# Square Like Attack on Camellia

Lei Duo[1], Chao Li[1], and Keqin Feng[2]

[1] Department of Science, National University of Defense Technology,
Changsha, China
duoduolei@gmail.com
[2] Department of Math, Tsinghua University,
Beijing, China

**Abstract.** In this paper, a square like attack on Camellia is presented, by which 9-round 128-bit key Camellia without $FL/FL^{-1}$ functions layer and whitening is breakable with complexity of $2^{86.9}$ encryptions and $2^{66}$ data and 12-round 256-bit key Camellia without $FL/FL^{-1}$ function layer and whitening is breakable with the complexity of $2^{250.8}$ encryptions and $2^{66}$ data. And we can also apply such method to block cipher having XORing sBoxes in diffusion layer.

**Keywords:** Camellia, Block Cipher, Square attack.

## 1 Introduction

Camellia [1] is a symmetric key block cipher developed jointly in 2000 at NTT and Mitsubishi Electric Corporation. It has the modified Feistel structure with irregular rounds, which is called the $FL/FL^{-1}$ functions layers. Camellia has been accepted by ISO/IEC [11] as an international standard. It is also a winner of NESSIE, CRYPTREC project and IETF [11].

Efficient methods analyzing Camellia include linear attack [13], differential attack [13] truncated differential attack [6,8,14], impossible differential attack [16,14], higher order differential attack [4,7], Collision attack [10,15] and square attack [10,5,17]. The best attack on 128-bit key Camellia was linear attack [13], which can attack 10-round Camellia without $FL/FL^{-1}$ functions layer and whitening with complexity of $2^{121}$. The best attack against 256-bit key Camellia was impossible differential attack, which can attack 12-round Camellia without $FL/FL^{-1}$ functions layer and whitening with complexity of $2^{181}$.

In this paper, we improve the attacking results on Camellia. Our method uses active set [2], which was first introduced in square attack [2,3], to build the attack, however, the balanced byte is not core byte in our attack, special properties on XORing of active sBoxes are applied to build the distinguisher, so we call it square like attack. Such properties are first discovered and are in effect on the ciphers with XORing in diffusion layer.

Brief description of Camellia is presented in section 2. In section 3, active bytes transformations on Camellia are illustrated and some new properties are demonstrated. Our basic attacking method is described in section 4. Section 5

S. Qing, H. Imai, and G. Wang (Eds.): ICICS 2007, LNCS 4861, pp. 269–283, 2007.

is its extension. The paper concludes with our most important results contrast with other known results.

## 2 Description of the Camellia

Camellia has a 128-bit block size and supports 128-, 192- and 256-bit keys. Camellia with a 128-bit key and 256-bit key is written as 128-Camellia, 256-Camellia. The design of Camellia is based on the Feistel structure and its number of rounds is 18 (128-bit key) or 24 (192-, 256-bit key). The $FL/FL^{-1}$ functions layer is inserted in it every 6 rounds in order to thwart future unknown attacks. Before the first round and after the last round, there are pre- and post-whitening layers.

We refer $x^{(r)}, k^{(r)}$ to the $r$th round output and $r$th round subkey, refer $x_L^{(r)}$ and $x_R^{(r)}$ to the left, right half bytes of $x^{(r)}$, which implies $x^{(r)} = x_L^{(r)} \| x_R^{(r)}$. Let $P_L \| P_R$ and $C_L \| C_R$ be the Plaintext and Ciphertext.

Let $x^{(r,i)}$ be the $i$th byte of $x^{(r)}$. The $x_L^{(r)}$ is a 8-byte sequence, we have $x_L^{(r)} = (x_L^{(r,1)}, \ldots, x_L^{(r,8)})$. $F$ function contains key-addition $K$-function, sBoxes transformation $S$-function and diffusion function $P$-function, these functions are described as follows. The figure illustration of $F$-function is Fig.1.

The key addition function is

$$K(x_L^{(r)}, k^{(r+1)}) \overset{def}{=} (x_L^{(r,1)} \oplus k^{(r+1,1)}, \ldots, x_L^{(r,8)} \oplus k^{(r+1,8)}).$$

$S$-function contains 4 types of S-boxes $s_1$, $s_2$, $s_3$, and $s_4$. $s_2$,$s_3$,$s_4$ are variations of $s_1$,

$$S(y_1, \ldots, y_8) \overset{def}{=} (s_1(y_1), s_2(y_2), s_3(y_3), s_4(y_4), s_2(y_5), s_3(y_6), s_4(y_7), s_1(y_8)).$$

The relation among the four sBoxes is that

$$s_2(a) = s_1(a) \lll_1, \quad s_3(a) = s_1(a) \ggg_1, \quad s_4(a) = s_1(a \lll_1).$$

Let $P(z_1, ..., z_8) \overset{def}{=} (z'_1, ..., z'_8)$. The P-function:$\{0,1\}^{64} \mapsto \{0,1\}^{64}$ maps $(z_1, ..., z_8)$ to $(z'_1, ..., z'_8)$. The P-function and its inverse function $P^{-1}$ are

$$\begin{array}{ll}
z'_1 = z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8 \\
z'_2 = z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8 \\
z'_3 = z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8 \\
z'_4 = z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7 \\
z'_5 = z_1 \oplus z_2 \oplus z_6 \oplus z_7 \oplus z_8 \\
z'_6 = z_2 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_8 \\
z'_7 = z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8 \\
z'_8 = z_1 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7
\end{array}, \qquad
\begin{array}{l}
z_1 = z'_2 \oplus z'_3 \oplus z'_4 \oplus z'_6 \oplus z'_7 \oplus z'_8 \\
z_2 = z'_1 \oplus z'_3 \oplus z'_4 \oplus z'_5 \oplus z'_7 \oplus z'_8 \\
z_3 = z'_1 \oplus z'_2 \oplus z'_4 \oplus z'_5 \oplus z'_6 \oplus z'_8 \\
z_4 = z'_1 \oplus z'_2 \oplus z'_3 \oplus z'_5 \oplus z'_6 \oplus z'_7 \\
z_5 = z'_1 \oplus z'_2 \oplus z'_5 \oplus z'_7 \oplus z'_8 \\
z_6 = z'_2 \oplus z'_3 \oplus z'_5 \oplus z'_6 \oplus z'_8 \\
z_7 = z'_3 \oplus z'_4 \oplus z'_5 \oplus z'_6 \oplus z'_7 \\
z_8 = z'_1 \oplus z'_4 \oplus z'_6 \oplus z'_7 \oplus z'_8
\end{array}$$

The $R$ round Camellia without $FL/FL^{-1}$ functions and pre-, post- whitening function is written as follows,

$$\begin{cases}
x_L^{(0)} \| x_R^{(0)} & = P_L \| P_R \\
x_L^{(r)} & = x_R^{(r-1)} \oplus K(S(P(x_l^{(r-1)}))), \\
x_R^{(r)} & = x_L^{(r-1)}, \\
C_L \| C_R & = x_L^{(R)} \| x_R^{(R)}.
\end{cases}$$

