上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia

Ya Liu[1], Leibo Li[2], Dawu Gu[1], Xiaoyun Wang[2,3],

Zhiqiang Liu[1], Jiazhe Chen[2], Wei Li[4]

1. Shanghai Jiao Tong University, 2. Shangdong University

3. Tsinghua University, 4.Donghua University

FSE 2012

Mar. 19 , 2012

LoCCS

Outline

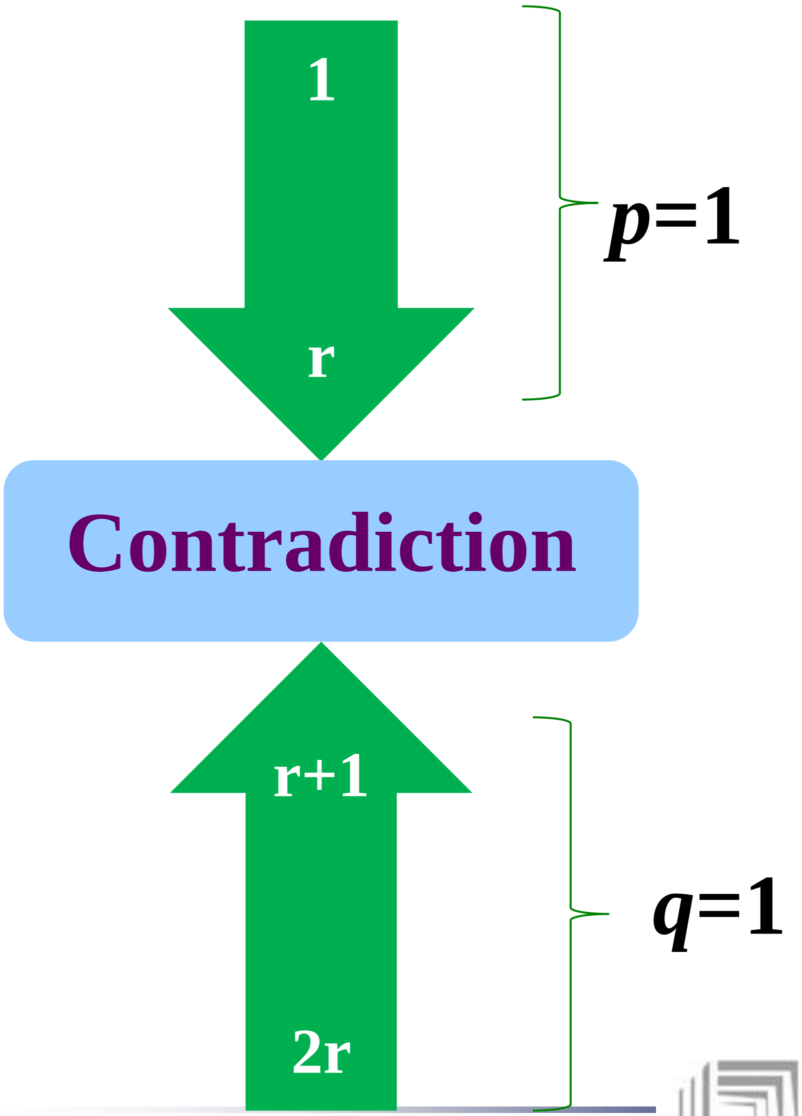
- **Impossible Differential Cryptanalysis**
- **The Block Cipher Camellia**
- **Our Results**
  - **7-Round Impossible Differentials of Camellia for Weak Keys and Their Applications (***By Leibo Li, Xiaoyun Wang, Jiazhe Chen***)**
  - **8-Round Impossible Differentials of Camellia and Their Applications (**By *Ya Liu, Dawu Gu, Zhiqiang Liu, Wei Li***)**
- **Conclusion**

Impossible Differential Cryptanalysis (1/2)

- **Impossible differential attack was independently proposed by Knudsen and Biham.**
  - L.R. Knudsen: *DEAL – A 128-bit Block Cipher*, AES Proposal, 1998
  - E. Biham, A. Biryukov and A. Shamir: *Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials* (EUROCRYPT 99)

Impossible Differential Cryptanalysis (2/2)

