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

Jiqiang Lu

Institute for Infocomm Research,
Agency for Science, Technology and Research,
1 Fusionopolis Way, Singapore 138632
jlu@i2r.a-star.edu.sg, lvjiqiang@hotmail.com

Joint work with Wun-She Yap and Yongzhuang Wei.

28 March 2012

Outline:

1. Block Cipher Cryptanalysis
2. The MISTY1 Block Cipher
3. $2^{103.57}$ Weak Keys for a Related-Key Differential Attack
4. 2^{92} Weak Keys for a Related-Key Amplified Boomerang Attack
5. Conclusions

1.1 Block Cipher

- An important primitive in symmetric-key cryptography.
  * Main purpose: provide confidentiality — A most fundamental security goal.
- An algorithm that transforms a fixed-length data block into another data block of the same length under a secret user key.
  * Input: plaintext.
  * Output: ciphertext.
  * Three sub-algorithms: encryption, decryption, key schedule.
- Constructed by repeating a simple function many times, known as the iterated method.
  * An iteration: a round.
  * The repeated function: the round function.
  * The key used in a round: a round subkey.
  * The number of iterations: the number of rounds.
  * The round subkeys are generated from the user key under a key schedule algorithm.

1.2 A Cryptanalytic Attack

- An algorithm that distinguishes a cryptosystem from a random function.
- Usually measured using the following three metrics:
  * Data complexity
    - The numbers of plaintexts and/or ciphertexts required.
  * Memory (storage) complexity
    - The amount of memory required.
  * Time (computational) complexity
    - The amount of computation or time required, how many encryptions/decryptions or memory accesses.
- Goals:
  * Break a cryptosystem (ideally, in a practical complexity).
  * Enable more secure cryptosystems to be designed.

1.3 Four Cryptanalysis Scenarios

- Ciphertext-only attack scenario
  * Have access to a number of ciphertexts.
- Known-plaintext attack scenario
  * Have access to a number of ciphertexts and the corresponding plaintexts.
- Chosen-plaintext/cipertext attack scenario
  * Can choose a number of plaintexts (or ciphertexts), and be given the corresponding ciphertexts (or plaintexts).
- Adaptive chosen plaintext and ciphertext attack scenario
  * Can choose plaintexts (or ciphertexts) and be given the corresponding ciphertexts (or plaintexts). Based on the information obtained, the attacker can then choose further plaintexts/ciphertexts, and be given the corresponding ciphertexts/plaintexts ...

1.4 Three Elementary Cryptanalysis Techniques

Assume an n-bit block cipher with a k-bit user key $E_K(\cdot)$.

- A dictionary attack
  - * Build a table of all possible ciphertexts corresponding to one particular plaintext, with one entry for each possible key: $C_i = E_{K_i}(P)$.
  - * Data: 2^k ciphertexts, Memory: 2^k n-bit, Time: negligible.
- A codebook attack:
  - * Build a table of the ciphertexts for all the plaintexts encrypted using one unknown key: $C_i = E_K(P_i)$.
  - * Data: 2^n plaintext-ciphertext pairs, Memory: 2^n n-bit, Time: negligible.
- An exhaustive key search (or brute force search) attack:
  - * Try every possible key, given a known plaintext-ciphertext pair. The correct key will yield the correct correspondence: $E_{K_i}(P) \stackrel{?}{\rightarrow} C$.
  - * Data: negligible, Memory: negligible, Time: 2^k encryptions.

1.5 Advanced Cryptanalysis Techniques

An attack is commonly regarded as effective if it is faster than an exhaustive key search.

A trade-off between data, time and/or memory.

- Meet-in-the-middle attack
  - Reflection-meet-in-the-middle attack, Higher-order meet-in-the-middle attack
- Differential cryptanalysis
  - Truncated differential, Higher-order differential, Impossible differential
  - Boomerang, Amplified boomerang, Rectangle attacks, Impossible boomerang
- Linear cryptanalysis
- Differential-linear cryptanalysis
- Integral cryptanalysis
  - Square attack, Saturation attack
- Slide attack, Reflection attack
- Related-key attack
- Algebraic cryptanalysis

1.5.1 Differential Cryptanalysis

- Introduced in 1990 by Biham and Shamir.
- Work in a chosen-plaintext/ciphertext attack scenario.
- Take advantage of how a specific difference in a pair of plaintexts can affect a difference in the pair of ciphertexts (under the same key).
- A differential is the combination of the input difference and the output difference.
- The probability of the differential (α, β) for an *n*-bit block cipher $\mathbb{E}$, written $\Delta\alpha \rightarrow \Delta\beta$, is

$$\Pr_{\mathbb{E}}(\Delta\alpha \rightarrow \Delta\beta) = \Pr_{P \in \{0,1\}^n}(\mathbb{E}(P) \oplus \mathbb{E}(P \oplus \alpha) = \beta).$$

- For a random function, the expected probability of any differential is 2^{-n}.

