The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher

Jiqiang Lu

Presenter: Matt Henrickson

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

Joint work with Y. Wei, J. Kim and E. Pasalic.

INDOCRYPT 2012

Outline:

1.1 Introduction

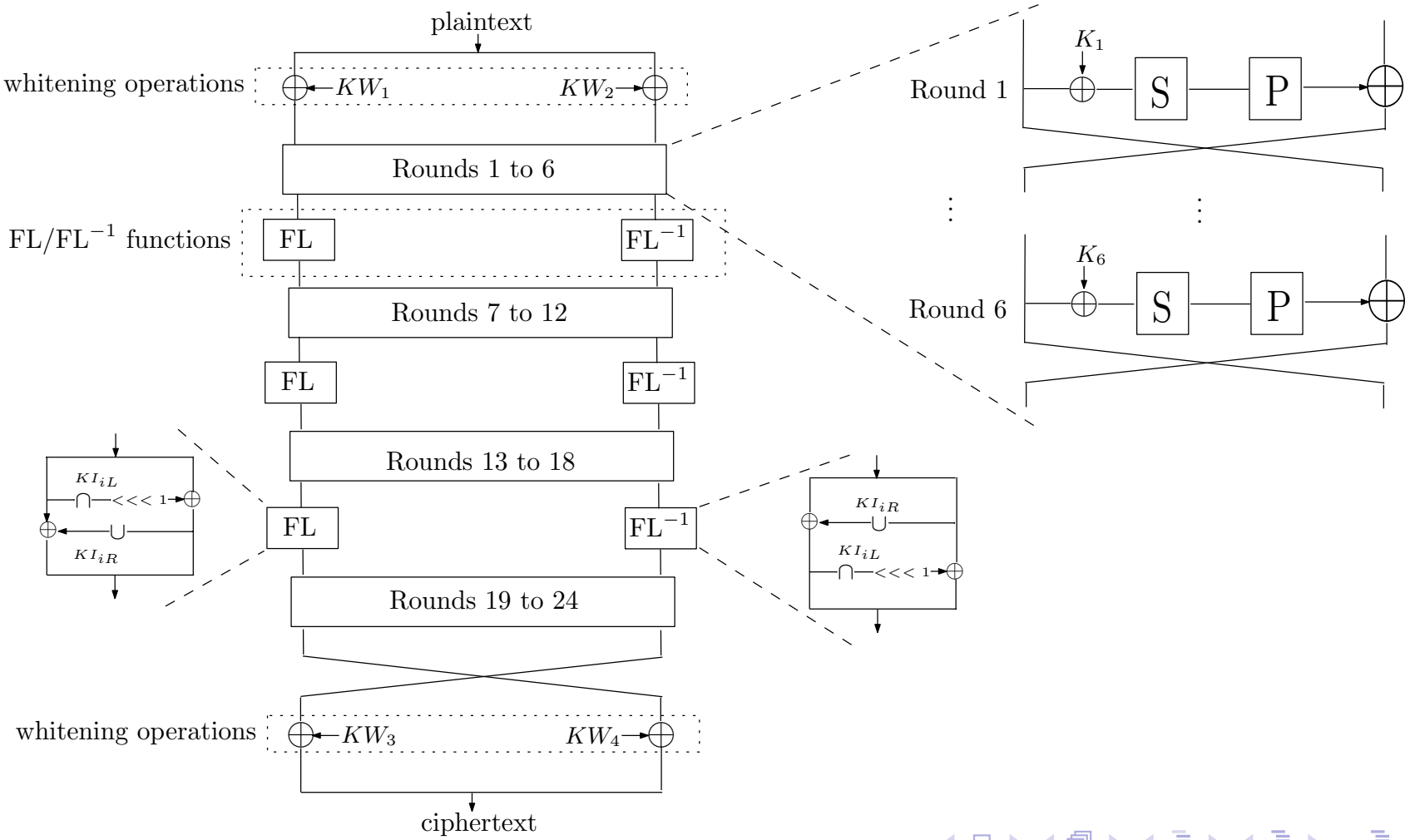
Block cipher:

- An important primitive in symmetric-key cryptography.
- Main purpose: provide data confidentiality.