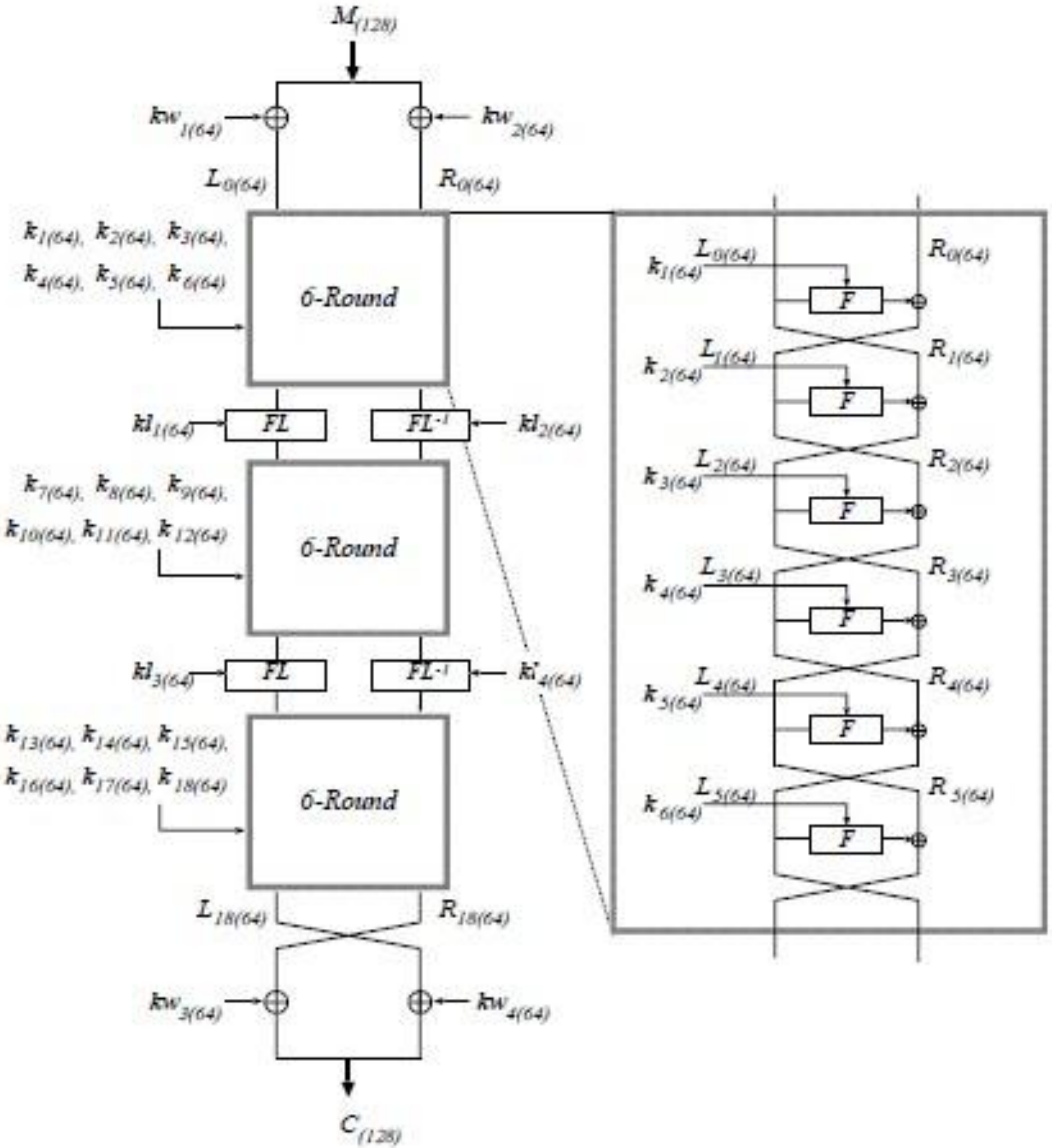
- **Basic ideas:** *Impossible differential attack uses differentials that hold with probability zero to derive the right key by discarding the wrong keys which lead to the impossible differential.*
- Some block ciphers were analyzed by using impossible differentials: *ARIA*, *AES*, *CLEFIA*, *MISTY1*…



Camellia (1/3)

- K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita. *Camellia: A 128-bit Block Cipher Suitable for Multiple Platforms-Design and Analysis* (SAC 2000)
- In 2002, Camellia was selected an e-government recommended cipher by **CRYPTREC**.
- In 2003, Camellia was recommended in **NESSIE** block cipher portfolio.
- In 2005, Camellia was adopted as an **ISO/IEC** international standard.
- Basic Information
  - **Block Size:** 128 bits
  - **Key Sizes:** 128/192/256 (Camellia-128/192/256)
  - **The Number of Rounds:** 18/24
  - **Structure:** Feistel structure with some key-dependent functions FL/FL^{-1} inserted every 6 rounds.

Encryption Procedure of Camellia(2/3)



Property of FL/FL^{-1} (3/3)