If $\Pr_{\mathbb{E}}(\Delta\alpha \rightarrow \Delta\beta) > 2^{-n}$, we can use the differential to distinguish $\mathbb{E}$ from a random function.

1.5.2 Related-Key (Differential) Cryptanalysis

- Independently introduced by Knudsen in 1992 and Biham in 1993.
- Different from differential cryptanalysis: The pair of ciphertexts are obtained by encrypting the pair of plaintexts using two different keys with a particular relationship, e.g. certain difference.
- Probability of a related-key differential:

$$\Pr_{\mathbb{E}_K,\mathbb{E}_{K'}}(\Delta\alpha \to \Delta\beta) = \Pr_{P\in\{0,1\}^n}(\mathbb{E}_K(P) \oplus \mathbb{E}_{K'}(P \oplus \alpha) = \beta).$$

- For a random function, the expected probability of any related-key differential is 2^{-n}.

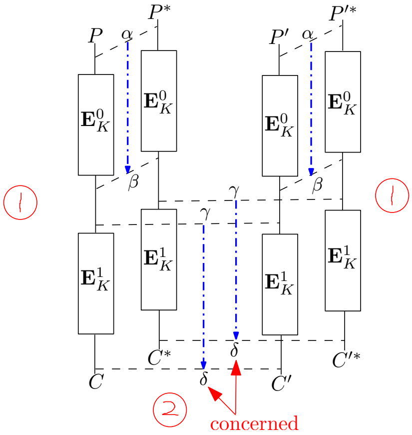
If $\Pr_{\mathbb{E}_K,\mathbb{E}_{K'}}(\Delta\alpha \to \Delta\beta) > 2^{-n}$, we can use the related-key differential to distinguish $\mathbb{E}$ from a random function.

1.5.3 Amplified Boomerang Attack

- Introduced in 2000 by Kelsey, Kohno and Schneier (as a variant of the boomerang attack).
- Work in a chosen-plaintext/ciphertext attack scenario.
- Based on an amplified boomerang distinguisher:
  - Treat a block cipher $\mathbb{E}$ as a cascade of two sub-ciphers $\mathbb{E} = \mathbb{E}^0 \circ \mathbb{E}^1$.
  - Defined to be a pair of differentials $(\Delta\alpha \to \Delta\beta, \Delta\gamma \to \Delta\delta)$:
    - $\Delta\alpha \to \Delta\beta$ for $\mathbb{E}^0$ with probability p;
    - $\Delta\gamma \to \Delta\delta$ for $\mathbb{E}^1$ with probability q.
  - Concerned event: $\mathbb{E}(P) \oplus \mathbb{E}(P') = \delta$ and $\mathbb{E}(P \oplus \alpha) \oplus \mathbb{E}(P' \oplus \alpha) = \delta$
  - Probability: $p^2 q^2 2^{-n}$ approximately (under assumptions).
- For a random function, the expected probability of any amplified boomerang distinguisher is 2^{-2n}.

If $p^2q^2 > 2^{-n}$, we can use the distinguisher to distinguish between $\mathbb{E}$ and a random function.

An Amplified Boomerang Distinguisher

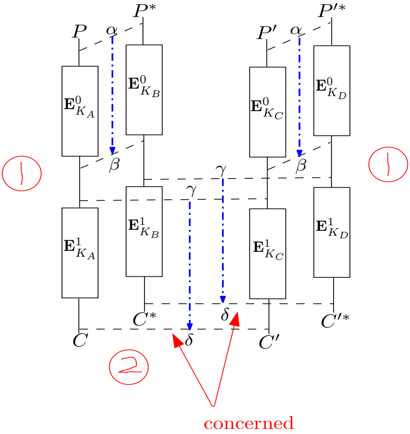


1.5.4 Related-Key Amplified Boomerang Attack

- A combination of the amplified boomerang attack and related-key cryptanalysis.
- Based on a related-key amplified boomerang distinguisher.
  - * Treat a block cipher $\mathbb{E}$ as $\mathbb{E} = \mathbb{E}^0 \circ \mathbb{E}^1$.
  - * Work typically in a related-key attack scenario with four related keys K_A, K_B, K_C, K_D:
    - $K_A \oplus K_B = K_C \oplus K_D$;
    - $K_A \oplus K_C = K_B \oplus K_D$.
  - * Consist of four related-key differentials.
  - * Concerned event: $\mathbb{E}_{K_A}(P) \oplus \mathbb{E}_{K_C}(P') = \delta$ and $\mathbb{E}_{K_B}(P \oplus \alpha) \oplus \mathbb{E}_{K_D}(P' \oplus \alpha) = \delta$.
  - * Probability: $p^2q^2 2^{-n}$ approximately (under assumptions).
- For a random function, the expected probability of any related-key amplified boomerang distinguisher is 2^{-2n}.

