	2^{65} Bytes	2^{70} Enc.	[6]
8† (1 – 8)	2^{105}‡	Related-key differential	2^{63} CC	2^{37} Bytes	$2^{86.6}$ Enc.	[8]
	$2^{102.57}$	Related-key differential	2^{61} CC	2^{35} Bytes	$2^{84.6}$ Enc.	[9]
full	$2^{103.57}$	Related-key differential	2^{61} CC	$2^{99.2}$ Bytes	$2^{90.93}$ Enc.	Sect. 4§

†: Exclude the first/last two FL functions; ‡: There is a flaw, see Section 3 for detail; §: Complexity is only for one class of weak keys.

the first cryptanalytic attack on the full version of the AES [28] block cipher with 256 key bits.

In this paper, we show for the very first time that the full MISTY1 cipher can be distinguished from an ideal cipher (in the related-key model), mainly from a theoretical perspective: Building on Dai and Chen's work described in [8, 9], we present a related-key differential attack on the full MISTY1 cipher under certain weak key assumptions. First, we spot a flaw in Dai and Chen's differential cryptanalysis results from [8], and find that there are only about $2^{102.57}$ weak keys in their weak key class such that their 7-round related-key differential holds, but with probability 2^{-58}. Then, we use the 7-round related-key differential with probability 2^{-58} to break the full MISTY1 under the class of $2^{102.57}$ weak keys. Finally, we observe that there also exists a different class of $2^{102.57}$ weak keys under which similar results hold. 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, and Enc. refers to the required number of encryption operations of the relevant version of MISTY1.

We would like to mention that the original version of this paper, entitled "weak keys of the full MISTY1 block cipher for related-key cryptanalysis", contained a set of 2^{92} weak keys of the full MISTY1 for a related-key amplified boomerang attack [25], but we remove it from this proceedings version, because of page constraints.

The remainder of the paper is organised as follows. In the next section, we give the notation and describe the MISTY1 cipher. In Section 3 we review Dai and Chen's class of weak keys and their 7-round related-key differential characteristic, and give our corrected class of weak keys and 7-round related-key differential. We present our attack on MISTY1 in Section 4. In Section 5 we describe another class of weak keys. Section 6 concludes this paper.

2 Preliminaries

In this section we give the notation and briefly describe the MISTY1 cipher.

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) of two bit strings of the same length
$\cap$: bitwise logical AND of two bit strings of the same length
$\cup$: bitwise logical OR of two bit strings of the same length
$||$: bit string concatenation

2.2 The MISTY1 Block Cipher

MISTY1 [26] 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** : $\{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32}$ is a key-dependent linear function. If $X = (X_L||X_R)$ is a 32-bit block of two 16-bit words X_L, X_R, 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** : $\{0,1\}^{16} \times \{0,1\}^{16} \to \{0,1\}^{16}$ is a non-linear function. If $X = (X_L||X_R)$ and $Y = (Y_1||Y_2)$ are 16-bit blocks, here X_L, Y_2 are 9 bits long and X_R, Y_1 are 7 bits long, 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.
  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. $\mathbf{FI}(X, Y) = (XL_3||XR_3)$.
- **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 of two 16-bit words X_L, X_R, $Y = (Y_1||Y_2||Y_3||Y_4)$ 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. $\mathbf{FO}(X, Y, Z) = (XL_3 \oplus Y_4)||XR_3$.

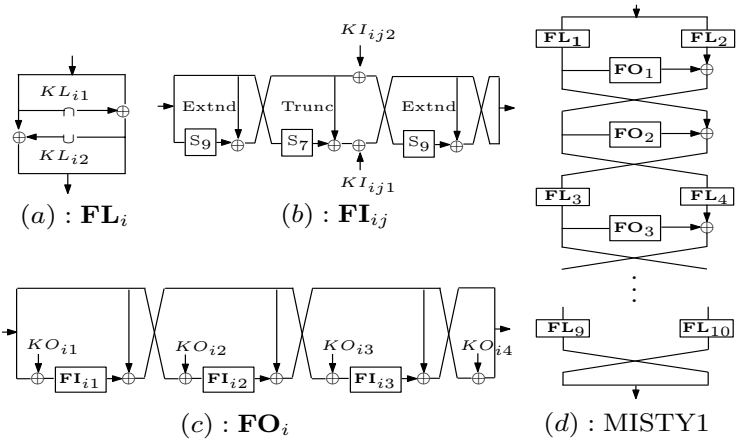

Fig. 1. MISTY1 and its components

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.