- Key-dependent Functions: FL/FL^{-1}

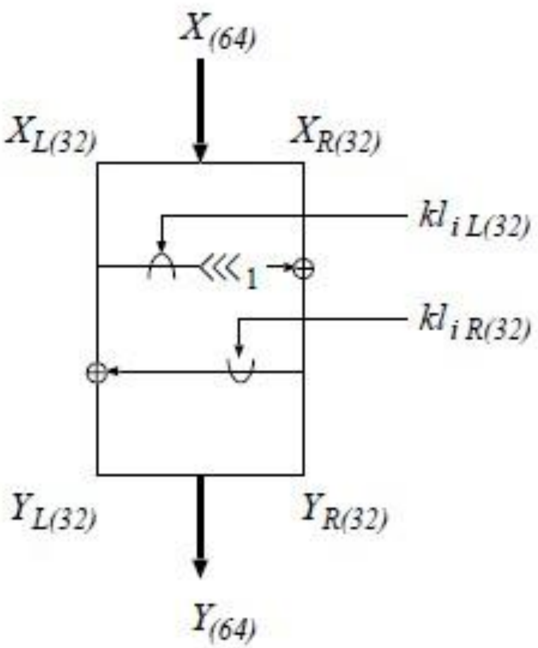


Fig. 4. *FL*-function

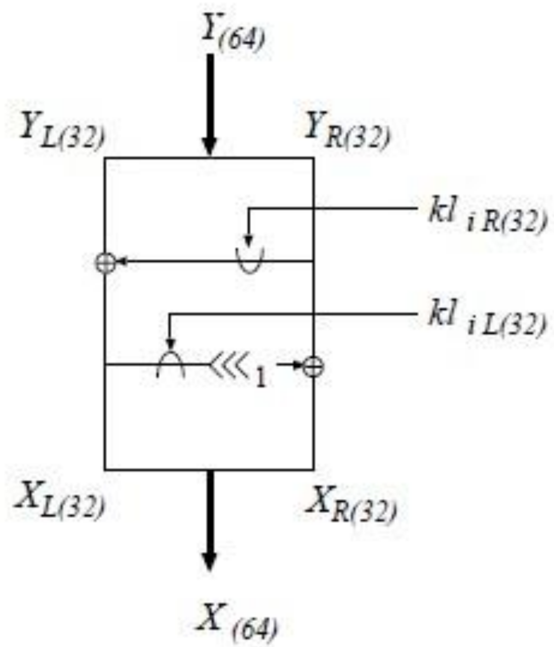
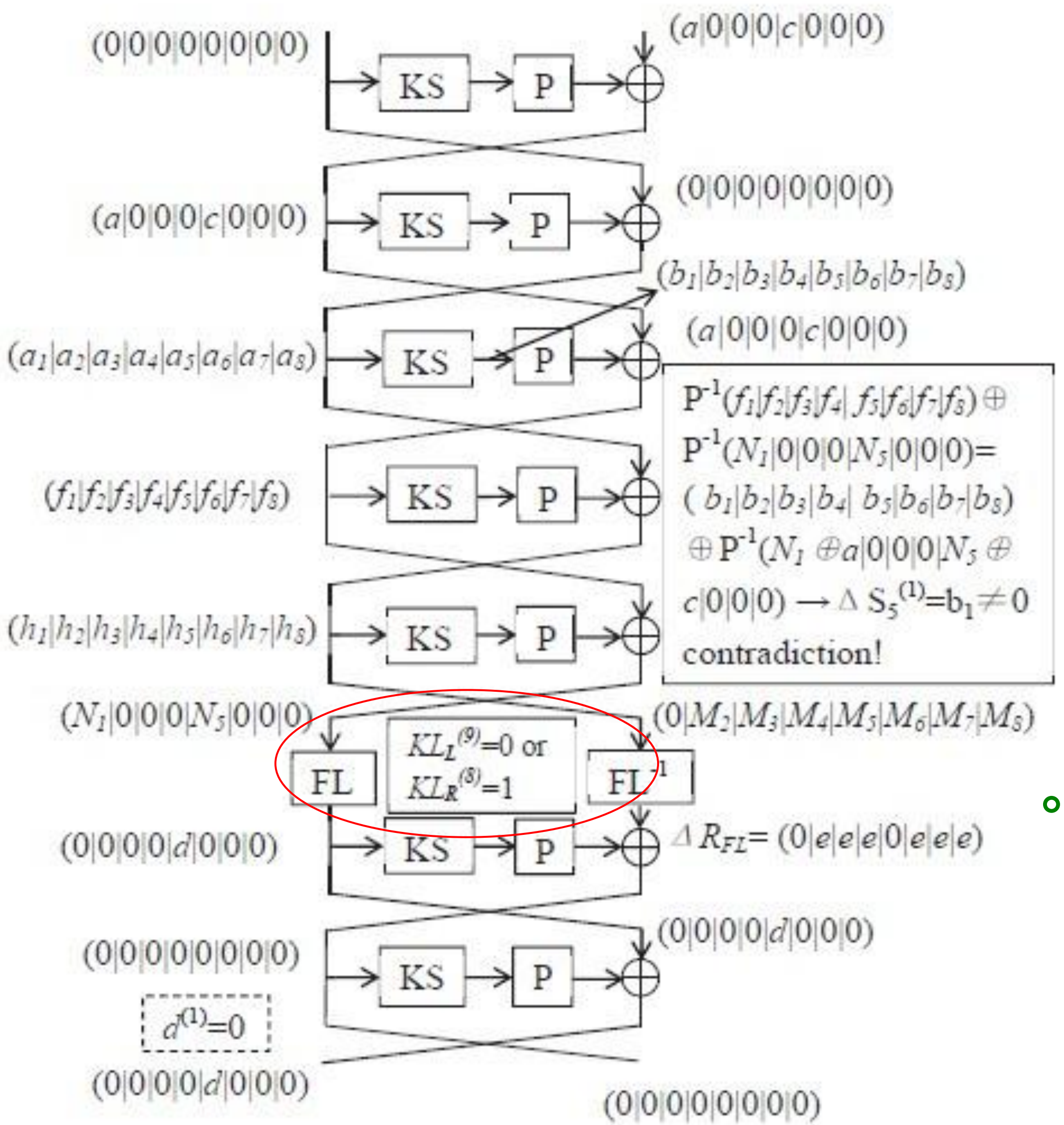


Fig. 5. FL^{-1}-function

$$\Delta Y_R = ((\Delta X_L \cap kl_L) \lll 1) \oplus \Delta X_R, \qquad \Delta Y_L = \Delta X_L \oplus \Delta Y_R \oplus (\Delta Y_R \cap kl_R);$$

$$\Delta X_L = \Delta Y_L \oplus \Delta Y_R \oplus (\Delta Y_R \cap kl_R), \qquad \Delta X_R = ((\Delta X_L \cap kl_L) \lll 1) \oplus \Delta Y_R.$$

7-Round Impossible Differentials of Camellia for Weak Keys



75%

htt

LoCCS

7-Round Impossible Differentials of Camellia for Weak Keys

- $(0|0|0|0|0|0|0|0,a|0|0|0|c|0|0|0) \nrightarrow (0|0|0|0|d|0|0|0,0|0|0|0|0|0|0|0)$ with conditions $KL_L^{(9)}=0$ or $KL_R^{(8)}=1$, and $d^{(1)}=0$.
- $(0|0|0|0|0|0|0|0,0|a|0|0|0|c|0|0) \nrightarrow (0|0|0|0|0|d|0|0,0|0|0|0|0|0|0|0)$ with conditions $KL_L^{(17)}=0$ or $KL_R^{(16)}=1$, and $d^{(1)}=0$.
- $(0|0|0|0|0|0|0|0,0|0|a|0|0|0|c|0) \nrightarrow (0|0|0|0|0|0|d|0,0|0|0|0|0|0|0|0)$ with conditions $KL_L^{(25)}=0$ or $KL_R^{(24)}=1$, and $d^{(1)}=0$.
- $(0|0|0|0|0|0|0|0,0|0|0|a|0|0|0|c) \nrightarrow (0|0|0|0|0|0|0|d,0|0|0|0|0|0|0|0)$ with conditions $KL_L^{(1)}=0$ or $KL_R^{(32)}=1$, and $d^{(1)}=0$.