If $p^2q^2 > 2^{-n}$, we can use the distinguisher to distinguish between $\mathbb{E}$ and a random function.

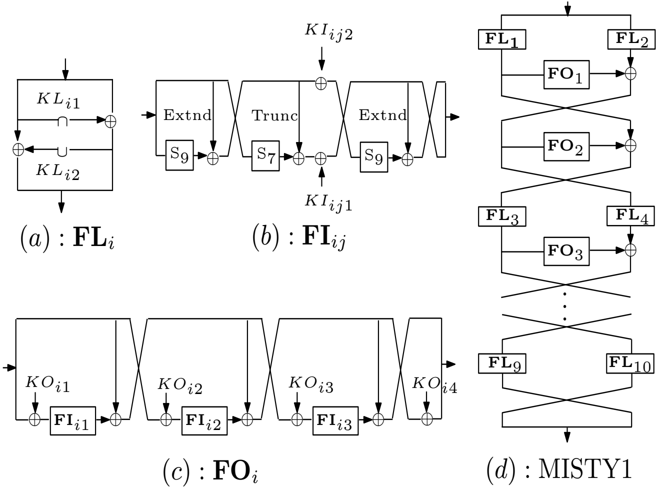
A Related-Key Amplified Boomerang Distinguisher



2.1 Introduction

- Designed by Mitsubishi (Matsui et al.), published in 1995.
- A 64-bit block cipher, a user key of 128 bits, and a recommended number of 8 rounds, with a total of 10 key-dependent logical functions **FL**:
  - two **FL** functions at the beginning;
  - two **FL** functions inserted after every two rounds.
- A Japanese CRYPTREC-recommended e-government cipher, an European NESSIE selected cipher, an ISO international standard.
- Widely used in Mitsubishi products as well as in Japanese military.

2.2 Structure



2.3 Key Schedule

1. Represent a user key 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

$$K'_i = \mathbf{FI}(K_i, K_{i+1}), \text{ for } i = 1, 2, \cdots, 8.$$

3. Subkeys:

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

2.4 Security

- Has been extensively analysed against a variety of cryptanalytic methods.
- No whatever cryptanalytic attack on the full version.

3.1 Related Work

Dai and Chen's related-key differential attack on 8-round MISTY1 with only the last 8 **FL** functions (INSCRYPT 2011).

- A class of 2^{105} weak keys.
  - * A weak key is a user key under which a cipher is more vulnerable to be attacked.
- A 7-round related-key differential characteristic with probability 2^{-60}.
- Attacking the 8-round reduced version under weak keys.
  - * Attack procedure is straightforward, by conducting a key recovery on $\mathbf{FO}_1$ in a way similar to the early abort technique for impossible differential cryptanalysis.
  - * Data complexity: 2^{63} chosen ciphertexts.
  - * Memory complexity: 2^{35} bytes.
  - * Time complexity: $2^{86.6}$ encryptions.

3.1.1 A Class of 2^{105} Weak Keys

Three binary constants:

* 7-bit $a = 0010000$;
* 16-bit $b = 0010000000010000$;
* 16-bit $c = 0010000000000000$.

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

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

Let K'_A, K'_B be the corresponding 128-bit words generated by the key schedule:

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

The class of weak keys is defined to be the set of all possible (K_A, K_B) satisfying the following 10 conditions:

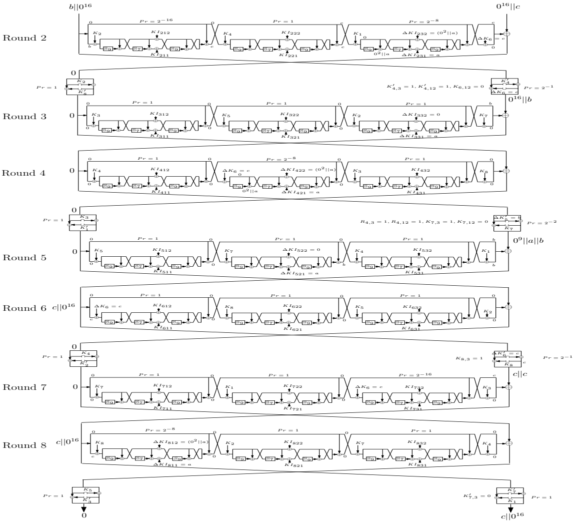
$$K_6 \oplus K_6^* = c, \quad K'_5 \oplus K'^*_5 = b, \quad K'_6 \oplus K'^*_6 = c, \quad K_{6,12} = 0, \quad K_{7,3} = 1,$$
$$K_{7,12} = 0, \quad K_{8,3} = 1, \quad K'_{4,3} = 1, \quad K'_{4,12} = 1, \quad K'_{7,3} = 0.$$