$$KO_{i1} = K_i, KO_{i2} = K_{i+2}, KO_{i3} = K_{i+7}, KO_{i4} = K_{i+4};$$
$$KI_{i1} = K'_{i+5}, KI_{i2} = K'_{i+1}, KI_{i3} = K'_{i+3};$$
$$KL_i = K_{\frac{i+1}{2}} || K'_{\frac{i+1}{2}+6}, \text{ for } i = 1, 3, 5, 7, 9; \text{otherwise, } KL_i = K'_{\frac{i}{2}+2} || K_{\frac{i}{2}+4}.$$

MISTY1 takes a 64-bit plaintext P as input, and has a variable number of rounds; the officially 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.

3 A Related-Key Differential for 7-Round MISTY1 under a Class of $2^{102.57}$ Weak Keys

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}.

3.1 A Class of 2^{105} Weak Keys Owing 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 $c = (a||0^9)$, where 0^2 represents a binary string of 2 zeros, and so on.

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 [8] 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. In Fig. 3 in the Appendix 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 [24] as well as in Chapter 4.2 of [23]).

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 program 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.[3] 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 program 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] Note that this is not a mistake under the stochastic equivalence hypothesis for differential cryptanalysis given in [21], although it contradicts the fact.

4 Related-Key Differential Attack on the Full MISTY1 under the Class of $2^{102.57}$ Weak Keys

In this section, we devise a related-key differential attack on the full MISTY1 under a weak key from the class of $2^{102.57}$ weak keys, basing it on the 7-round related-key differential with probability 2^{-58}.

4.1 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. 2.

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. 2, 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 $X = (\mathrm{Trunc}(A)||(B \oplus (0^2||\mathrm{Trunc}(A))))$. A simple computer program reveals that $\mathrm{Trunc}(A)$ 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 $\overbrace{00?0000000000000||00?0000000000000}^{32\ bits}$, 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. 2.

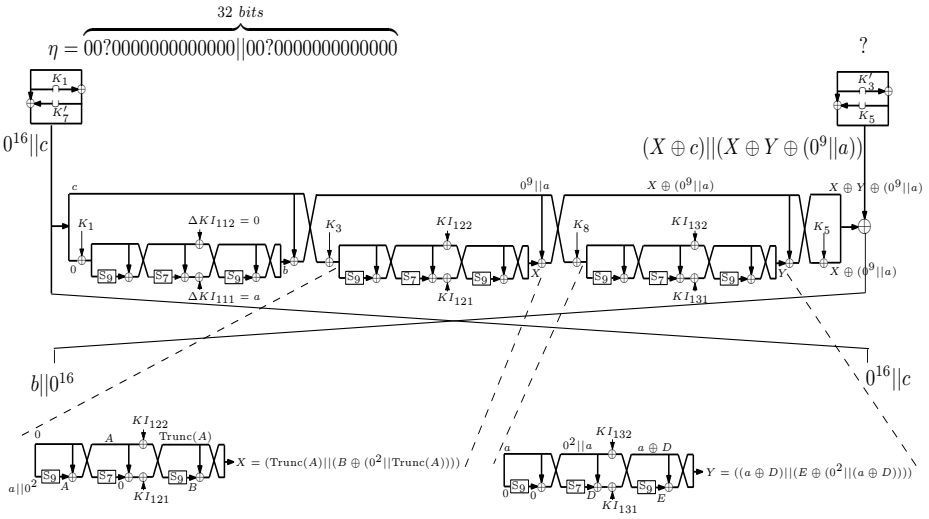

Fig. 2. Propagation of α through the inverse of Round 1 with $\mathbf{FL}_1$ and $\mathbf{FL}_2$

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 obtain 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.*

4.2 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 $2^{16} \times 2^{-1} \times 2^{16} \times 2^8 \times 2^{-16} = 2^{23}$ 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 the plaintext for ciphertext C encrypted under K_A by $P = (PL_L||PL_R, PR_L||PR_R)$, and the plaintext for ciphertext C^* encrypted under K_B by $P^* = (PL^*_L||PL^*_R, PR^*_L||PR^*_R)$.
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.