The Camellia block cipher:

- Designed by NTT and Mitsubishi in 2000.
- Has a 128-bit block size, a user key of 128, 192 or 256 bits.
- Has 18 rounds for a 128-bit key, 24 rounds for a 192/256-bit key.
- Is a Japanese CRYPTREC-recommended e-government cipher.
- Is a European NESSIE selected algorithm.
- Is an ISO international standard.

1.2 Structure



1.3 Security

Has been analysed against a variety of cryptanalytic techniques:

- Differential cryptanalysis.
- Truncated differential cryptanalysis.
- Higher-order differential cryptanalysis.
- Impossible differential cryptanalysis.
- Linear cryptanalysis.
- Square/integral cryptanalysis.
- Boomerang/rectangle attacks.

In terms of the numbers of attacked rounds, the most efficient technique is impossible differential cryptanalysis, that broke

- Camellia with FL/FL^{-1} functions: 11-round Camellia-128, 12-round Camellia-192 and 14-round Camellia-256.
- Camellia without FL/FL^{-1} functions: 12-round Camellia-128, 14-round Camellia-192 and 16-round Camellia-256.

2.1 Introduction

Exhaustive key search (or brute force search) attack:

- Try every possible key K, given a known plaintext-ciphertext pair (P, C). The correct key should yield the correct correspondence: $\mathbf{E}_K(P) \stackrel{?}{\rightarrow} C$.
- Data and Memory complexity: negligible; Time complexity: 2^k encryptions.

A cryptanalytic attack is commonly regarded as effective if it is faster than exhaustive key search.

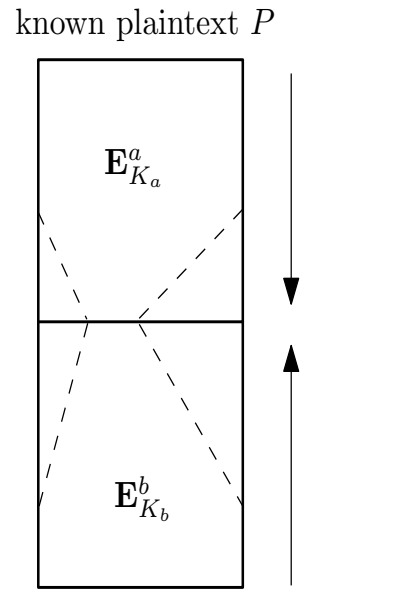
Meet-in-the-middle (MitM) attack:

- A semi-advanced cryptanalysis technique, a data/memory/time tradeoff to exhaustive key search.
- First introduced in 1977 by Diffie and Hellman for analysing a block cipher in a known-plaintext attack scenario.
- Was used later in a chosen-plaintext attack scenario.

2.2 MitM Attack in Known-Plaintext Scenario

Consider a block cipher with a $2k$-bit key: $\mathbf{E}_K = \mathbf{E}^b_{K_b}(\mathbf{E}^a_{K_a}(\cdot))$.

- An exhaustive key search takes 2^{2k} encryptions.



Offline Precomputation Phase

K_a	0	1	$\cdots$	$2^k - 1$
$\mathbf{E}^a_{K_a}(P)$	$\star$	$\star$	$\cdots$	$\star$

Sorted by $\mathbf{E}^a_{K_a}(P)$.

The value-in-the-middle can be truncated.

Memory complexity: 2^k; Time complexity: 2^k encryptions of $\mathbf{E}^a$.

Online Attack Phase

1. Guess K_b, compute $(\mathbf{E}^b_{K_b})^{-1}(C)$;
2. Check whether $(\mathbf{E}^b_{K_b})^{-1}(C)$ exists in the precomputation table;
   If yes, the guessed K_b and the corresponding K_a are probably correct.