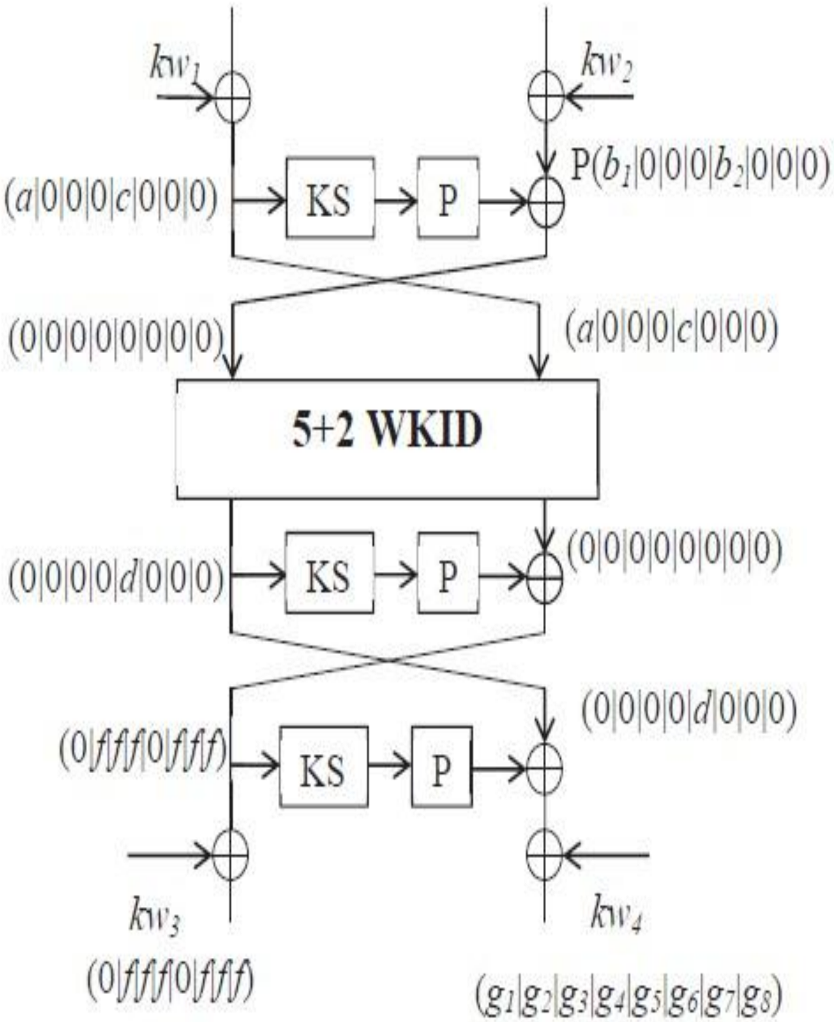
5+2 WKID

7-Round Impossible Differentials of Camellia for Weak Keys

- $(0|0|0|0|d|0|0|0,0|0|0|0|0|0|0|0) \nrightarrow (0|0|0|0|0|0|0|0,a|0|0|0|c|0|0|0)$ with conditions $KL'^{(9)}_L=0$ or $KL'^{(8)}_R=1$, and $d^{(1)}=0$.
- $(0|0|0|0|0|d|0|0,0|0|0|0|0|0|0|0) \nrightarrow (0|0|0|0|0|0|0|0,0|a|0|0|0|c|0|0)$ with conditions $KL'^{(17)}_L=0$ or $KL'^{(16)}_R=1$, and $d^{(1)}=0$.
- $(0|0|0|0|0|0|d|0,0|0|0|0|0|0|0|0) \nrightarrow (0|0|0|0|0|0|0|0,0|0|a|0|0|0|c|0)$ with conditions $KL'^{(25)}_L=0$ or $KL'^{(24)}_R=1$, and $d^{(1)}=0$.
- $(0|0|0|0|0|0|0|d,0|0|0|0|0|0|0|0) \nrightarrow (0|0|0|0|0|0|0|0,0|0|0|a|0|0|0|c)$ with conditions $KL'^{(1)}_L=0$ or $KL'^{(32)}_R=1$, and $d^{(1)}=0$.

2+5 WKID

Impossible Differential Attack on10-Round Camellia-128 for Weak Keys



- **Data Collections:**

  2^n Structures, $2^{n+63} \times 2^{-64} = 2^{n-1}$ pairs

- **Key Recovery:**

$K_{1,\{1,5\}}, K_{10,8}, K_{10,\{2,3,4,6,7\}}, K_{10,\{1,5\}}, K_{9,5}$

$$\varepsilon = 2^{80} \times (1 - 2^{-8})^{2^{n-66}} = 1$$
$$\Rightarrow n = 79.8$$

Time Complexity: $2^{111.8}$ encryptions;

Data Complexity: $2^{111.8}$ CP;

Memory Complexity: $2^{84.8}$ Bytes.

Impossible Differential Attack on 10-Round Camellia-128 for the Whole Key Space

- **Phases 1 to 4**: Perform an impossible differential attack on 10-round Camellia-128 by using each of **5+2 WKID:**

(0|0|0|0|0|0|0|0,a|0|0|0|c|0|0|0)↛ (0|0|0|0|d|0|0|0,0|0|0|0|0|0|0|0)

(0|0|0|0|0|0|0|0,0|a|0|0|0|c|0|0)↛ (0|0|0|0|0|d|0|0,0|0|0|0|0|0|0|0)

(0|0|0|0|0|0|0|0,0|0|a|0|0|0|c|0)↛ (0|0|0|0|0|0|d|0,0|0|0|0|0|0|0|0)

(0|0|0|0|0|0|0|0,0|0|0|a|0|0|0|c)↛ (0|0|0|0|0|0|0|d,0|0|0|0|0|0|0|0)