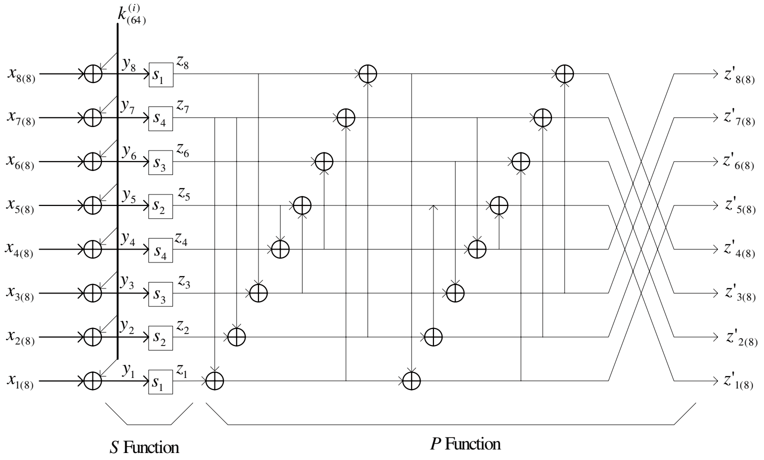

**Fig. 1.** Round function of Camellia-1

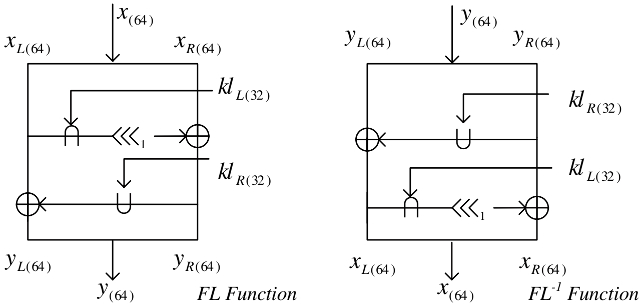

**Fig. 2.** $FL/FL^{-1}$ functions

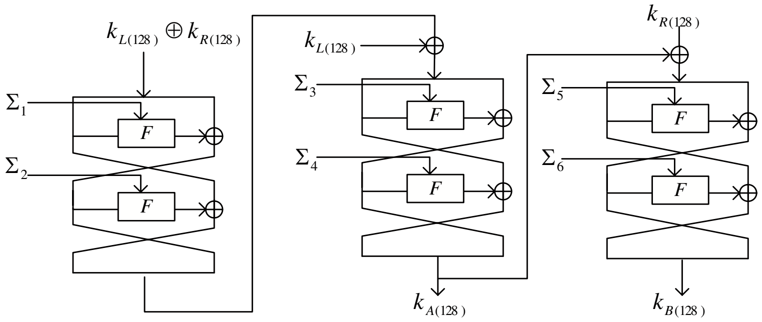

**Fig. 3.** Key Schedule of Camellia

The $P$-permutation, which is a linear transformation, can be move into previous round or post round. If pre-, post-whitening and $FL/FL^{-1}$ are not taken

**Table 1.** Round Keys.( We only give the first 14 rounds key.)

| 128bit key | | | 192-,256-bit key | | |
|---|---|---|---|---|---|
| | subkey | value | | subkey | value |
| Pre-whitening | $kw^{(1)}$ | $(k_L \lll_{0})_L$ | Pre-whitening | $kw^{(1)}$ | $(k_L \lll_{0})_L$ |
| | $kw^{(2)}$ | $(k_L \lll_{0})_R$ | | $kw^{(2)}$ | $(k_L \lll_{0})_R$ |
| $F$ (Round1) | $k^{(1)}$ | $(k_A \lll_{0})_L$ | $F$ (Round1) | $k^{(1)}$ | $(k_B \lll_{0})_L$ |
| $F$ (Round2) | $k^{(2)}$ | $(k_A \lll_{0})_R$ | $F$ (Round2) | $k^{(2)}$ | $(k_B \lll_{0})_R$ |
| $F$ (Round3) | $k^{(3)}$ | $(k_L \lll_{15})_L$ | $F$ (Round3) | $k^{(3)}$ | $(k_R \lll_{15})_L$ |
| $F$ (Round4) | $k^{(4)}$ | $(k_L \lll_{15})_R$ | $F$ (Round4) | $k^{(4)}$ | $(k_R \lll_{15})_R$ |
| $F$ (Round5) | $k^{(5)}$ | $(k_A \lll_{15})_L$ | $F$ (Round5) | $k^{(5)}$ | $(k_A \lll_{15})_L$ |
| $F$ (Round6) | $k^{(6)}$ | $(k_A \lll_{15})_R$ | $F$ (Round6) | $k^{(6)}$ | $(k_A \lll_{15})_R$ |
| $FL$ | $k^{(l1)}$ | $(k_A \lll_{30})_L$ | $FL$ | $k^{(l1)}$ | $(k_R \lll_{30})_L$ |
| $FL^{-1}$ | $k^{(l2)}$ | $(k_A \lll_{30})_R$ | $FL^{-1}$ | $k^{(l2)}$ | $(k_R \lll_{30})_R$ |
| $F$ (Round7) | $k^{(7)}$ | $(k_L \lll_{45})_L$ | $F$ (Round7) | $k^{(7)}$ | $(k_B \lll_{30})_L$ |
| $F$ (Round8) | $k^{(8)}$ | $(k_L \lll_{45})_R$ | $F$ (Round8) | $k^{(8)}$ | $(k_B \lll_{30})_R$ |
| $F$ (Round9) | $k^{(9)}$ | $(k_A \lll_{45})_L$ | $F$ (Round9) | $k^{(9)}$ | $(k_L \lll_{45})_L$ |
| $F$ (Round10) | $k^{(10)}$ | $(k_L \lll_{60})_R$ | $F$ (Round10) | $k^{(10)}$ | $(k_L \lll_{45})_R$ |
| $F$ (Round11) | $k^{(11)}$ | $(k_A \lll_{60})_L$ | $F$ (Round11) | $k^{(11)}$ | $(k_A \lll_{45})_L$ |
| $F$ (Round12) | $k^{(12)}$ | $(k_A \lll_{60})_R$ | $F$ (Round12) | $k^{(12)}$ | $(k_A \lll_{45})_R$ |
| $FL$ | $k^{(l3)}$ | $(k_L \lll_{77})_L$ | $FL$ | $k^{(l3)}$ | $(k_L \lll_{60})_L$ |
| $FL^{-1}$ | $k^{(l4)}$ | $(k_L \lll_{77})_R$ | $FL^{-1}$ | $k^{(l4)}$ | $(k_L \lll_{60})_R$ |
| $F$ (Round13) | $k^{(13)}$ | $(k_L \lll_{94})_L$ | $F$ (Round13) | $k^{(13)}$ | $(k_R \lll_{60})_L$ |
| $F$ (Round14) | $k^{(14)}$ | $(k_L \lll_{94})_R$ | $F$ (Round14) | $k^{(14)}$ | $(k_R \lll_{60})_R$ |
| Round15∼Round18 | | | Round15∼Round18 | | |
| Postwhitening | $kw^{(3)}$ | $(k_A \lll_{111})_L$ | $FL$ | $kl^{(5)}$ | $(k_A \lll_{77})_L$ |
| | $kw^{(4)}$ | $(k_A \lll_{111})_R$ | $FL^{-1}$ | $kl^{(6)}$ | $(k_A \lll_{77})_R$ |
| | | | Round19∼Round24 | | |
| | | | Postwhitening | $kw^{(3)}$ | $(k_B \lll_{111})_L$ |
| | | | | $kw^{(4)}$ | $(k_B \lll_{111})_R$ |

into consideration, two equivalence structures of Camellia called Camellia-3 and Camellia-4 [10] are given as follows.