The number:

$$|K_1| = 2^{16}, |K_2| = 2^{16}, |K_3| = 2^{16}, |(K_4, K_5)| = 2^{30}, |(K_6, K_7, K_8)| = 2^{27}.$$

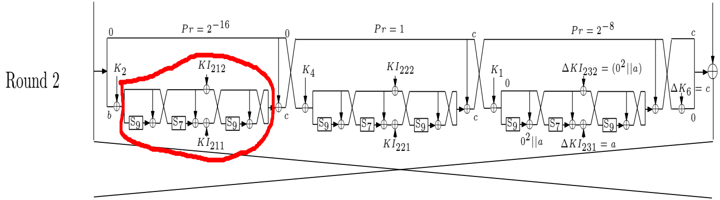
Therefore, a total of 2^{105} weak keys.

3.1.2 A 7-Round Related-Key Differential Characteristic



3.2 A Corrected Class of Weak Keys

Focus on the 7-round related-key differential characteristic.

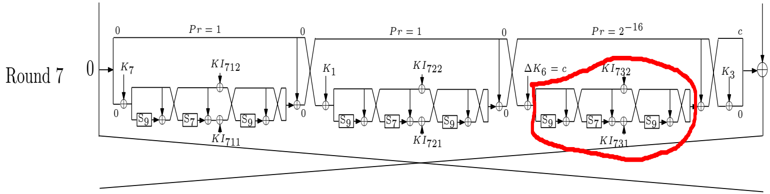


Not all the 2^{15} possible K_7' (i.e. KI_{21}) defined by the weak key class make $\Pr_{\mathbf{FI}_{21}}(\Delta b \to \Delta c) > 0$!

The number of K_7' defined by the weak key class is 2^{15}, the number of K_7' satisfying $\Pr_{\mathbf{FI}_{21}}(\Delta b \to \Delta c) > 0$ is about $2^{14.57}$.

The number of K_7' defined by the weak key class & satisfying $\Pr_{\mathbf{FI}_{21}}(\Delta b \to \Delta c) > 0$ is about $2^{13.57}$.

$\Pr_{\mathbf{FI}_{21}}(\Delta b \to \Delta c) = 2^{-15}/2^{-14}/2^{-13.42}$.



Not all the 2^{16} possible K_2' (i.e. KI_{73}) defined by the weak key class make $\Pr_{\mathbf{FI}_{73}}(\Delta c \to \Delta c) > 0$!

The number of K_2' defined by the weak key class is 2^{16}, the number of K_2' satisfying $\Pr_{\mathbf{FI}_{21}}(\Delta b \to \Delta c) > 0$ is 2^{15}.

The number of K_2' defined by the weak key class & satisfying $\Pr_{\mathbf{FI}_{73}}(\Delta c \to \Delta c) > 0$ is 2^{15}.

$\Pr_{\mathbf{FI}_{73}}(\Delta c \to \Delta c) = 2^{-15}$.

As a result,

- A class of $2^{102.57}$ weak keys:
  $|K_1| = 2^{16}, |(K_2, K_3)| = 2^{31}, |(K_4, K_5)| = 2^{30}, |(K_6, K_7, K_8)| \approx 2^{25.57}$
  - $|K_3| = 2^{16}$, $|K_5| = 2^{16}$.
  - $|K_7'| = 2^{13.57}$; $\forall K_7'$, $\exists\ 2^{12}$ (K_6', K_8).
  - $|K'_{2,8-16}| = 2^8$, $|K_3'| = 2^{16}$, $|K'_{4,8-16}| = 2^8$.
- A 7-round related-key differential with probability 2^{-58}.
  - $(b||0^{32}||c) \rightarrow (0^{32}||c||0^{16})$.