- **Phase 5**: If the attacks above all fail, then we obtain the key information as following:

$$K_A^{(95,103,111,119)} = 0 \text{ and } K_A^{(6,14,22,30)} = 1,$$

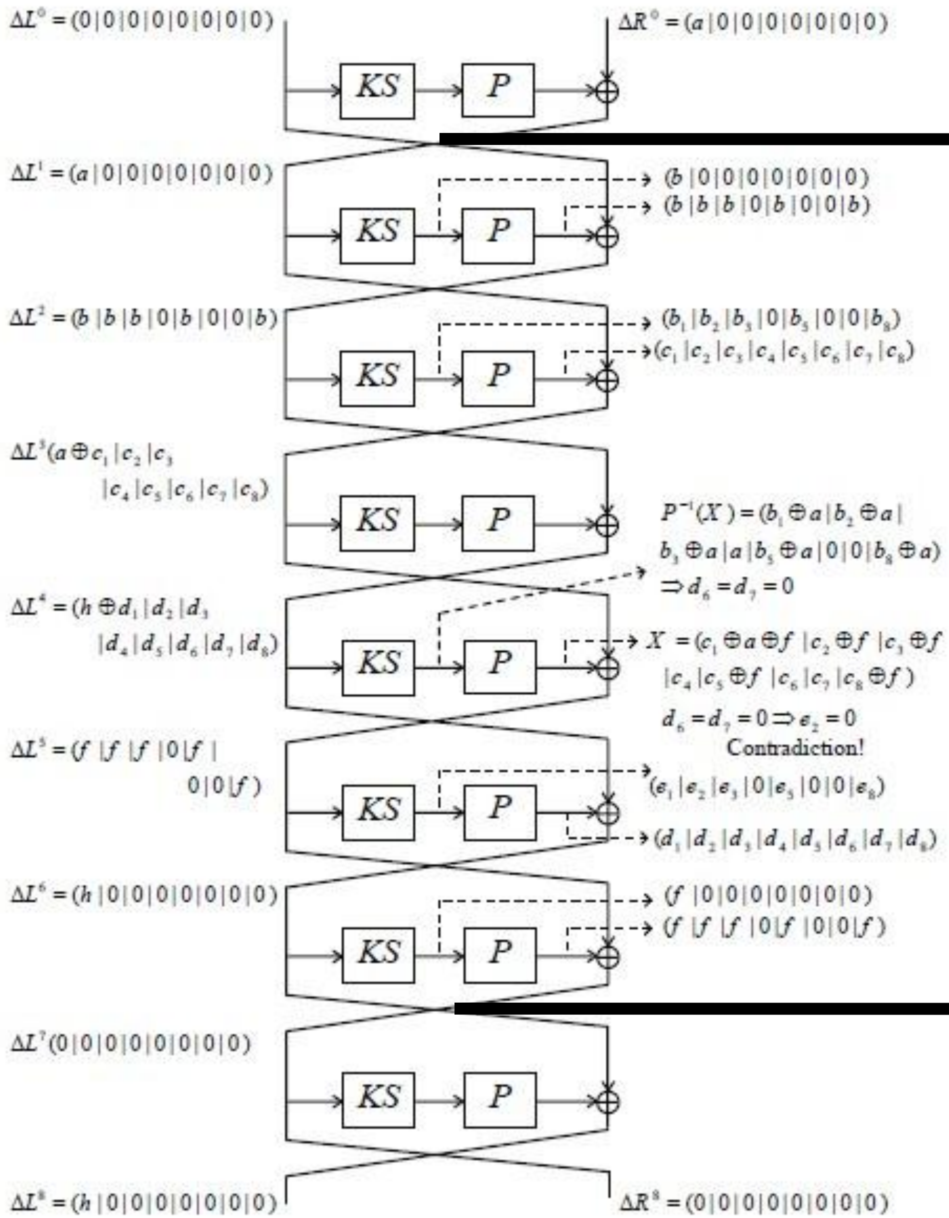
Guess the remaining keys.

DC: $2^{113.8}$ CP; TC: 2^{120} encryptions; MC:$2^{84.8}$ Bytes.

The Applications of 7-Round Impossible Differentials of Camellia with Weak Keys

- We attack 10-round Camellia-128 with $2^{113.8}$ chosen plaintexts and 2^{120} encryptions, 11-round Camellia-192 with $2^{114.64}$ chosen plaintexts and 2^{184} encryptions and 12-round Camellia-256 with $2^{116.17}$ chosen plaintexts and 2^{240} encryptions, which start from the first round.
- We attack 12-round Camellia-192 with $2^{120.1}$ chosen plaintexts and 2^{184} encryptions and 14-round Camellia-256 with 2^{120} chosen plaintexts and $2^{250.5}$ encryptions, which include two FL/FL^{-1} layers.