The Camellia-3 is

$$\begin{cases} \widetilde{x}_L^{(0)} \| \widetilde{x}_R^{(0)} &= P_L \| P^{-1}(P_R) \\ \widetilde{x}_L^{(r)} &= \widetilde{x}_R^{(r-1)} \oplus S(\widetilde{x}_l^{(r-1)} \oplus k^{(r)}), \qquad r \text{ is odd} \\ \widetilde{x}_L^{(r)} &= P(\widetilde{x}_R^{(r-1)} \oplus S(P(\widetilde{x}_l^{(r-1)}) \oplus k^{(r)})), \qquad r \text{ is even} \\ \widetilde{x}_R^{(r)} &= \widetilde{x}_L^{(r-1)}, \\ C_L \| C_R &= \widetilde{x}_L^R \| P(\widetilde{x}_R^R). \end{cases}$$

The Camellia-4 is

$$\begin{cases} \widehat{x}_L^{(0)} \| \widehat{x}_R^{(0)} &= P^{-1}(P_L) \| P_R \\ \widehat{x}_L^{(r)} &= P(\widehat{x}_R^{(r-1)} \oplus S(P(\widehat{x}_l^{(r-1)}) \oplus k^{(r)})), \qquad r \text{ is odd} \\ \widehat{x}_L^{(r)} &= \widehat{x}_R^{(r-1)} \oplus S(\widehat{x}_l^{(r-1)} \oplus k^{(r)}), \qquad r \text{ is even} \\ \widehat{x}_R^{(r)} &= \widehat{x}_L^{(r-1)}, \\ C_L \| C_R &= P(\widehat{x}_L^R) \| \widehat{x}_R^R. \end{cases}$$

The $FL/FL^{-1}$ functions are shown in Fig.2, which are defined as follows: $(\{0,1\}^{64} \times \{0,1\}^{64} \rightarrow \{0,1\}^{64})$, $(x_L \| x_R, kl_L \| kl_R) \rightarrow y_L \| y_R$. The $FL$ function is

$$\begin{aligned} y_R &= ((x_L \cap kl_L) \lll_1) \oplus x_R, \\ y_L &= (y_R \cup kl_R) \oplus x_L. \end{aligned}$$

Fig.3 shows the key schedule of Camellia. Two 128-bit variables $k_L$ and $k_R$ are defined as follows. For 128-bit keys, the 128-bit key $k$ is used as $k_L$ and $k_R$ is $\mathbf{0}$. For 256-bit keys, the left 128-bit of the key $k$ is used as $k_L$ and the right 128-bit of $k$ is used as $k_R$. Two 128-bit variables $k_A$ and $k_B$ are generated from $k_L$ and $k_R$ as shown in Fig.3, in which $\Sigma_i (i = 1, \ldots, 6)$ are constants used as $Key$. The round keys are rotation of $k_A$,$k_B$,$k_L$ and $k_R$, which is shown in Table2.

# 3 Basic Attacks on Camellia

## 3.1 Preliminaries

The concepts of square attack and $\Lambda$-set were introduced by Daemen et. al [2].

Let $\Gamma$-set be a 256 collection of state bytes $\alpha^{(i)} = (\alpha^{(i,1)}, \ldots, \alpha^{(i,n)})$, $i \in [0..255]$, where $\alpha^{(i,j)}$ is the $j$th byte of $\alpha^{(i)}$. If the $j$th byte of elements in $\Gamma$ are different from one another,

$$\alpha^{(i,j)} \neq \alpha^{(i',j)}, \forall i, i' \in [0..255], i \neq i'$$

the $j$th byte is called active byte. The $j$th byte is called fixed byte, if the $j$th bytes are unchanged in $\Gamma$-set.

$$\alpha^{(i,j)} = \alpha^{(i',j)}, \forall i, i' \in [0..255], i \neq i'$$

And if $\sum_{i \in [0..255]} \alpha^{(i,j)} = 0$, then the $j$th byte is called balanced byte. To make thing simple, we use $\lambda, \theta, \delta$, and $\gamma$ to signify a byte and active byte is denoted $\lambda$, fixed byte is denoted $\theta$ and balanced byte is denoted $\delta$, other is denoted $\gamma$. A $\Gamma$-set is called $\Theta$-set, if all its bytes are fixed bytes. A $\Gamma$-set is called $\Lambda$-set, if all its bytes are active bytes or fixed bytes.

The following Theorem 1 is the most important properties of this paper and the attack is based on which. Before that, let give some notions. Let $\Lambda = \{\lambda^{(i)}\}$ be a one byte $\Lambda$-set , $\Theta = \{\theta^{(i)}\}$ be one byte $\Theta$-set and $\theta^{(i)} = \theta$. Let $Count_{f(\Lambda,\Theta)}(\gamma) \overset{def}{=} \#\{\gamma | f(\lambda^{(i)}, \theta^{(i)}) = \gamma, \lambda^{(i)} \in \Lambda, \theta^{(i)} \in \Theta, i \in [0..255]\}$. The $Count_{f(\Lambda,\Theta)}(\gamma)$ is the count of $\gamma$, when the inputs changes trough the input sets $\Lambda$ and $\Theta$.

The S-box of Camellia has following properties.

**Theorem 1.** *Let $\Lambda = \{\lambda^{(i)}\}$ be a $\Lambda$-set and $\Theta = \{\theta^{(i)}\}$ be $\Theta$-set, in which $\theta^{(i)} = \theta$ and $\lambda^{(i)}, \theta \in \{0,1\}^8$. S-Boxes of Camellia have following properties*

1. $Count_{s_\iota(\Lambda)}(\gamma) = 1$, $\iota \in \{1,2,3,4\}$, $\gamma \in \{0,1\}^8$;
2. $Count_{s_1(\Lambda) \oplus s_2(\Lambda)}(\gamma) \in \{0,2\}$, $\gamma \in \{0,1\}^8$;
3. $Count_{s_1(\Lambda) \oplus s_3(\Lambda)}(\gamma) \in \{0,2\}$, $\gamma \in \{0,1\}^8$;
4. $Count_{s_2(\Lambda) \oplus s_3(\Lambda)}(\gamma) \in \{0,4\}$, $\gamma \in \{0,1\}^8$;

5. *$Count_{s_\iota(\Lambda)\oplus s_\iota(\Lambda\oplus\Theta)}(\gamma)=\{0,2,4\}$, $\iota\in\{1,2,3,4\}$, $\gamma\in\{0,1\}^8$;*
6. *$Count_{s_\iota(\Lambda)\oplus s_\iota(\Lambda\oplus\Theta_1)\oplus s_\kappa(\Lambda)\oplus s_\kappa(\Lambda\oplus\Theta_2)}(\gamma) = \{0,2,4,6,8,\ldots\}$, $\iota,\kappa \in \{1,2,3,4\}$, $\iota\neq\kappa$ and $\gamma\in\{0,1\}^8$,*

*where $\Lambda\oplus\Theta \overset{def}{=} \{\lambda^{(i)}\oplus\theta^{(i)}\}$.*

The proof is omitted for we can check them directly. The item 1 is based on the sBoxes are permutations and item 2,3,4 are based on the liner relation between sBoxes $s_1, s_2$ and $s_3$. Item 5 is ,in fact, the differential table of sBoxes.