3.3.1 Precomputation

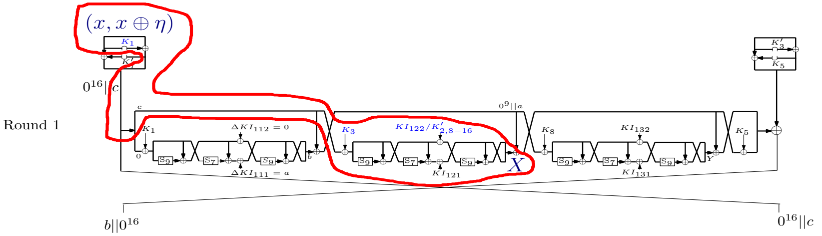
Hash table $\mathcal{T}_1$:

$(x, x \oplus \eta)$: The left halves of a plaintext pair

Only three possible input differences $\eta = \overbrace{00?0000000000000||00?0000000000000}^{32\ bits}$

X: output difference of $\mathbf{FI}_{12}$

Store satisfying $(K_1, K_3, K'_{2,8-16})$ into Table $\mathcal{T}_1$ indexed by (x, η, X)



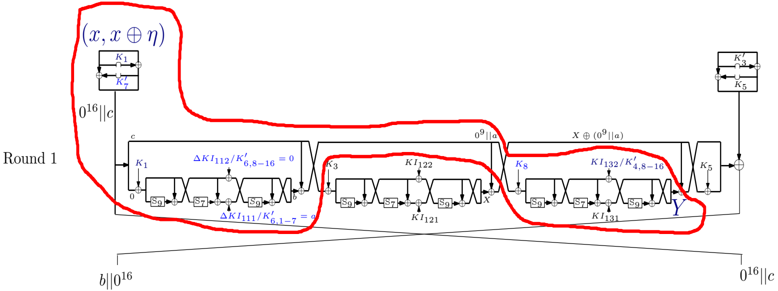
Memory complexity: $2^{75.91}$ bytes; Time complexity: $2^{73.59}$ **FI** computations.

For every (x, η, X), there are 2^{23} satisfying $(K_1, K_3, K'_{2,8-16})$ on average.

Hash table $\mathcal{T}_2$:

Y: output difference of $\mathbf{FI}_{13}$

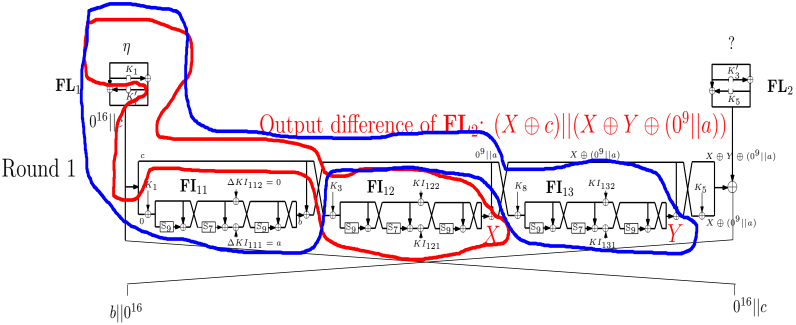
Store satisfying (K_6, K_7, K_8) into Table $\mathcal{T}_2$ indexed by $(x, \eta, Y, K_1, K'_{4,8-16})$



Memory complexity: $2^{84.74}$ bytes; Time complexity: $2^{84.16}$ **FI** computations.

For every $(x, \eta, Y, K_1, K'_{4,8-16})$, there are $2^{9.57}$ satisfying (K_6, K_7, K_8) on average.