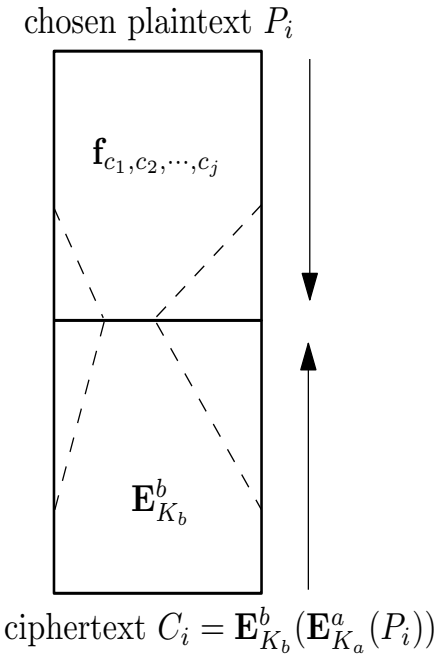
Memory complexity: negligible; Time complexity: 2^k decryptions of $\mathbf{E}^b$.

Total time complexity: $2^k + 2^k = 2^{k+1} < 2^{2k}$, faster than exhaustive key search.

2.3 MitM Attack in Chosen-Plaintext Scenario

Take a set of N chosen plaintexts P_i with a particular property.

- E.g. one byte fixed, and the other bytes taking all possible values.
- The concerned value-in-the-middle may be expressed as a function of a smaller number of unknown bits than the number of bits from K_a, say $\mathbf{f}_{c_1,c_2,\cdots,c_j}(P_i)$.



Offline Precomputation Phase

$(c_1, c_2, \cdots, c_j)$	0	1	$\cdots$	$2^j - 1$
$(\mathbf{f}_{c_1,c_2,\cdots,c_j}(P_1), \cdots, \mathbf{f}_{c_1,c_2,\cdots,c_j}(P_N))$	$(\star_1, \cdots, \star_N)$	$(\star_1, \cdots, \star_N)$	$\cdots$	$(\star_1, \cdots, \star_N)$

Memory complexity: $N \times 2^j$; Time complexity: $N \times 2^j$ computations of $\mathbf{f}$.

Online Attack Phase

1. Guess K_b, compute $((\mathbf{E}^b_{K_b})^{-1}(C_1), \cdots, (\mathbf{E}^b_{K_b})^{-1}(C_N))$;
2. Check whether $((\mathbf{E}^b_{K_b})^{-1}(C_1), \cdots, (\mathbf{E}^b_{K_b})^{-1}(C_N))$ exists in the precomputation table; If yes, the guessed K_b is probably correct.

Memory complexity: negligible; Time complexity: $N \times 2^k$ decryptions of $\mathbf{E}^b$.

Thus, if $N \times 2^j + N \times 2^k < 2^{2k}$, faster than exhaustive key search.

3. Higher-Order Meet-in-the-Middle Attack

MitM attack: A basic unit of value-in-the-middle is obtained from a plaintext.

- $\mathbf{E}^a_{K_a}(P)$ in a known-plaintext attack scenario;
- $\mathbf{f}_{c_1,c_2,\cdots,c_j}(P_i)$ in a chosen-plaintext attack scenario.

Higher-order meet-in-the-middle (HO-MitM) attack: A basic unit of value-in-the-middle is obtained from multiple plaintexts.

- $\mathbf{f}(E^a_{K^*_a}(P_1),\cdots,E^a_{K^*_a}(P_t)) = \mathbf{f}((E^b_{K^*_b})^{-1}(C_1),\cdots,(E^b_{K^*_b})^{-1}(C_t))$, for some function $\mathbf{f}$ that has a distinguishing property.
- The core is to cancel some key-dependent/unknown component(s) or parameter(s) when constructing a basic unit of value-in-the-middle.

HO-MitM attacks with a basic input unit of two plaintexts are not novel and have appeared under the name of MitM attacks.

- Use a general differential property to cancel some constant parameters.