### 3.2 5-Round Distinguishers

In this section, we build a 5-round distinguishers on Camellia-4. Let $\Theta \overset{def}{=} \{\theta^{(i,1)}, \ldots, \theta^{(i,8)}\}$ be a $\Theta$-set. Let $\Lambda_0 \overset{def}{=} \{\lambda_0^{(i,1)}, \theta_0^{(i,2)}, \ldots, \theta_0^{(i,8)}\}$ be a $\Lambda$-set, in which the first byte is a active byte. We select the plaintext set as $\{P_L\} = \Theta$ and $\{P_R\} = \Lambda_0$. Let $F(\Theta) \overset{def}{=} \{F(\theta^{(i)})\}$. Let $\Theta_1 = \{\theta_1^{(i,1)}, \ldots, \theta_1^{(i,8)}\} \overset{def}{=} P^{-1}(\Theta)$. Let $\Theta_2 = \{\theta_2^{(i,1)}, \ldots, \theta_2^{(i,8)}\} \overset{def}{=} P(S(K(P(\Theta_1))))$. Then, five round Camellia-4 has following properties.

$$\begin{aligned}
\widehat{x}_R^{(0)} &= P_R = (\lambda_0^{(i,1)}, \theta_0^{(i,2)}, \ldots, \theta_0^{(i,8)}),\\
\widehat{x}_R^{(1)} &= P^{-1}(P_L) = (\theta_1^{(i,1)}, \ldots, \theta_1^{(i,8)}),\\
\widehat{x}_R^{(2)} &= P(S(K(P(\widehat{x}_R^{(1)})))) \oplus \widehat{x}_R^{(0)} = (\lambda_0^{(i,1)} \oplus \theta_2^{(i,1)}, \theta_0^{(i,2)} \oplus \theta_2^{(i,2)}, \ldots, \theta_0^{(i,8)} \oplus \theta_2^{(i,8)}),\\
\widehat{x}_R^{(3)} &= S(K(\widehat{x}_R^{(2)})) \oplus \widehat{x}_R^{(1)}\\
&= (s_1(\lambda_0^{(i,1)} \oplus \theta_2^{(i,1)} \oplus k^{(2,1)}) \oplus \theta_1^{(i,1)}, s_2(\theta_0^{(i,2)} \oplus \theta_2^{(i,2)} \oplus k^{(2,2)}) \oplus \theta_1^{(i,2)}\\
&\quad , \ldots, s_1(\theta_0^{(i,8)} \oplus \theta_2^{(i,8)} \oplus k^{(2,8)}) \oplus \theta_1^{(i,8)})\\
&\overset{def}{=} (s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)}, s_2(\theta_3^{(i,2)}) \oplus \theta_1^{(i,2)}), \ldots, s_1(\theta_3^{(i,8)}) \oplus \theta_1^{(i,8)})
\end{aligned}$$

Let

$$\left.\begin{aligned}
\widetilde{\lambda}_1^{(i)} &\overset{def}{=} s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)} \oplus (\oplus_{j\in\{3,4,6,7,8\}}(s_1(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,1)}\\
\widetilde{\lambda}_2^{(i)} &\overset{def}{=} s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)} \oplus (\oplus_{j\in\{2,4,5,7,8\}}(s_2(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,2)}\\
\widetilde{\lambda}_3^{(i)} &\overset{def}{=} s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)} \oplus (\oplus_{j\in\{2,3,5,6,8\}}(s_3(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,3)}\\
\widetilde{\theta}_4^{(i)} &\overset{def}{=} (\oplus_{j\in\{2,3,4,5,6,7\}}(s_4(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,4)}\\
\widetilde{\lambda}_5^{(i)} &\overset{def}{=} s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)} \oplus (\oplus_{j\in\{2,6,7,8\}}(s_2(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,5)}\\
\widetilde{\theta}_6^{(i)} &\overset{def}{=} (\oplus_{j\in\{2,3,5,7,8\}}(s_3(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,6)}\\
\widetilde{\theta}_7^{(i)} &\overset{def}{=} (\oplus_{j\in\{3,4,5,6,8\}}(s_4(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,7)}\\
\widetilde{\lambda}_8^{(i)} &\overset{def}{=} s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)} \oplus (\oplus_{j\in\{4,5,6,7\}}(s_1(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,8)}
\end{aligned}\right. ,$$

then,

$$\begin{aligned}
\widehat{x}_R^{(4,1)} &= s_1(\widetilde{\lambda}_1) \oplus s_3(\widetilde{\lambda}_3) \oplus s_4(\widetilde{\theta}_4) \oplus s_3(\widetilde{\theta}_6) \oplus s_4(\widetilde{\theta}_7) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta_2^{(i,1)} \oplus \lambda_2^{(i,1)}\\
\widehat{x}_R^{(4,2)} &= s_1(\widetilde{\lambda}_1) \oplus s_2(\widetilde{\lambda}_2) \oplus s_4(\widetilde{\theta}_4) \oplus s_2(\widetilde{\lambda}_5) \oplus s_4(\widetilde{\theta}_7) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta_2^{(i,2)}
\end{aligned}$$

$$\begin{aligned}
\widehat{x}_R^{(4,3)} &= s_1(\widetilde{\lambda}_1) \oplus s_2(\widetilde{\lambda}_2) \oplus s_3(\widetilde{\lambda}_3) \oplus s_2(\widetilde{\lambda}_5) \oplus s_3(\widetilde{\theta}_6) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta_2^{(i,3)}\\
\widehat{x}_R^{(4,4)} &= s_2(\widetilde{\lambda}_2) \oplus s_3(\widetilde{\lambda}_3) \oplus s_4(\widetilde{\theta}_4) \oplus s_2(\widetilde{\lambda}_5) \oplus s_3(\widetilde{\theta}_6) \oplus s_4(\widetilde{\theta}_7) \oplus \theta_2^{(i,4)}\\
\widehat{x}_R^{(4,5)} &= s_1(\widetilde{\lambda}_1) \oplus s_2(\widetilde{\lambda}_2) \oplus s_3(\widetilde{\theta}_6) \oplus s_4(\widetilde{\theta}_7) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta_2^{(i,5)}\\
\widehat{x}_R^{(4,6)} &= s_2(\widetilde{\lambda}_2) \oplus s_3(\widetilde{\lambda}_3) \oplus s_2(\widetilde{\lambda}_5) \oplus s_4(\widetilde{\theta}_7) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta_2^{(i,6)}\\
\widehat{x}_R^{(4,7)} &= s_3(\widetilde{\lambda}_3) \oplus s_4(\widetilde{\theta}_4) \oplus s_2(\widetilde{\lambda}_5) \oplus s_3(\widetilde{\theta}_6) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta_2^{(i,7)}\\
\widehat{x}_R^{(4,8)} &= s_1(\widetilde{\lambda}_1) \oplus s_4(\widetilde{\theta}_4) \oplus s_2(\widetilde{\lambda}_5) \oplus s_3(\widetilde{\theta}_6) \oplus s_4(\widetilde{\theta}_7) \oplus \theta_2^{(i,8)}.
\end{aligned}$$

Let us consider some properties of $\widehat{x}_R^{(4)}$ and $\widehat{x}_R^{(5)}$.