3.3.2 Attack Outline



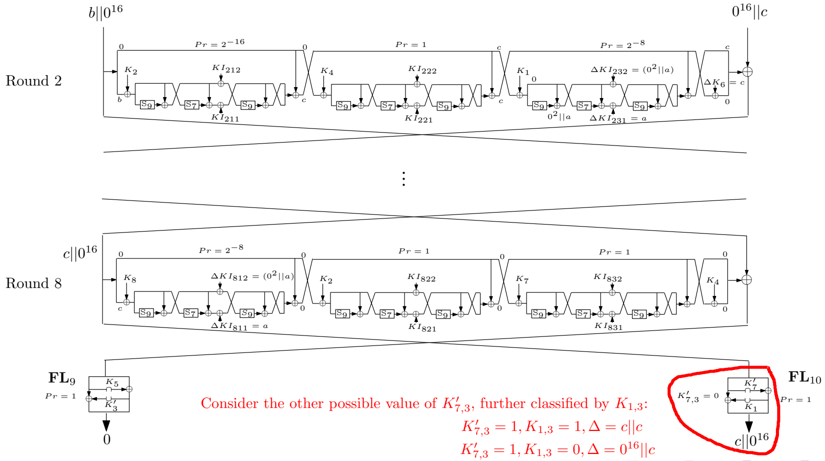
Step 1: Choose 2^{60} ciphertext pairs with difference $(0^{32}||c||0^{16})$.
Step 2: Keep plaintext pairs with difference $(\eta||?)$
Step 3: Focus on $\mathbf{FL}_2$. Guess (K_3', K_5), compute X, Y.
Step 4: Focus on $\mathbf{FL}_1$ and $\mathbf{FI}_{12}$. Obtain satisfying $(K_1, K_3, K'_{2,8-16})$ from Table $\mathcal{T}_1$.
Step 5: Retrieve K_4 from $K_3' = \mathbf{FI}(K_3, K_4)$, compute $K_4' = \mathbf{FI}(K_4, K_5)$.
Step 6: Focus on $\mathbf{FL}_1$, $\mathbf{FI}_{11}$ and $\mathbf{FI}_{13}$. Obtain satisfying (K_6, K_7, K_8) from Table $\mathcal{T}_2$.
Step 7: Increase 1 to counters for $(K_1, K'_{2,8-16}, K_3, K_4, K_5, K_6, K_7, K_8)$.
Step 8: For a subkey guess whose counter number is larger than or equal to 3, exhaustively search the remaining 7 key bits.

3.3.3 Attack Complexity

- Data complexity: 2^{61} chosen ciphertexts.
- Memory complexity: $2^{99.2}$ bytes.
- Time complexity: $2^{87.94}$ encryptions.
- Success probability: 76%.

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

Focus on the 7-round related-key differential characteristic:



Consider the other possible value of $K'_{7,3}$, further classified by $K_{1,3}$:

$K'_{7,3} = 1, K_{1,3} = 1, \Delta = c||c$

$K'_{7,3} = 1, K_{1,3} = 0, \Delta = 0^{16}||c$

4.1 Related Work

Chen and Dai's related-key amplified boomerang attack on 8-round MISTY1 with only the first 8 **FL** functions (CHINACRYPT 2011).

- A class of 2^{90} weak keys.
- A 7-round related-key amplified boomerang distinguisher with probability 2^{-118}.
- Attacking the 8-round reduced version under weak keys.
  * Attack procedure is straightforward, by conducting a key recovery on $\mathbf{FO}_8$ in a way similar to the early abort technique.
  * Data complexity: 2^{63} chosen plaintexts.
  * Memory complexity: 2^{65} bytes.
  * Time complexity: 2^{70} encryptions.

4.1.1 A Class of 2^{90} Weak Keys

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

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

Let K'_A, K'_B, K'_C, K'_D be the corresponding 128-bit words generated by the key schedule:

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

The class of weak keys is defined to be the set of all possible (K_A, K_B, K_C, K_D) satisfying the following 12 conditions:

$$K_2 \oplus K_2^* = c, \quad K_6 \oplus K_6^* = c, \quad K'_1 \oplus K'^*_1 = b, \quad K'_5 \oplus K'^*_5 = b,$$
$$K'_2 \oplus K'^*_2 = c, \quad K'_6 \oplus K'^*_6 = c, \quad K_{5,3} = 1, \quad K_{5,12} = 0,$$
$$K'_{4,3} = 0, \quad K_{7,3} = 1, \quad K_{7,12} = 0, \quad K_{8,3} = 0.$$

The number:

$$|K_1| = 2^{16}, |(K_2, K_3)| = 2^{16}, |(K_4, K_5)| = 2^{29}, |(K_6, K_7)| = 2^{14}, |K_8| = 2^{15}.$$

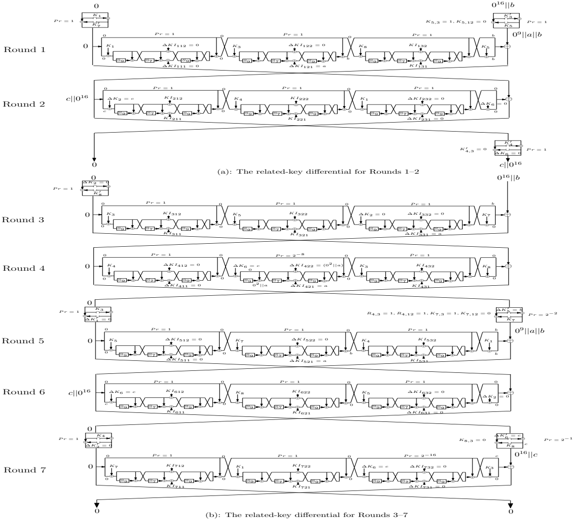
Therefore, a total of 2^{90} weak keys.