4.3 Attack Complexity

The attack requires $2^{60} \times 2 = 2^{61}$ chosen ciphertexts. In Step 3, only $2^{60} \times 2^{-30} \times \frac{3}{4} \approx 2^{29.58}$ plaintext pairs are expected to satisfy the condition, and it takes about 2^{60} memory accesses to obtain the satisfying plaintext 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 precomputation phase; owing 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 precomputation 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 it requires two memory accesses for a single access to an entry whose length is between 65 and 128 bits 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.

The question that how many memory accesses (table lookups) are equivalent to one MISTY1 encryption in terms of time depends closely on the used platform and MISTY1 implementation as well as the storage location of the hash table. In theoretical block cipher cryptanalysis, it is usually assumed by default that a hash table is stored in an ideal place, RAM say, like an S-box table; and it takes an almost constant time to access an entry in a hash table,

independently of the number of entries. Thus, an extremely conservative estimate is: 16 memory accesses equal a full MISTY1 encryption in terms of time, assuming that in every round, Round i say, the $\mathbf{FI}_{i1}$ and $\mathbf{FI}_{i2}$ functions are implemented in parallel, equivalent to one memory access, and the subsequent $\mathbf{FI}_{i3}$ function is equivalent to one memory access, (neglecting the computational complexity for other operations and the key schedule); that is, one round is equivalent to 2 memory accesses. Therefore, the attack has a total time complexity of about $\frac{2^{93.15}+2^{94.15}}{16} + 2^{87.9} \approx 2^{90.93}$ 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.

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

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 cipher algorithm.

6 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 cipher algorithm.

For the very first time, our result exhibits a cryptographic weakness in the full MISTY1 cipher algorithm, mainly from an academic point of view: The cipher does not behave like an ideal cipher (in the related-key model); thus it

cannot be regarded to be an ideal cipher. From a practical point of view, our attack does not pose a significant threat to the security of MISTY1, for it works under the assumptions of weak-key and related-key scenarios and its complexity is beyond the power of a general computer of today. But nevertheless our result means 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 differential cryptanalysis, roughly, one of every twenty-two million 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 thank Prof. Wenling Wu for her help, Yibin Dai for providing the final version of their paper at INSCRYPT 2011, and several anonymous referees for their comments on earlier versions of the paper.

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 (1994)
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., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology 4(1), 3–72 (1991)
5. 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)
6. 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)
7. CRYPTREC — Cryptography Research and Evaluatin Committees, report 2002 (2003)
8. Dai, Y.: Personal communications (February 2012)
9. Dai, Y.-b., Chen, S.-z.: Weak-Key Class of MISTY1 for Related-Key Differential Attack. In: Wu, C.-K., Yung, M., Lin, D. (eds.) Inscrypt 2011. LNCS, vol. 7537, pp. 227–236. Springer, Heidelberg (2012)
10. 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)
11. International Standardization of Organization (ISO), International Standard – ISO/IEC 18033-3, Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers (2005/2010)
12. 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)

13. Kim, J., Hong, S., Preneel, B., Biham, E., Dunkelman, O., Keller, N.: Related-key boomerang and rectangle attacks: theory and experimental analysis. IEEE Transactions on Information Theory 58(7), 4948–4966 (2012)
14. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Zheng, Y., Seberry, J. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg (1993)
15. Knudsen, L.R.: Truncated and Higher Order Differentials. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 196–211. Springer, Heidelberg (1995)
16. Knudsen, L.R.: DEAL — a 128-bit block cipher. Technical report, Department of Informatics, University of Bergen, Norway (1998)
17. Knudsen, L.R., Wagner, D.: Integral Cryptanalysis. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 112–127. Springer, Heidelberg (2002)
18. Kühn, U.: Cryptanalysis of Reduced-Round MISTY. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 325–339. Springer, Heidelberg (2001)
19. Kühn, U.: Improved Cryptanalysis of MISTY1. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 61–75. Springer, Heidelberg (2002)
20. Lai, X.: Higher order derivatives and differential cryptanalysis. In: Communications and Cryptography, pp. 227–233. Academic Publishers (1994)
21. 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)
22. 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)
23. Lu, J.: Cryptanalysis of block ciphers. PhD thesis, University of London, UK (2008)
24. 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)
25. Lu, J., Yap, W.S., Wei, Y.: Weak keys of the full MISTY1 block cipher for related-key cryptanalysis. Cryptology ePrint Archive, Report 2012/066 (2012)
26. Matsui, M.: New Block Encryption Algorithm MISTY. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)
27. NESSIE — New European Schemes for Signatures, Integrity, and Encryption, final report of European project IST-1999-12324 (2004)
28. National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES), FIPS-197 (2001)
29. 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)
30. 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)
31. 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)