Since $\widehat{x}_R^{(4,8)} = s_1(\widetilde{\lambda}_1) \oplus s_4(\widetilde{\theta}_4) \oplus s_2(\widetilde{\lambda}_5) \oplus s_3(\widetilde{\theta}_6) \oplus s_4(\widetilde{\theta}_7) \oplus \theta_2^{(2,8)}$ and $\widehat{x}_R^{(5,8)} = s_1(\widehat{x}_R^{(4,8)} \oplus k^{(5,8)})$, we have

$$Count_{\{\widehat{x}_R^{(4,8)}\}}(\gamma) \in \{0,2\}, \text{ if } \widetilde{\lambda}_1 = \widetilde{\lambda}_5, \tag{1}$$

$$Count_{\{\widehat{x}_R^{(5,8)}\}}(\gamma) \in \{0,2\}, \text{ if } \widetilde{\lambda}_1 = \widetilde{\lambda}_5, \tag{2}$$

To make $\widetilde{\lambda}_1 = \widetilde{\lambda}_5$, we have,

$$\begin{aligned}
&\widetilde{\lambda}_1 = \widetilde{\lambda}_5\\
\Leftrightarrow\ & s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)} \oplus (\oplus_{j\in\{3,4,6,7,8\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,1)}\\
=\ & s_1(\lambda_0^{(i,1)} \oplus \theta_3^{(i,1)}) \oplus \theta_1^{(i,1)} \oplus (\oplus_{j\in\{2,6,7,8\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,5)}\\
\Leftrightarrow\ & (\oplus_{j\in\{3,4,6,7,8\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,1)}\\
=\ & (\oplus_{j\in\{2,6,7,8\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,5)}\\
\Leftrightarrow\ & (\oplus_{j\in\{3,4\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,1)} = (\oplus_{j\in\{2\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,5)}
\end{aligned}$$

So, $\widetilde{\lambda}_1 = \widetilde{\lambda}_5$ requires,

$$(\oplus_{j\in\{2,3,4\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,1)} \oplus k^{(4,5)} = 0 \tag{3}$$

Let $\Theta\|\Lambda \overset{def}{=} \{\theta^{(i)}\|\lambda^{(i)}\}$. Let 256 $\Lambda$-set be

$$(\Theta\|\Lambda_0)_\iota = (\{\theta^{(i,1)}, \ldots, \theta^{(i,8)}, \lambda_0^{(i,1)}, \theta_0^{(i,2)}, \ldots, \theta_0^{(i,8)}\})_\iota, \iota \in [0..255]$$

in which, $\lambda_0^{(i,1)}$ is active byte, other bytes are fixed bytes, $\theta_0^{(i,2)}$( or $\theta_0^{(i,3)}$, $\theta_0^{(i,4)}$) is different for different $\iota$ and other bytes are unchanged for all $\iota \in [0..255]$.

In five round Camellia-4, if we select plaintext set as $(\{P_L\|P_R\})_\iota = (\Theta\|\Lambda_0)_\iota$, then existing one $\iota$ makes $\widetilde{\lambda}_1 = \widetilde{\lambda}_5$. For, when $\Theta$ is unchanged, the left part of Eq.3 is only influenced by $s_\iota(\theta_3^{(i,j)}), j \in \{2,3,4\}$. And $s_\iota(\theta_3^{(i,j)})$ is only influenced by $\theta_0^{(i,j)}$, where $j \in \{2,3,4\}$. Then we find a 5-round distinguisher on Camellia-4. There are some more 5-round distinguishers as follows.

For, $\widehat{x}_R^{(4,2)} = s_1(\widetilde{\lambda}_1) \oplus s_2(\widetilde{\lambda}_2) \oplus s_4(\widetilde{\theta}_4) \oplus s_2(\widetilde{\lambda}_5) \oplus s_4(\widetilde{\theta}_7) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta^{(2,2)}$,

$$Count_{\{\widehat{x}_R^{(4,2)}\}}(\gamma) \in \{0,2,4\}, \text{ if } \widetilde{\lambda}_1 = \widetilde{\lambda}_8 \text{ or } \widetilde{\lambda}_2 = \widetilde{\lambda}_5. \tag{4}$$

$$Count_{\{\widehat{x}_R^{(5,2)}\}}(\gamma) \in \{0,2,4\}, \text{ if } \widetilde{\lambda}_1 = \widetilde{\lambda}_8 \text{ or } \widetilde{\lambda}_2 = \widetilde{\lambda}_5. \tag{5}$$

If $\widetilde{\lambda}_2 = \widetilde{\lambda}_5$, then we have

$$\widetilde{\lambda}_2 = \widetilde{\lambda}_5 \Leftrightarrow (\oplus_{j\in\{4,5,6\}}(s_\iota(\theta_3^{(i,j)}) \oplus \theta_1^{(i,j)})) \oplus k^{(4,2)} \oplus k^{(4,5)} = 0,$$

For $\widetilde{\lambda}_1 = \widetilde{\lambda}_8$, we have

$$\widetilde{\lambda}_1 = \widetilde{\lambda}_8 \Leftrightarrow \bigoplus_{j\in\{3,5,8\}} s_\iota(\theta_2^{(i,j)} \oplus k^{(2,j)}) \oplus \theta_1^{(i,j)}) \oplus k^{(4,1)} \oplus k^{(4,5)} = 0.$$

In five round Camellia-4, if we select plaintext set as $(\{P_L \| P_R\})_\iota = (\Theta \| \Lambda_0)_\iota$, in which if $\theta_0^{(i,4)}$( or $\theta_0^{(i,5)}$, $\theta_0^{(i,6)}$) is different for different $\iota$, then existing one $\iota$ makes $\widetilde{\lambda}_2 = \widetilde{\lambda}_5$ and if $\theta_0^{(i,3)}$( or $\theta_0^{(i,5)}$, $\theta_0^{(i,8)}$) is different for different $\iota$, then existing one $\iota$ makes $\widetilde{\lambda}_1 = \widetilde{\lambda}_8$.

Now, let us reconsider,

$$\widehat{x}_R^{(4,2)} = s_1(\widetilde{\lambda}_1) \oplus s_2(\widetilde{\lambda}_2) \oplus s_4(\widetilde{\theta}_4) \oplus s_2(\widetilde{\lambda}_5) \oplus s_4(\widetilde{\theta}_7) \oplus s_1(\widetilde{\lambda}_8) \oplus \theta^{(2,2)},$$

If we have $\widetilde{\lambda}_1 = \widetilde{\lambda}_2 \wedge \widetilde{\lambda}_5 = \widetilde{\lambda}_8$ or $\widetilde{\lambda}_1 = \widetilde{\lambda}_5 \wedge \widetilde{\lambda}_2 = \widetilde{\lambda}_8$, then we have

$$\begin{aligned} &Count_{\{\widehat{x}_R^{(4,2)}\}}(\gamma) \in \{0, 2, 4, 6, 8, \ldots\}, \\ &Count_{\{\widehat{x}_R^{(5,2)}\}}(\gamma) \in \{0, 2, 4, 6, 8, \ldots\}. \end{aligned}$$

Similarly, when the $\Lambda$-set $\Lambda_0$ is selected as $\{\theta_0^{(0,1)}, \lambda_0^{(0,2)}, \theta_0^{(0,3)}, \ldots, \theta_0^{(0,8)}\}$, $\{\theta_0^{(0,1)}, \theta_0^{(0,2)}, \lambda_0^{(0,3)}, \theta_0^{(0,4)}, \ldots, \theta_0^{(0,8)}\}$ or $\{\theta_0^{(0,1)}, \theta_0^{(0,2)}, \theta_0^{(0,3)}, \lambda_0^{(0,4)}, \theta_0^{(0,5)}, \ldots, \theta_0^{(0,8)}\}$, we can get similar properties, these properties are summarized in Table 2.

## 4 The Square Like Attack

In this section, we construct the attacks on Camellia without pre-, post- whitening and $FL/FL^{-1}$ functions.

The 6-round Square like attack uses the property of that, in Camellia-4 if the 1st byte of $\{P_R\}$ is active byte and $(\widetilde{\lambda}_1 = \widetilde{\lambda}_5)$ then, $Count_{\{\widehat{x}_R^{(5,8)}\}}(\gamma) \in \{0, 2\}$. This attack can be described by the following steps.