4.1.2 A 7-Round Related-Key Amp. Boo. Distinguisher

A 7-round related-key amplified boomerang distinguisher with probability $p^2q^22^{-n} = 1^2 \times (2^{-27})^2 \times 2^{-64} = 2^{-118}$ under weak keys.

* $\mathbb{E}_0$: Rounds 1 –2, including **FL**$_4$ but excluding **FL**$_3$.
* $\mathbb{E}_1$: Rounds 3 –7, including **FL**$_3$ (but excluding **FL**$_4$).
* Related-key differential $\Delta\alpha \rightarrow \Delta\beta$ for $\mathbb{E}_0$: $(0^{48}||b) \rightarrow (0^{32}||c||0^{16})$ with probability 1.
* Related-key differential $\Delta\gamma \rightarrow \Delta\delta$ for $\mathbb{E}_1$: $(0^{48}||b) \rightarrow 0$ with probability 2^{-27}.

The Two Related-Key Differentials Used

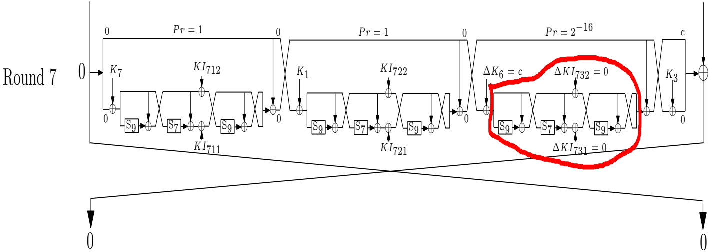


(a): The related-key differential for Rounds 1–2

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

4.2 An Improved 7-Round Distinguisher

Focus on the second related-key differential:



Surprisingly, all the possible $(K_2', K_2'^*)$ (i.e. KI_{73}) defined by the weak key class make $\Pr_{\mathbf{FI}_{73}}(\Delta c \to \Delta c) > 0$!

$\Pr_{\mathbf{FI}_{73}}(\Delta c \to \Delta c) = 2^{-15}$.

Thus, a 7-round related-key amplified boomerang distinguisher with probability 2^{-116}.

4.3.1 Precomputation

Hash table $\mathcal{T}_1$:

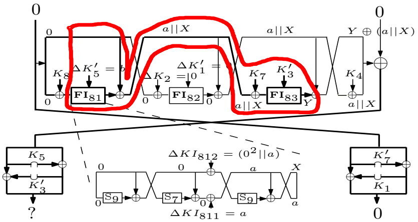
$x \in \{0,1\}^{32}$: Input of $\mathbf{FO}_8$ without K_8.

X: The right 9 bits of the output difference of $\mathbf{FL}_{81}$

Y: Output difference of $\mathbf{FL}_{83}$

Store satisfying x into Table $\mathcal{T}_1$ indexed by (K_3', K_5', K_7, X, Y).

Round 8



Memory complexity: 2^{79} bytes; Time complexity: 2^{71} **FI** computations.

For every (K_3', K_5', K_7, X, Y), there are 2^8 satisfying x on average.

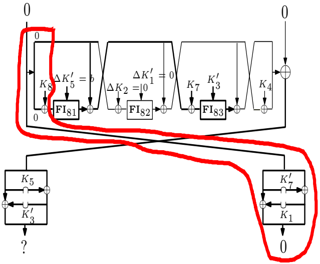
Hash table $\mathcal{T}_2$:

$x \in \{0,1\}^{32}$: Input of $\mathbf{FL}_{10}^{-1}$.

λ: Output of $\mathbf{FL}_{10}^{-1}$ after being xored with $(K_8 || 0^{16})$.

Store (K_1, K_8) into Table $\mathcal{T}_2$ indexed first by K_7 and then by (x, λ).

Round 8

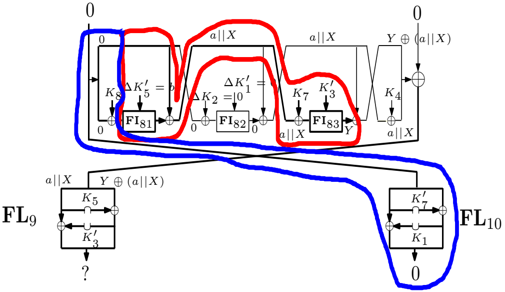


$\mathbf{FL}_{10}$

Memory complexity: 2^{78} bytes; Time complexity: 2^{76} **FL** computations.

Set a binary marker, "up" and "down", to the set of 2^{32} (x, λ) under each (K_7, K_1, K_8).