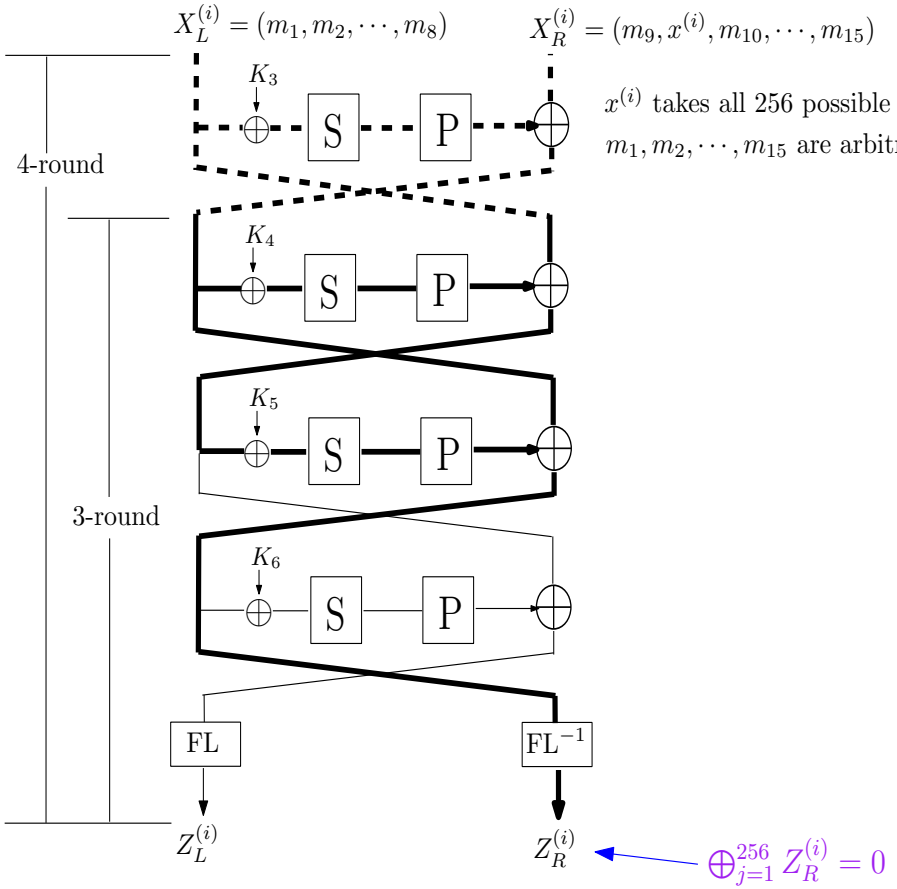
HO-MitM properties for 5 and 6-round Camellia with FL/FL^{-1} functions, where a basic unit of value-in-the-middle is obtained from 256 plaintexts:

- Cancel key-dependent component $\mathbf{FL}^{-1}(\cdot, KI)$ by using a 3 or 4-round integral property of Camellia.
- An alias: the integral-meet-in-the-middle attack.

4.1 3 and 4-Round Integral Properties with FL/FL^{-1}

Take 256 inputs $X^{(i)} = (m_1, m_2, \cdots, m_8, m_9, x^{(i)}, m_{10}, \cdots, m_{15})$.

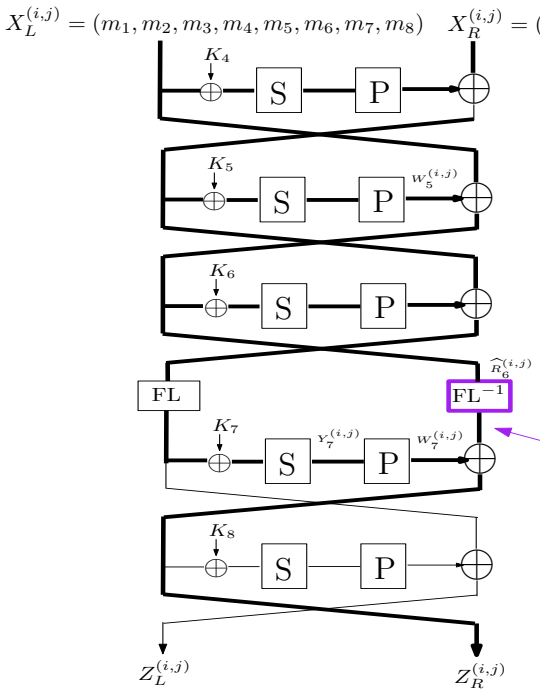
Previously known, published in 2003.