**Step1.** Select 256 $\Lambda$-set $\Lambda_\iota = \{\lambda_\iota^{(i,1)}, \theta_\iota^{(i,2)}, \ldots, \theta_\iota^{(i,8)}\}$, $\iota \in [0..255]$, in which $\lambda_\iota^{(i,1)} = \lambda_{\iota'}^{(i,1)}$, $\theta_\iota^{(i,j)} = \theta_{\iota'}^{(i,j)}$, $j \in \{2, 3, 5, 6, 7, 8\}$ and $\theta_\iota^{(i,4)} \neq \theta_{\iota'}^{(i,4)}, \forall \iota \neq \iota'$, and a $\Theta$-set $\Theta$. The 256 Plaintext sets are $(\{P_L \| P_R\})_\iota = (\Theta \| \Lambda_\iota)$. Then get the ciphertext sets $(\{C_L \| C_R\})_\iota$ and record them.

**Step 2.** For each $(\{C_L \| C_R\})_\iota$, Guess $k^{(6,8)}$, then check $Count_{\{x_R^{(5,8)}\}}(\gamma) \in \{0, 2\}$ being satisfied or not by Eq(6).

$$\widehat{x}_R^{(5,8)} = s_1(\widehat{x}_R^{(6,8)} \oplus k^{(5,8)}) \tag{6}$$

In this 6-round attack, the time that step 1 takes is $2^{16}$ 6-round encryptions takeing. Since Eq.(6) has 1 additions, 1 substitutions, getting $\widehat{x}_R^{(6)}$ from $C_R$ takes 5 addition, and 6-round Camellia has $44 \times 6$ additions, $8 \times 6$ substitutions, then the time of each guessing key in step 2 takes almost $\frac{1}{48}$ times 6 round encryption.

**Table 2.** Relation between active byte and special properties on its fifth round outputs, in which $\{P_L\} = \{\theta^{(i,1)}, \ldots, \theta^{(i,8)}\}$

| $Plaintext - set$ | $Count_{\{\mathbf{Byte}\}}(\gamma) \in$ **Set** if (**Condition**) | | |
|---|---|---|---|
| $\{P_R\}$ | **Byte** | **Set** | **Condition** |
| $\{\lambda^{(i,1)}, \theta^{(i,2)}, \ldots, \theta^{(i,8)}\}$ | $\widehat{x}_R^{(5,8)}$ | $\{0,2\}$ | $\widetilde{\lambda}_1 = \widetilde{\lambda}_5$ |
| | $\widehat{x}_R^{(5,2)}$ | $\{0,2,4\}$ | $\widetilde{\lambda}_1 = \widetilde{\lambda}_8 \vee \widetilde{\lambda}_2 = \widetilde{\lambda}_5$ |
| | | $\{0,2,4,6,\ldots\}$ | $(\widetilde{\lambda}_1 = \widetilde{\lambda}_2 \wedge \widetilde{\lambda}_5 = \widetilde{\lambda}_8)$ or $(\widetilde{\lambda}_1 = \widetilde{\lambda}_5 \wedge \widetilde{\lambda}_2 = \widetilde{\lambda}_8)$ |
| | $\widehat{x}_R^{(5,4)}$ | $\{1\}$ | $\widetilde{\lambda}_2 = \widetilde{\lambda}_5$ |
| | $\widehat{x}_R^{(5,5)}$ | $\{1\}$ | $\widetilde{\lambda}_1 = \widetilde{\lambda}_8$ |
| $\{\theta^{(i,1)}, \lambda^{(i,2)}, \theta^{(i,3)}, \ldots, \theta^{(i,8)}\}$ | $\widehat{x}_R^{(5,5)}$ | $\{0,4\}$ | $\widetilde{\lambda}_2 = \widetilde{\lambda}_3$ |
| | $\widehat{x}_R^{(5,2)}$ | $\{0,2,4\}$ | $\widetilde{\lambda}_2 = \widetilde{\lambda}_5 \vee \widetilde{\lambda}_3 = \widetilde{\lambda}_6$ |
| | | $\{0,2,4,6,\ldots\}$ | $(\widetilde{\lambda}_2 = \widetilde{\lambda}_3 \wedge \widetilde{\lambda}_5 = \widetilde{\lambda}_6)$ or $(\widetilde{\lambda}_2 = \widetilde{\lambda}_6 \wedge \widetilde{\lambda}_3 = \widetilde{\lambda}_5)$ |
| | $\widehat{x}_R^{(5,1)}$ | $\{1\}$ | $\widetilde{\lambda}_3 = \widetilde{\lambda}_6$ |
| | $\widehat{x}_R^{(5,6)}$ | $\{1\}$ | $\widetilde{\lambda}_2 = \widetilde{\lambda}_5$ |
| $\{\theta^{(i,1)}, \theta^{(i,2)}, \lambda^{(i,3)}, \theta^{(i,4)}, \ldots, \theta^{(i,8)}\}$ | Pseudo Random Function | | |
| | $\widehat{x}_R^{(5,2)}$ | $\{0,2,4\}$ | $\widetilde{\lambda}_3 = \widetilde{\lambda}_6 \vee \widetilde{\lambda}_4 = \widetilde{\lambda}_7$ |
| | | $\{0,2,4,6,\ldots\}$ | $(\widetilde{\lambda}_3 = \widetilde{\lambda}_4 \wedge \widetilde{\lambda}_6 = \widetilde{\lambda}_7)$ or $(\widetilde{\lambda}_3 = \widetilde{\lambda}_7 \wedge \widetilde{\lambda}_4 = \widetilde{\lambda}_6)$ |
| | $\widehat{x}_R^{(5,2)}$ | $\{1\}$ | $\widetilde{\lambda}_4 = \widetilde{\lambda}_7$ |
| | $\widehat{x}_R^{(5,7)}$ | $\{1\}$ | $\widetilde{\lambda}_3 = \widetilde{\lambda}_6$ |
| $\{\theta^{(i,1)}, \ldots, \theta^{(i,3)}, \lambda^{(i,4)}, \theta^{(i,5)}, \ldots, \theta^{(i,8)}\}$ | Pseudo Random Function | | |
| | $\widehat{x}_R^{(5,2)}$ | $\{0,2,4\}$ | $\widetilde{\lambda}_4 = \widetilde{\lambda}_7 \vee \widetilde{\lambda}_1 = \widetilde{\lambda}_8$ |
| | | $\{0,2,4,6,\ldots\}$ | $(\widetilde{\lambda}_1 = \widetilde{\lambda}_4 \wedge \widetilde{\lambda}_7 = \widetilde{\lambda}_8)$ or $(\widetilde{\lambda}_1 = \widetilde{\lambda}_7 \wedge \widetilde{\lambda}_4 = \widetilde{\lambda}_8)$ |
| | $\widehat{x}_R^{(5,3)}$ | $\{1\}$ | $\widetilde{\lambda}_1 = \widetilde{\lambda}_8$ |
| | $\widehat{x}_R^{(5,8)}$ | $\{1\}$ | $\widetilde{\lambda}_4 = \widetilde{\lambda}_7$ |

In step 2, Eq.(6) repeats $2^8$ times for $2^8$ guessed key. The probability of wrong key passing the checking is $2^8 \times \binom{256}{128} \times \binom{256}{2} \times \binom{254}{2} \times \ldots \times \binom{2}{2} \times (128!)^{-1} \times 128! \times 256^{-256} = 2^8 \times \frac{256!256!}{2^{128}256^{256}128!128!} \approx \frac{2^8 2\pi 256 256^{256} 256^{256} e^{128} e^{128}}{2^{128} 2\pi 128 e^{256} e^{256} 256^{256} 128^{128} 128^{128}} = 2^{-119}(\frac{2}{e})^{256}$, so only right key can pass step 2, then the 6-round attack's complexity is $2^{16}(1 + 2^8 \times \frac{1}{48}) \approx 2^{18.4}$. The selected Plaintexts are $2^{16}$.