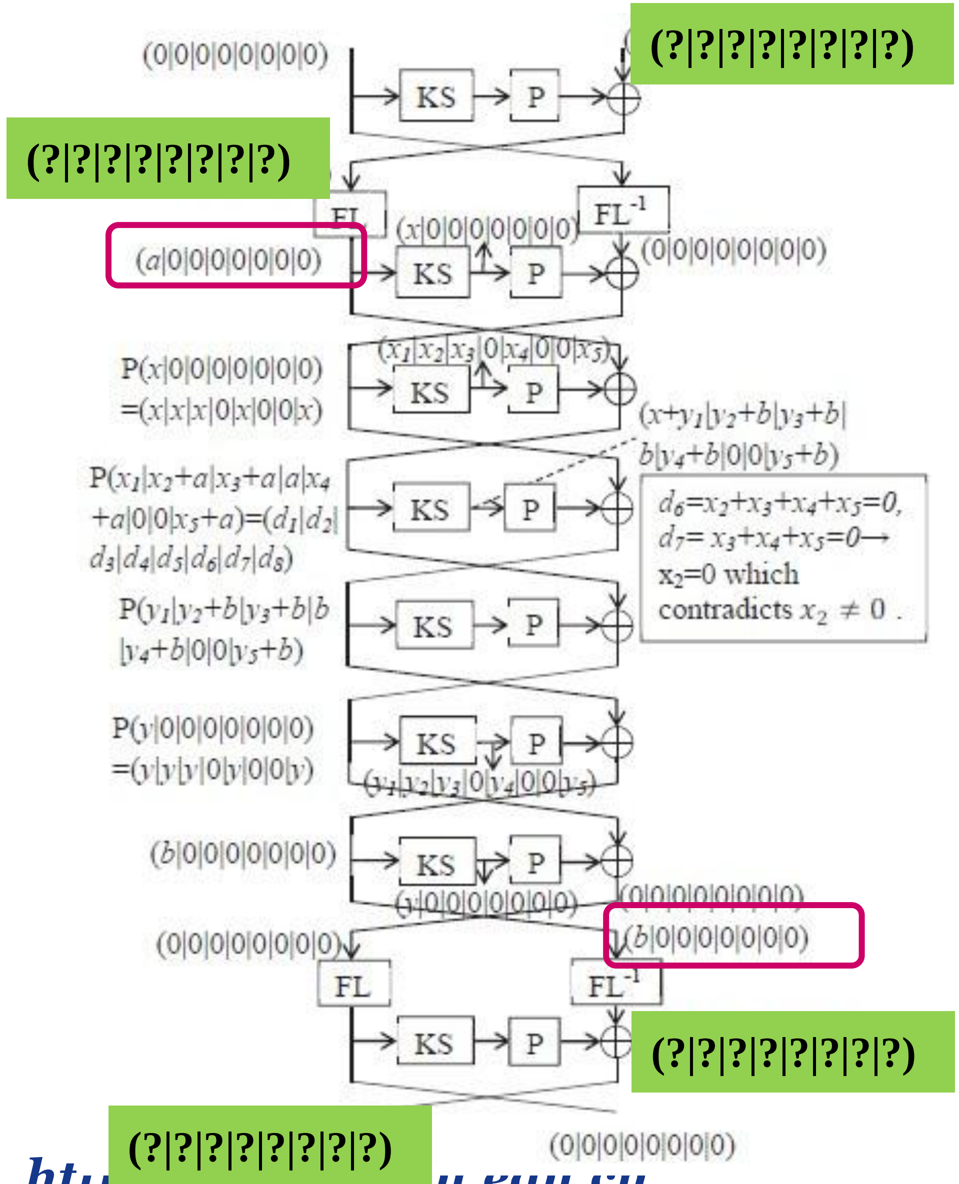
8-Round Impossible Differentials of Camellia without the Keyed Layers



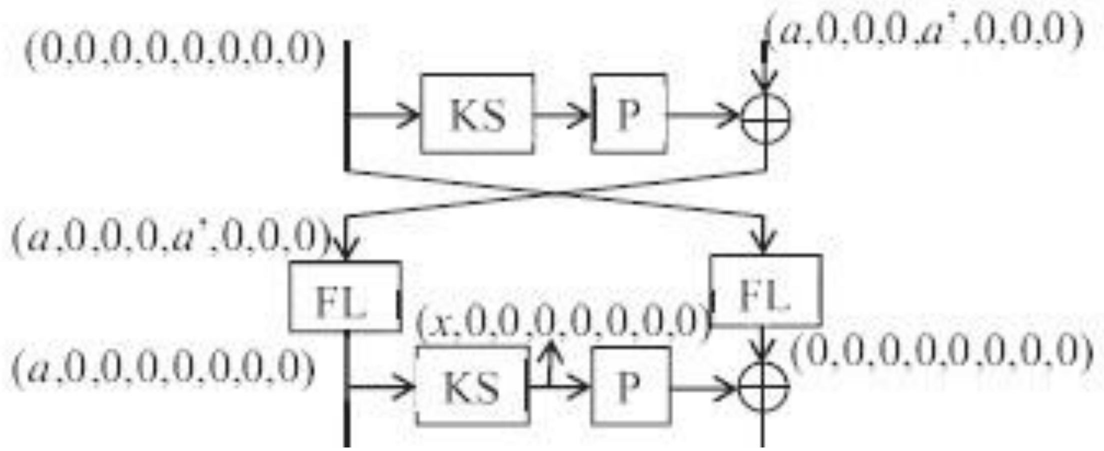
Insert key-dependent functions FL/FL^{-1}

Insert key-dependent functions FL/FL^{-1}

8-Round Impossible Differentials of Camellia with Two Keyed Layers



Property of FL



- **Proposition 7.** If the input difference of FL is $(a,0,0,0,a',0,0,0)$, where $a^{(1)} = a'^{(8)} = 0$ and

$$a'^{(i)} = \begin{cases} 0, & kl_L^{(i+1)} = 0; \\ a^{(i+1)}, & kl_L^{(i+1)} = 1; \end{cases} \quad for\ 1 \le i \le 7,$$

then the output difference of *FL* is $(a,0,0,0,0,0,0,0)$.

8-Round Impossible Differentials of Camellia with Two Keyed Layers

Proposition 8.

- the input difference of the 1st round: $(0,0,0,0,0,0,0,0,a,0,0,0,a',0,0,0)$;
- the output difference of the 8th round: $(b,0,0,0,b',0,0,0,0,0,0,0,0,0,0,0)$;
- a , $b \neq 0$, and $a^{(1)} = b^{(1)} = a'^{(8)} = b'^{(8)} = 0$.
- $$a'^{(i)} = \begin{cases} 0, & \text{if } kl_1^{(i+1)} = 0; \\ a^{(i+1)}, & \text{if } kl_1^{(i+1)} = 1; \end{cases} \quad b'^{(i)} = \begin{cases} 0, & \text{if } kl_4^{(i+1)} = 0; \\ b^{(i+1)}, & \text{if } kl_4^{(i+1)} = 1; \end{cases} \quad \text{for } 1 \leq i \leq 7,$$

where four subkeys $kl_i (i = 1, \cdots, 4)$ are used in two FL/FL^{-1} layers.