$x^{(i)}$ takes all 256 possible values;
$m_1, m_2, \cdots, m_{15}$ are arbitray but fixed constants.

4.2 5-Round HO-MitM Property with FL/FL^{-1}

Take 256 inputs $X^{(i,j)} = (m_1, m_2, \cdots, m_8, x^{(i)}, y^{(j)}, m_{10}, \cdots, m_{14})$.



$x^{(i)} \in [0, 255]$;
$y^{(j)}$ takes all 256 possible values;
$m_1, m_2, \cdots, m_{14}$ are arbitray but fixed constants.

$$Z_R^{(i,j)} = \mathbf{FL}^{-1}(X_L^{(i,j)} \oplus W_5^{(i,j)}, KI_2) \oplus W_7^{(i,j)}$$
$$\Rightarrow \mathbf{P}^{-1}(Z_R^{(i,j)}) = \mathbf{P}^{-1}(\mathbf{FL}^{-1}(X_L^{(i,j)} \oplus W_5^{(i,j)}, KI_2)) \oplus Y_7^{(i,j)}$$

$\sum_{j=1}^{256} = 0$

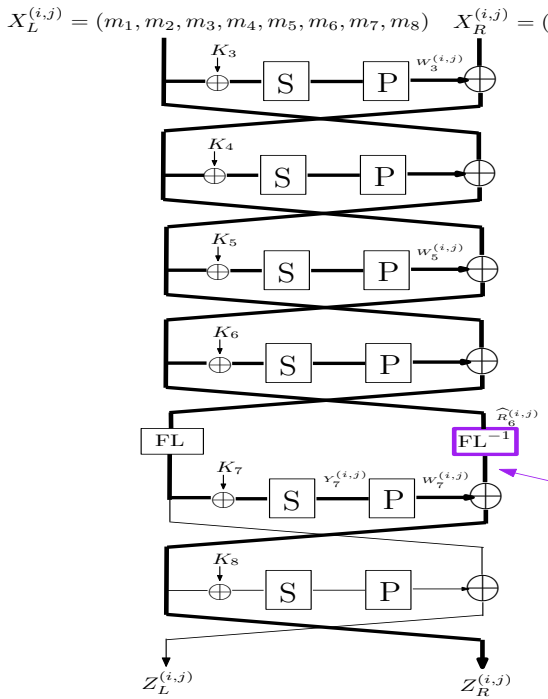
$$\oplus_{j=1}^{256} \mathbf{P}^{-1}(Z_R^{(i,j)})$$
$$= (\oplus_{j=1}^{256} \mathbf{P}^{-1}(\mathbf{FL}^{-1}(X_L^{(i,j)} \oplus W_5^{(i,j)}, KI_2))) \oplus (\oplus_{j=1}^{256} Y_7^{(i,j)})$$
$$= (\oplus_{j=1}^{256} \mathbf{P}^{-1}(\mathbf{FL}^{-1}(\widehat{R}_6^{(i,j)}, KI_2))) \oplus (\oplus_{j=1}^{256} Y_7^{(i,j)})$$
$$= \oplus_{j=1}^{256} Y_7^{(i,j)}$$

Cancel $\oplus_{j=1}^{256} \mathbf{P}^{-1}(\mathbf{FL}^{-1}(\widehat{R}_6^{(i,j)}, KI_2)))$

Then, Byte 7 of $\mathbf{P}^{-1}(\bigoplus_{j=1}^{256} Z_R^{(i,j)})$ can be expressed with a function of $x^{(i)}$ and 13 constant 8-bit parameters.