7-round attack adds one round at the beginning, uses the structure of Camellia-3 and selects the input sets to make $(\{\widetilde{x}_L^{(1)} \| \widetilde{x}_R^{(1)}\})_\iota = (\Theta \| \Lambda_\iota)$. The selected 256 plaintext sets are

$$(\{P_L\})_\iota = \Lambda_\iota = \{\lambda_\iota^{(i,1)}, \theta_\iota^{(i,2)}, \ldots, \theta_\iota^{(i,8)}\},$$
$$(\{P_R\})_\iota = \{P^{-1}(s_1(\lambda_\iota^{(i,1)} \oplus k^{(1,1)}), \theta_\iota^{(i,2)}, \theta_\iota^{(i,3)}, s_4(\theta_\iota^{(i,4)} \oplus k^{(1,4)}), \theta_\iota^{(i,5)}, \ldots, \theta_\iota^{(i,8)})\}.$$

We have $\{\widetilde{x}_R^{(0)}\}_i = \{s_1(\lambda_\iota^{(i,1)} \oplus k^{(1,1)}), \theta_\iota^{(i,2)}, \theta_\iota^{(i,3)}, s_4(\theta_\iota^{(i,4)} \oplus k^{(1,4)}), \theta_\iota^{(i,5)}, \ldots, \theta_\iota^{(i,8)}\}_\iota$. Then, $k^{(1,1)}$, $k^{(1,4)}$ and $k^{(7,8)}$ are guessing key bytes.

This 7-round attack selects $2^{32}$ plaintext and the attacking complexity is $2^{16} \times 2^{16}(1 + 2^8 \times \frac{1}{56}) \approx 2^{34.5}$. The chosen plaintext are $2^{32}$.

The 8-round attack is similar to 7-round attack, just adds one round at the end and guesses the 8th round key bytes to get the $\tilde{x}_R^{(7,8)}$. Getting $\tilde{x}_R^{(7,8)}$ from $\tilde{x}_R^{(8)}$ needs five 8th round key bytes $k^{(8,1)}, k^{(8,4)}, k^{(8,5)}, k^{(8,6)}, k^{(8,7)}$ and needs 11 addition and 6 S-box transformation, which equals 1/8 8-round encryption. Then, the complexity of this attack is $2^{32} \times (1 + 2^{40} \times (\frac{1}{8} + 2^8 \times \frac{1}{64})) \approx 2^{74}$. The chosen plaintexts are $2^{32}$.

In 9-round attack, we add one round at the beginning and use the structure of Camellia-4, where the selected special plaintexts should satisfy the properties of that $(\{\widehat{x}_L^{(2)} \| \widehat{x}_R^{(2)}\})_\iota = (\Theta \| \Lambda_\iota)$. So the plaintext are,

$$\left\{\begin{array}{l} P_L^{(1)} \\ P_L^{(2)} \\ P_L^{(3)} \\ P_L^{(4)} \\ P_L^{(5)} \\ P_L^{(6)} \\ P_L^{(7)} \\ P_L^{(8)} \end{array}\right\}_\iota = \left\{\begin{array}{l} s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus s_4(\theta_\iota^{(i,1)} \oplus k^{(2,4)}) \\ s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus s_4(\theta_\iota^{(i,1)} \oplus k^{(2,4)}) \\ s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \\ s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \\ s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \\ \theta_\iota^{(i,6)} \\ s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \\ s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \end{array}\right\}_\iota ,$$

$$\left\{\begin{array}{l} P_R^{(1)} \\ P_R^{(2)} \\ P_R^{(3)} \\ P_R^{(4)} \\ P_R^{(5)} \\ P_R^{(6)} \\ P_R^{(7)} \\ P_R^{(8)} \end{array}\right\}_\iota = \left\{\begin{array}{l} s_1(s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \oplus k^{(1,1)}) \\ s_2(s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \oplus k^{(1,2)}) \\ s_3(s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus k^{(1,3)}) \\ s_4(s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \oplus k^{(1,4)}) \\ s_2(s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus k^{(1,5)}) \\ \theta_\iota^{(i,6)} \\ s_4(s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \oplus k^{(1,7)}) \\ s_1(s_1(\lambda_\iota^{(i,1)} \oplus k^{(2,1)}) \oplus s_4(\theta_\iota^{(i,4)} \oplus k^{(2,4)}) \oplus k^{(1,8)}) \end{array}\right\}_\iota ,$$

The complexity of this attack is $2^{88} \times (1 + 2^{40} \times (\frac{1}{9} + 2^8 \times \frac{1}{72})) \approx 2^{129.8}$.

In 128-Camellia, part of the 9th round key bits are included in $k^{(1)}$ and $k^{(2)}$. Then, in step 2, we check $Count_{\{x_R^{(7,4)}\}}(\gamma) = 1$ being hold or not, the guessing key bytes are $k^{(1,1)}, k^{(1,2)}, k^{(1,3)}, k^{(1,4)}, k^{(1,5)}, k^{(1,7)}, k^{(1,8)}$, $k^{(2,1)}, k^{(2,4)}$, $k^{(8,4)}$, $k^{(9,2)}$, $k^{(9,3)}, k^{(9,4)}$, $k^{(9,5)}$, $k^{(9,6)}, k^{(9,7)}$. The 28 bits of 9th round key are included in first and second rounds guessing. The complexity of this 9-round attack becomes $2^{88} \times (1 + 2^{12}(\frac{1}{8} + 2^8 \times \frac{1}{72})) \approx 2^{102.2}$. The chosen plaintexts are $2^{88}$.

In 256-Camellia, the chosen plaintexts are same as attack on 128-Camellia. Since $k^{(7)} \| k^{(8)} = k^{(1)} \| k^{(2)}_{\lll 30}$, the complexity of 7-round attack becomes $2^{32} \times (1 + 1 \times \frac{1}{56}) \approx 2^{32}$, in which the guessing key bytes are $k^{(1,1)}, k^{(1,2)}, k^{(7,8)}$. Key bits of $k^{(7,8)}$ are included in key bits of $k^{(1,1)}$ and $k^{(1,2)}$.

In these basic attacks, we select 256 $\Lambda$-set $\Lambda_\iota$ that requires $\theta_\iota^{(i,4)} \neq \theta_{\iota'}^{(i,4)}$ to guarantee the existence of $\widetilde{\lambda}_1 = \widetilde{\lambda}_5$. However, to guarantee the $\Theta$-set $\Theta$ is

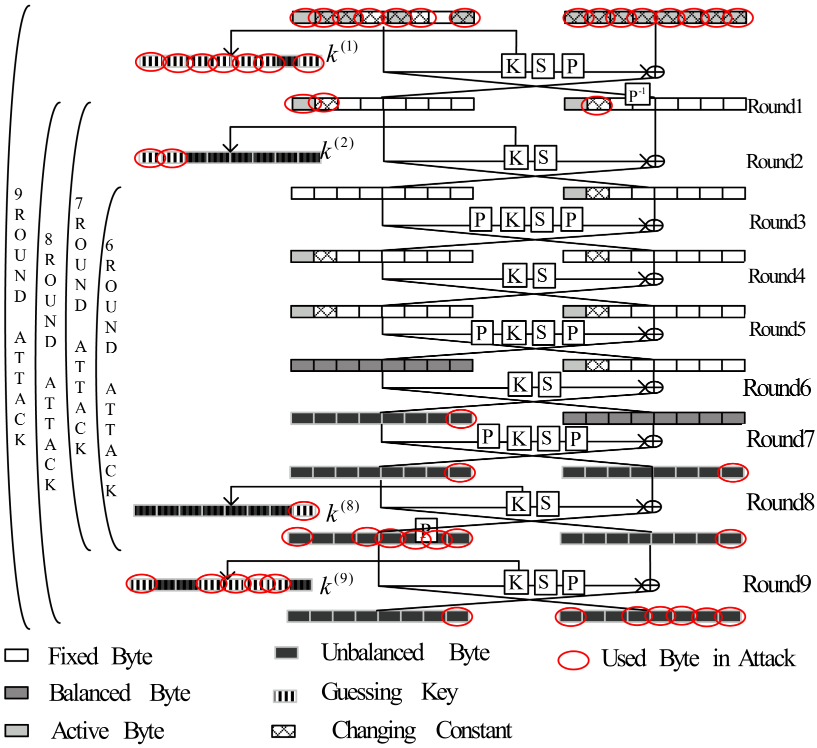

**Fig. 4.** Basic Attack on 6,7,8, and 9 round Camellia

unchanged, 7-round attack requires guessing 1 more key byte and 9-round attack requires guessing 3 more key bytes. In next section, we avert these key guessing.