4.3.2 Attack Outline



Step 1: Choose two sets of $2^{58.5}$ plaintext pairs with difference $(0^{48}||b)$.

Step 2: Keep the quartets such that each ciphertext pair has difference $(?||0)$.

Step 3: Focus on $\mathbf{FL}_9$. Guess K'_3, keep the quartets such that each pair has 7-bit difference a.

Step 4: Focus on $\mathbf{FL}_9$. Guess K_5, compute (X, Y) and (X^*, Y^*).

Step 5: Guess K_7, get the two possible values for K_6, and compute K'_5.

Step 6: Focus on $\mathbf{FI}_{81}$ and $\mathbf{FI}_{83}$. Obtain possible inputs to $\mathbf{FO}_8$ excluding XOR with K_8 from Table $\mathcal{T}_1$.

Step 7: Focus on $\mathbf{FL}_{10}$. Obtain (K_1, K_8) from Table $\mathcal{T}_2$.

Step 8: For a subkey guess whose counter is non-zero, exhaustively search the remaining key bits.

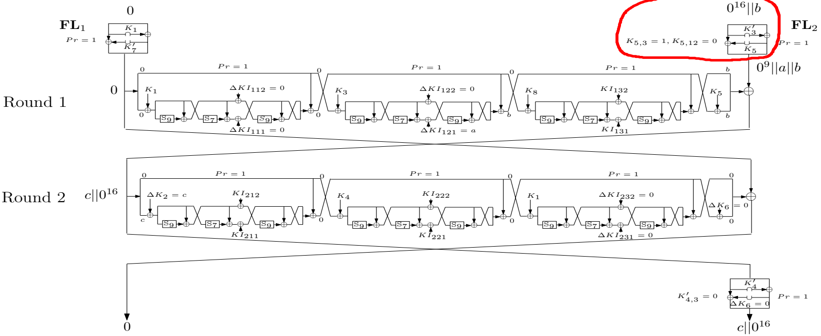
4.3.3 Attack Complexity

- Data complexity: $2^{60.5}$ chosen plaintexts.
- Memory complexity: $2^{80.07}$ bytes.
  * On-line: $2^{78.23}$;
  * Off-line: $2^{79.58}$.
- Time complexity: $2^{80.18}$ encryptions.
- Success probability: 86%.

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

Focus on the first related-key differential:

Consider the three other possible combinations of $(K_{5,3}, K_{5,12})$, further classified by $(K'_{3,3}, K'_{3,12})$



Thus, a total of 2^{92} weak keys.

5. Conclusions

Have presented related-key differential and amplified boomerang attacks on the full MISTY1 algorithm under certain weak key assumptions.

* Have described $2^{103.57}$ weak keys for a related-key differential attack on the full MISTY1.
* Have described 2^{92} weak keys for a related-key amplified boomerang attack on the full MISTY1.
* Quite theoretical, for the attacks work under the assumptions of weak-key and related-key scenarios and their complexities are very high.

The MISTY1 cipher does not behave like a random function (in the related-key model), and cannot be regarded to be an ideal cipher.

Summary of Main Cryptanalytic Results

#Rounds	FL	#Keys	Attack Type	Data	Time	Year
6 (1 – 6)	yes	2^{128}	Impossible differential	2^{51}CP	$2^{123.4}$Enc.	2008
6 (1 – 6)	yes	2^{128}	Higher-order differential	$2^{53.7}$CP	$2^{64.4}$Enc.	2008
6 (3 – 8)	yes	2^{128}	Integral	2^{32}CC	$2^{126.1}$Enc.	2009
7 (1 – 7)	yes	2^{128}	Higher-order differential	$2^{54.1}$CP	$2^{120.7}$Enc.	2008
$7^{\dagger}$ (2 – 8)	yes	2^{73}	Related-key amplified boomerang	2^{54}CP	$2^{55.3}$Enc.	2008
$8^{\dagger}$ (1 – 8)	yes	2^{90}	Related-key amplified boomerang	2^{63}CP	2^{70}Enc.	2011
$8^{\dagger}$ (1 – 8)	yes	$2^{105\ddagger}$	Related-key differential	2^{63}CC	$2^{86.6}$Enc.	2011
full	yes	$2^{103.57}$	Related-key differential	2^{61}CC	$2^{87.94}$Enc.	2012
		2^{92}	Related-key amplified boomerang	$2^{60.5}$CP	$2^{80.18}$Enc.	2012

CP: Chosen Plaintexts, CC: Chosen Ciphertexts, Enc.: Encryptions,

†: Exclude the first/last layer of two FL functions, ‡: There is a flaw.

Thank you!

Questions or Comments?