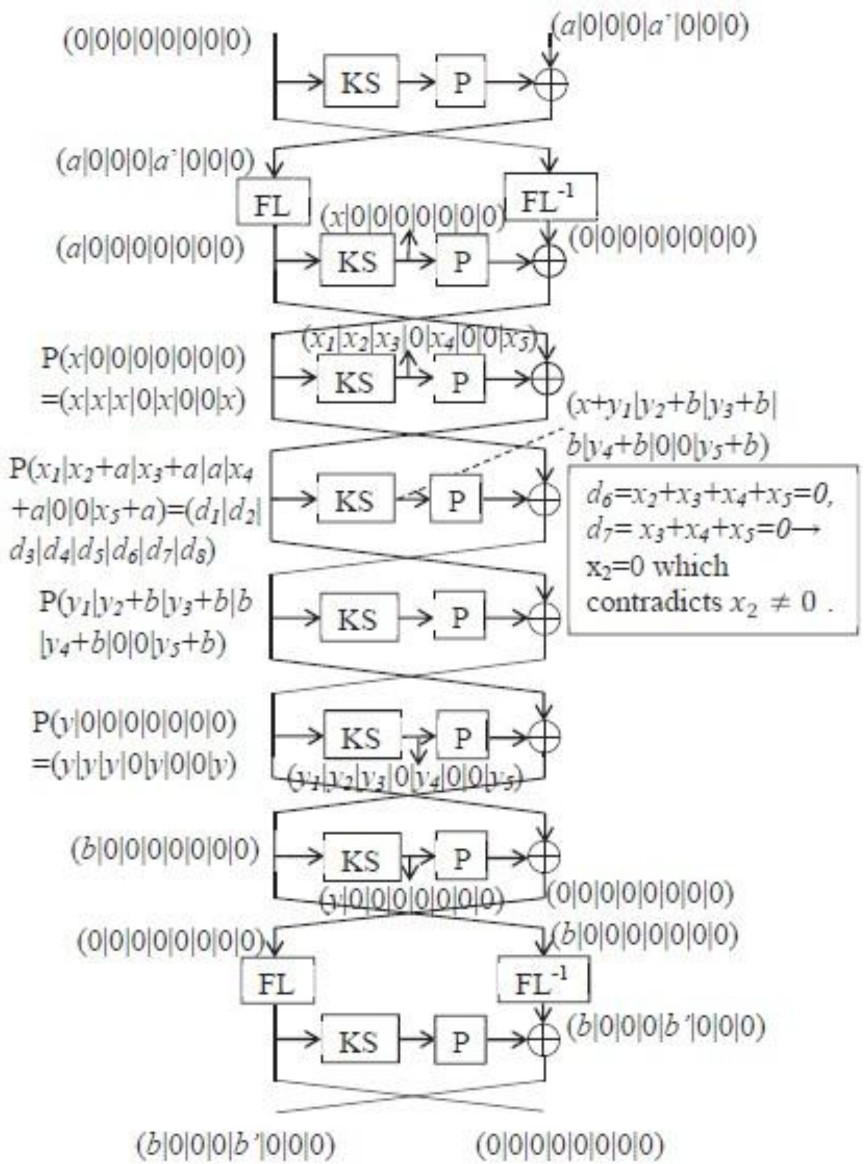
$\Rightarrow (0|0|0|0|0|0|0|0|a|0|0|0|a'|0|0|0) \nrightarrow_8 (b|0|0|0|b'|0|0|0|0|0|0|0|0|0|0|0)$

is an 8-round impossible differential of Camellia with two FL/FL^{-1} layers.

Δ_i denotes the corresponding 8-round differential for each different key values of $kl_1^{(2\sim7)}|kl_4^{(2\sim7)}$.

$A = \{\Delta_i | 0 \leq i \leq 2^{14} - 1\} \triangleq \{\delta_j | 1 \leq j \leq t\}$, where $t \leq 2^{14}$.

8-Round Impossible Differentials of Camellia with Two Keyed Layers



Attack Strategy

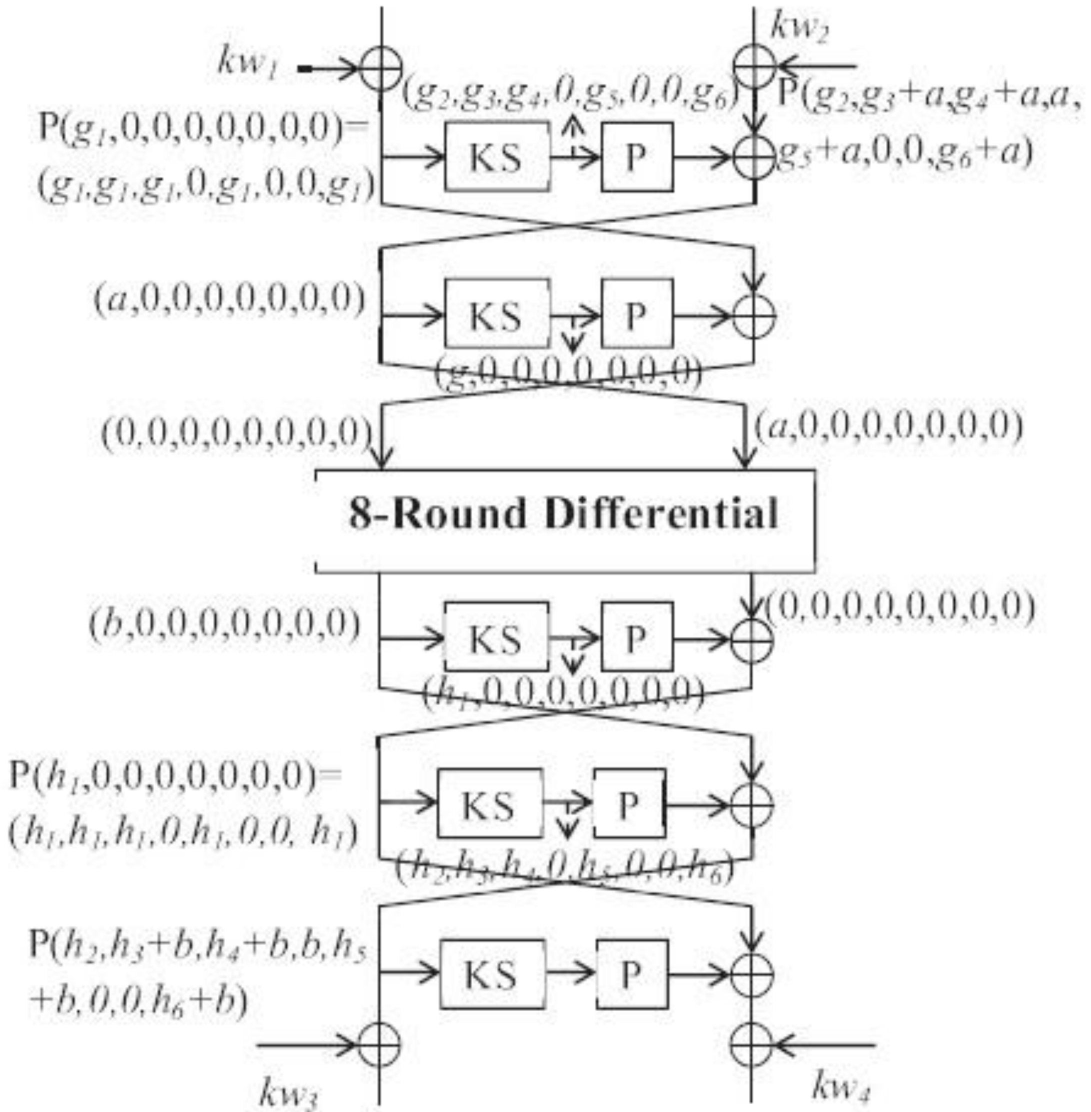
- Select $\delta_i \in A$, perform an impossible differential attack.
  - If **one** subkey is remained, we recover the secret key by the key schedule and verify whether it is correct by some plaintext-ciphertext pairs.
    - If success, end this attack.
    - Otherwise, try another differential δ_j(j≠i) of A and perform a new impossible differential attack.
  - If **no one** subkey or **more than one** subkeys are left, select δ_j (j≠i)∈A to execute a new impossible differential attack.