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

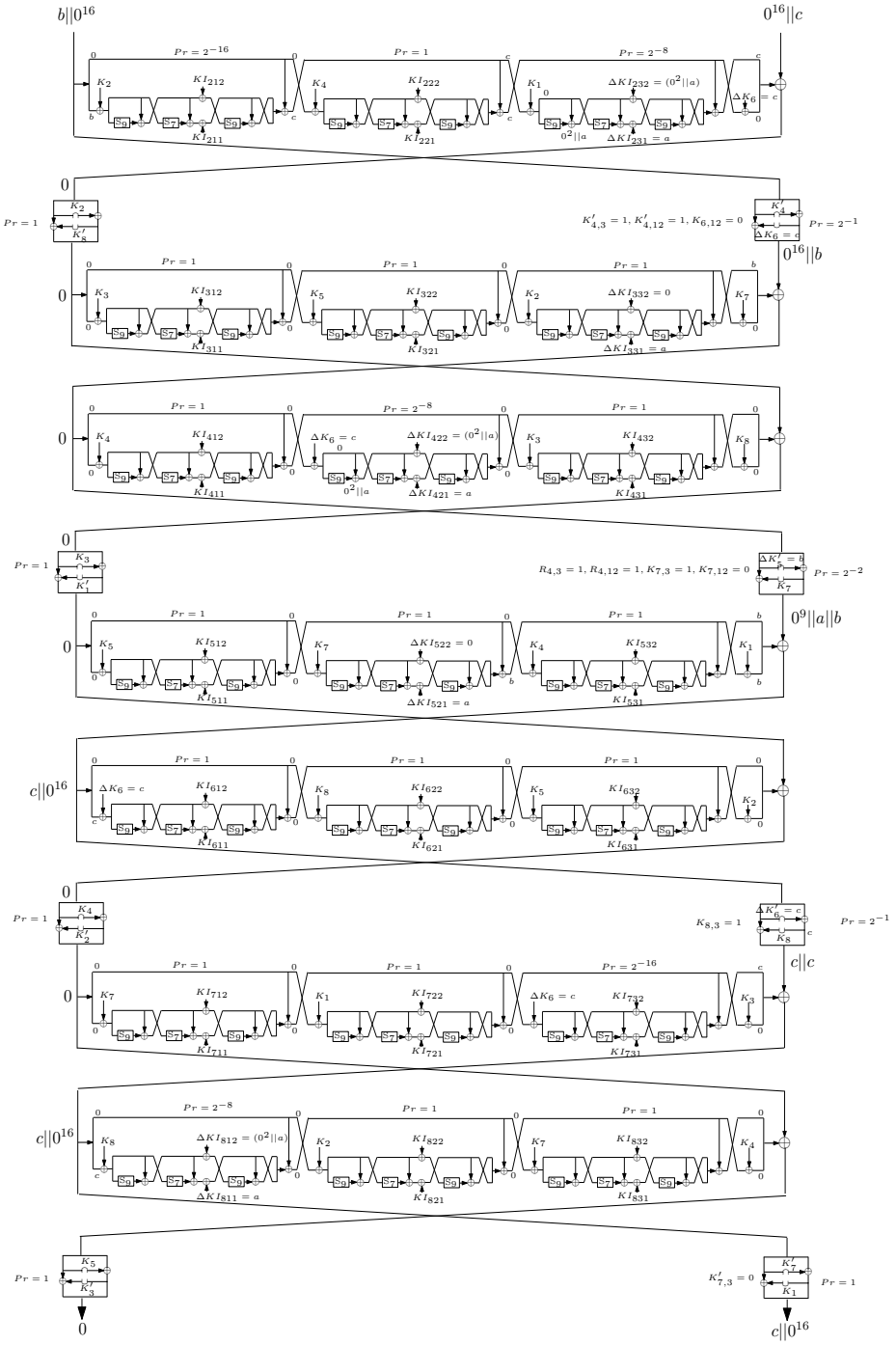

Fig. 3. Chen and Dai's related-key differential characteristic for Rounds 2–8