4.3 6-Round HO-MitM Property with FL/FL^{-1}

Take 256 inputs $X^{(i,j)} = (m_1, m_2, \cdots, m_8, x^{(i)}, y^{(j)}, m_{10}, \cdots, m_{14})$.



$x^{(i)} \in [0, 255]$;
$y^{(j)}$ takes all 256 possible values;
$m_1, m_2, \cdots, m_{14}$ are arbitray but fixed constants.

$$Z_R^{(i,j)} = \mathbf{FL}^{-1}(X_R^{(i,j)} \oplus W_3^{(i,j)} \oplus W_5^{(i,j)}, KI_2) \oplus W_7^{(i,j)}$$
$$\Rightarrow \mathbf{P}^{-1}(Z_R^{(i,j)}) = \mathbf{P}^{-1}(\mathbf{FL}^{-1}(X_R^{(i,j)} \oplus W_3^{(i,j)} \oplus W_5^{(i,j)}, KI_2)) \oplus Y_7^{(i,j)}$$

$\sum_{j=1}^{256} = 0$

$$\begin{aligned}
&\oplus_{j=1}^{256} \mathbf{P}^{-1}(Z_R^{(i,j)}) \\
&= (\oplus_{j=1}^{256} \mathbf{P}^{-1}(\mathbf{FL}^{-1}(X_R^{(i,j)} \oplus W_3^{(i,j)} \oplus W_5^{(i,j)}, KI_2))) \oplus (\oplus_{j=1}^{256} Y_7^{(i,j)}) \\
&= (\oplus_{j=1}^{256} \mathbf{P}^{-1}(\mathbf{FL}^{-1}(\widehat{R}_6^{(i,j)}, KI_2))) \oplus (\oplus_{j=1}^{256} Y_7^{(i,j)}) \\
&= \oplus_{j=1}^{256} Y_7^{(i,j)}
\end{aligned}$$

Cancel $\oplus_{j=1}^{256} \mathbf{P}^{-1}(\mathbf{FL}^{-1}(\widehat{R}_6^{(i,j)}, KI_2)))$

Then, Byte 6 of $\mathbf{P}^{-1}(\bigoplus_{j=1}^{256} Z_R^{(i,j)})$ can be expressed with a function of $x^{(i)}$ and 21 constant 8-bit parameters.

4.4 Cryptanalytic Results

The 5-round HO-MitM property with FL/FL^{-1} can be used to break 10-round Camellia-128 with FL/FL^{-1}:

* Data complexity: 2^{93} chosen plaintexts.
* Memory complexity: 2^{109} bytes.
* Time complexity: $2^{118.6}$ 10-round Camellia-128 encryptions.

The 6-round HO-MitM property with FL/FL^{-1} can be used to:

- break 11-round Camellia-192 with FL/FL^{-1};
  * Data complexity: 2^{94} chosen plaintexts.
  * Memory complexity: 2^{174} bytes.
  * Time complexity: $2^{180.2}$ 11-round Camellia-192 encryptions.
- break 12-round Camellia-256 with FL/FL^{-1}.
  * Data complexity: 2^{94} chosen plaintexts.
  * Memory complexity: 2^{174} bytes.
  * Time complexity: $2^{237.3}$ 12-round Camellia-256 encryptions.

4.5.1 A Comparison

Let $X^{(i)} = (m_1, m_2, \cdots, m_8, x^{(i)}, m_9, m_{10}, \cdots, m_{15})$.

- Corresponding 5-round MitM property:
  Byte 7 of $\mathbf{P}^{-1}(Z_R^{(i)})$ can be expressed with a function of $x^{(i)}$ and 198 constant 1-bit parameters.
  * Cannot be used to break 10-round Camellia-128 with FL/FL^{-1}.