Impossible Differential Attack on 13-Round Camellia-256

$(0|0|0|0|0|0|0|0|a|0|0|0|a'|0|0|0) \nrightarrow_8 (b|0|0|0|b'|0|0|0|0|0|0|0|0|0|0|0)$

- **Case 1.** a′=b′=0.
- **Case 2.** a′=0 and b′≠0, or a′ ≠0 and b′=0.
- **Case 3.** a′≠0 and b′≠ 0.

Impossible Differential Attack on 13-Round Camellia-256



The Applications of 8-Round Impossible Differentials of Camellia

- We construct 8-round impossible differentials of Camellia with two FL/FL^{-1} layers, the length of which is the same as the length of the known best impossible differential of Camellia without the FL/FL^{-1} layers.
- The key-dependent layers cannot resist impossible differential attack effectively.
- We attack 12-round Camellia-192 with 2^{123} chosen plaintexts and $2^{187.2}$ encryptions and 13-round Camellia-256 with 2^{123} chosen plaintexts and $2^{251.1}$ encryptions, which include the whitening and FL/FL^{-1} layers.

Summary of the attacks on Camellia

Key Size	Rounds	Attack Type	Data	Time(Enc)	Memory (Bytes)	Source
Camellia-128	9†	Square	2^{48}CP	2^{122}	2^{53}	[10]
	10†	Impossible DC	2^{118}CP	2^{118}	2^{93}	[17]
	10†	Impossible DC	$2^{118.5}$CP	$2^{123.5}$	2^{127}	[12]
	10(Weak Key)	Impossible DC	$2^{111.8}$CP	$2^{111.8}$	$2^{84.8}$	Section 3.2
	10	Impossible DC	$2^{113.8}$CP	2^{120}	$2^{84.8}$	Section 3.2
	11	Impossible DC	2^{122}CP	2^{122}	2^{102}	Section 4.4
Camellia-192	10	Impossible DC	2^{121}CP	$2^{175.3}$	$2^{155.2}$	[3]
	10	Impossible DC	$2^{118.7}$CP	$2^{130.4}$	2^{135}	[12]
	11†	Impossible DC	2^{118}CP	$2^{163.1}$	2^{141}	[17]
	11(Weak Key)	Impossible DC	$2^{112.64}$CP	$2^{146.54}$	$2^{141.64}$	Section 3.3
	11	Impossible DC	$2^{114.64}$CP	2^{184}	$2^{141.64}$	Section 3.3
	12	Impossible DC	2^{123}CP	$2^{187.2}$	2^{160}	Section 4.3
	12†	Impossible DC	$2^{120.1}$CP	2^{184}	$2^{124.1}$	Section 3.5
Camellia-256	last 11 rounds	High Order DC	2^{93}CP	$2^{255.6}$	2^{98}	[5]
	11	Impossible DC	2^{121}CP	$2^{206.8}$	2^{166}	[3]
	11	Impossible DC	$2^{119.6}$CP	$2^{194.5}$	2^{135}	[12]
	12(Weak Key)	Impossible DC	$2^{121.12}$CP	$2^{202.55}$	$2^{142.12}$	Section 3.4
	12	Impossible DC	$2^{116.17}$CP/CC	2^{240}	$2^{150.17}$	Section 3.4
	13	Impossible DC	2^{123}CP	$2^{251.1}$	2^{208}	Section 4.2
	14†	Impossible DC	2^{120}CC	$2^{250.5}$	2^{125}	Section 3.5

DC: Differential Cryptanalysis; CP/CC: Chosen Plaintexts/Chosen Ciphertexts;
Enc: Encryptions; †: The attack doesn't include the whitening layers.

Conclusion

- We attack 10-round Camellia-128, 11-round Camellia-192 and 12-round Camellia-256 for the weak keys which start from the first round. We also extend these attacks for the whole key space.
- We attack 12-round Camellia-192 from rounds 3 to 14 and 14-round Camellia-256 from rounds 10 to 23.
- We construct 8-round impossible differentials of Camellia, which shows the key-dependent layers cannot resist impossible differential attack effectively.
- We attack 12-round Camellia-192 and 13-round Camellia-256 with the whitening and key-dependent layers.

Q&A

Thanks!