- Corresponding 6-round MitM property:
  Byte 6 of $\mathbf{P}^{-1}(Z_R^{(i)})$ can be expressed with a function of $x^{(i)}$ and 264 constant 1-bit parameters.
  * Cannot be used to break 11-round Camellia-192 with FL/FL^{-1}.
  * Can be used to break 12-round Camellia-256 with FL/FL^{-1} by taking advantage of a data-memory-time tradeoff.

4.5.2 Note 1

5 and 6-round HO-MitM properties obtained from the above 5 and 6-round MitM properties by taking XOR between two inputs to cancel some constant parameters:

- Corresponding 5-round HO-MitM property: Byte 7 of $\mathbf{P}^{-1}(Z_R^{(i_1)} \oplus Z_R^{(i_2)})$ can be expressed with a function of $x^{(i_1)}, x^{(i_2)}$ and 127 constant 1-bit parameters.
- Corresponding 6-round HO-MitM property: Byte 6 of $\mathbf{P}^{-1}(Z_R^{(i_1)} \oplus Z_R^{(i_2)})$ can be expressed with a function of $x^{(i_1)}, x^{(i_2)}$ and 199 constant 1-bit parameters.

Cryptanalytic results:

* Can be used to marginally break 10-round Camellia-128 with FL/FL^{-1} by taking advantage of a data-memory-time tradeoff.
* Can be used to break 11-round Camellia-192 with FL/FL^{-1}.
* Can be used to break 12-round Camellia-256 with FL/FL^{-1}.

4.5.2 Note 2

5 and 6-round MitM properties obtained from the above 5 and 6-round MitM properties by considering only a smaller number of bits of the concerned byte, instead of the whole 8 bits:

- A 5-round MitM property: Bit 49 of $\mathbf{P}^{-1}(Z_R^{(i)})$ can be expressed with a function of $x^{(i)}$ and 100 constant 1-bit parameters.
- A 6-round MitM property: Bits (41,42) of $\mathbf{P}^{-1}(Z_R^{(i)})$ can be expressed with a function of $x^{(i)}$ and 179 constant 1-bit parameters.

Cryptanalytic results:

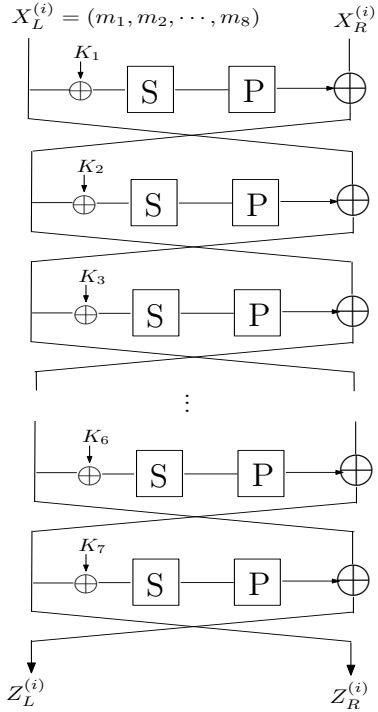
* Can be used to break 10-round Camellia-128 with FL/FL^{-1}.
* Can be used to break 11-round Camellia-192 with FL/FL^{-1} and whitening operations.
* Can be used to break 12-round Camellia-256 with FL/FL^{-1} and whitening operations.

HO-MitM properties for 7 and 8-round Camellia without FL/FL^{-1} functions, where a basic unit of value-in-the-middle is obtained from 2 plaintexts:

- Cancel several unknown parameters by using a general differential property.
- Such HO-MitM attacks are not novel, have appeared under the name of MitM attacks.

5.1 7-Round HO-MitM Property without FL/FL^{-1}

Take 256 inputs $X^{(i)} = (m_1, m_2, \cdots, m_8, x^{(i)}, m_9, m_{10}, \cdots, m_{15})$.

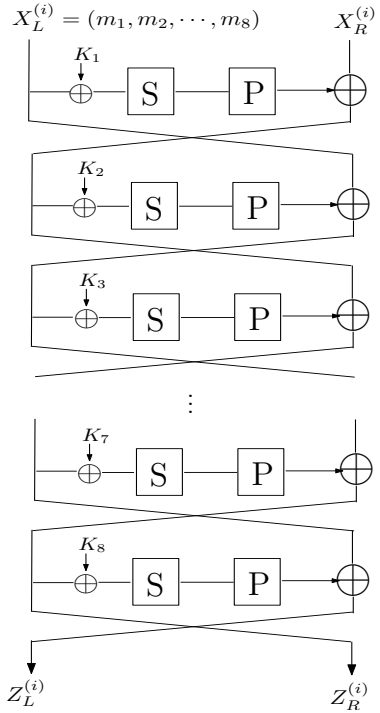


$x^{(i)} \in [0, 255]$
$m_1, m_2, \cdots, m_{15}$ are arbitray but fixed constants.

Then, Byte 6 of $\mathbf{P}^{-1}(Z_R^{(i_1)} \oplus Z_R^{(i_2)})$ can be expressed with a function of $x^{(i_1)}, x^{(i_2)}$ and 20 constant 8-bit parameters, where $x^{(i_1)}, x^{(i_2)} \in [0, 255]$.

5.2 8-Round HO-MitM Property without FL/FL^{-1}

Take 256 inputs $X^{(i)} = (m_1, m_2, \cdots, m_8, x^{(i)}, m_9, m_{10}, \cdots, m_{15})$.



$x^{(i)} \in [0, 255]$;
$m_1, m_2, \cdots, m_{15}$ are arbitray but fixed constants.

Then, Byte 6 of $\mathbf{P}^{-1}(Z_R^{(i_1)} \oplus Z_R^{(i_2)})$ can be expressed with a function of $x^{(i_1)}, x^{(i_2)}$ and 28 constant 8-bit parameters, where $x^{(i_1)}, x^{(i_2)} \in [0, 255]$.

5.3 Cryptanalytic Results

The 7-round HO-MitM property without FL/FL^{-1} can be used to break 14-round Camellia-192 without FL/FL^{-1}:

* Data complexity: 2^{118} chosen plaintexts.
* Memory complexity: 2^{166} bytes.
* Time complexity: $2^{164.6}$ 14-round Camellia-192 encryptions.

The 8-round HO-MitM property without FL/FL^{-1} can be used to break 16-round Camellia-256 without FL/FL^{-1}:

* Data complexity: 2^{120} chosen plaintexts.
* Memory complexity: 2^{230} bytes.
* Time complexity: 2^{252} 16-round Camellia-256 encryptions.

5.4 A Comparison

- Corresponding 7-round MitM property:
  Byte 6 of $\mathbf{P}^{-1}(X_L^{(i)} \oplus Z_R^{(i)})$ can be expressed with a function of $x^{(i)}$ and 21 constant 8-bit parameters.
  - Can be used to break 14-round Camellia-192 without FL/FL^{-1} at larger memory and time complexities.

- Corresponding 8-round MitM property:
  Byte 6 of $\mathbf{P}^{-1}(X_R^{(i)} \oplus Z_R^{(i)})$ can be expressed with a function of $x^{(i)}$ and 30 constant 8-bit parameters.
  - Can be used to break 16-round Camellia-256 without FL/FL^{-1} at a larger memory complexity.

6. Concluding Remarks

- Have proposed an extension of the meet-in-the-middle (MitM) attack — the higher-order meet-in-the-middle (HO-MitM) attack.
  - The core is to use multiple plaintexts to cancel some key-dependent parameters when constructing a basic unit of value-in-the-middle.
- By combining integral cryptanalysis with the MitM attack, have introduced a novel approach to construct HO-MitM attacks on 10-round Camellia-128 with FL/FL^{-1}, 11-round Camellia-192 with FL/FL^{-1} and 12-round Camellia-256 with FL/FL^{-1}.
  - One or two rounds inferior to the newly emerging best results.
- Have used an existing approach to construct HO-MitM attacks on 14-round Camellia-192 without FL/FL^{-1} and 16-round Camellia-256 without FL/FL^{-1}.
  - Match the best previously known results.