# 5 Improvements on the Attack

## 5.1 Basic Improvement

In 6-round attack, if we select $\{P_L\}_\iota = \Theta_\iota$ and $\{P_R\}_\iota = \Lambda_\iota$, in which the first byte of $\Lambda_\iota$ is active byte and other bytes of $\Lambda_\iota$ and $\Theta_\iota$ are random selected fixed bytes, then, for each $\Theta_\iota$ and $\Lambda_\iota$, the probability of $\widetilde{\lambda}_i = \widetilde{\lambda}_j, i \neq j$ is $\sum_{i=0}^{255} \frac{1}{256} \frac{1}{256} = \frac{1}{256}$. And the probability of non appearance of $\widetilde{\lambda}_i = \widetilde{\lambda}_j$ is $\frac{255}{256}$, for given $i, j \in \{1, \ldots, 8\}$. And when the attacker selects $t$ plaintext sets, the non appearance of $\widetilde{\lambda}_i = \widetilde{\lambda}_j$ is $(\frac{255}{256})^t$. We can improve the attack in following way.

**Step1.** Set $\iota = 1$.

**Step2.** Select a $\Lambda$-set $\Lambda_\iota$ and a $\Theta$-set $\Theta_\iota$, in which $\lambda_\iota^{(i,1)}$ is a active byte and other bytes are random selected fixed bytes. Set the Plaintext sets as $\{P_L \| P_R\}_\iota = \Theta_\iota \| \Lambda_\iota$ and get the ciphertext sets as $\{C_L \| C_R\}_\iota$.

**Step 3.** Guess $k^{(6,8)}$, gets $\widehat{x}_R^{(5,8)}$ by Eq(6), checks $Count_{\{\widehat{x}_R^{(5,8)}\}}(\gamma) \in \{0, 2\}$ being satisfied or not. If $Count_{\{\widehat{x}_R^{(5,8)}\}}(\gamma) > 2$ or $\#\{Count_{\{x_R^{(5,8)}\}}(\gamma) = 1\} > 128$, then selects a new key. If the exist a key $k^{(6,8)}$ pass the checking, then it is a correct key. Or else $\iota = \iota + 1$ and goto step 2.

In this 6-round attack, the time that step 2 takes is $2^8$ 6-round encryptions takeing. For each guessing key step 3 takes almost $\frac{1}{48}$ times 6 round encryption. In step 2, Eq.(6) repeats $2^8$ times. The probability of wrong key passing the checking is $2^{-119}(\frac{2}{e})^{256} \approx 2^{-232}$, so only right key can pass step 2. And when $\iota = 2^{10}$, the probability appearance of $\widetilde{\lambda}_1 = \widetilde{\lambda}_5$ is 0.99. Then the 6-round attack's complexity is $2^{18}(1 + 2^8 \times \frac{1}{48}) \approx 2^{20.4}$. The selected Plaintexts are $2^{18}$.

The 7,8,9-round 128-bit Camellia attacks use same structure as previous section. In 7-round attack, the guessing key bytes are $k^{(1,1)}$ and $k^{(7,8)}$. In 8-round attack, the guessing key bytes are $k^{(1,1)}, k^{(7,8)}, k^{(8,1)}, k^{(8,4)}, k^{(8,5)}, k^{(8,6)}, k^{(8,7)}$. In 9-round attack, the guessing key bytes are $k^{(1,1)}, k^{(1,2)}, k^{(1,3)}, k^{(1,5)}, k^{(1,8)}, k^{(2,1)}, k^{(8,8)}, k^{(9,1)}, k^{(9,4)}, k^{(9,5)}, k^{(9,6)}, k^{(9,7)}$, in which the 13 bits of 9th round key is included in 1st guess round key. The chosen plaintexts for 7,8 and 9 rounds are $2^{26}$, $2^{26}$ and $2^{66}$, respectively. The complexities are $2^{26} \times (1 + 2^8 \times \frac{1}{56}) = 2^{28.5}$, $2^{26} \times (1 + 2^{40}(\frac{1}{8} + 2^8 \times \frac{1}{64})) \approx 2^{68}$ and $2^{66} \times (1 + 2^{27}(\frac{1}{9} + 2^8 \times \frac{1}{72})) \approx 2^{94.9}$, respectively.

In 9-round attack, if we select the ciphertext similar as previous discussion on plaintext and check the $Count_{\{\widetilde{x}_R^{(2,5)}\}}(\gamma) = 1$ being satisfied or not, then the guessing round key bytes are $k^{(9,1)}, k^{(9,2)}, k^{(9,4)}, k^{(9,7)}, k^{(9,8)}, k^{(8,4)}, k^{(2,5)}, k^{(1,1)}, k^{(1,2)}, k^{(1,6)}, k^{(1,7)}, k^{(1,8)}$. Then, the complexity of attack becomes $2^{66} \times (1 + 2^{21}(\frac{1}{9} + 2^3 \times \frac{1}{72})) \approx 2^{84.8}$.

### 5.2 Improvement on 256-Bit Camellia

In 7,8,9 and 10-round attacks on 256-Camellia the chosen plaintext are same as above section. However, the 7th round key is same as first round key and 8th round key is same as 2nd round key, then in 7-round attack, the guessing round key bytes are $k^{(1,1)}$ and $k^{(7,5)}$, in which 6 bits of $k^{(7,5)}$ are included in $k^{(1,1)}$. In 8-round attack, the guessing round key bytes are $k^{(1,1)}, k^{(7,5)}, k^{(8,1)}, k^{(8,2)}, k^{(8,6)}, k^{(8,7)}$, and $k^{(8,8)}$. In 9-round attack, the guessing round key bytes are $k^{(1,1)}, k^{(1,2)}, k^{(1,3)}, k^{(1,5)}, k^{(1,8)}, k^{(2,1)}, k^{(8,5)}, k^{(9,1)}, k^{(9,2)}, k^{(9,6)}, k^{(9,7)}$, and $k^{(9,8)}$. In 10-round attack, the guessing round key bytes are $k^{(1,1)}, k^{(1,2)}, k^{(1,3)}, k^{(1,5)}, k^{(1,8)}, k^{(2,1)}, k^{(8,5)}, k^{(9,1)}, k^{(9,2)}, k^{(9,6)}, k^{(9,7)}, k^{(9,8)}$ and $k^{(10)}$. Since 6 bits of $k^{(8,5)}$ are included in $k^{(2,1)}$, the selected plaintext for 7,8,9 and 10-round attacks are $2^{26}$, $2^{26}$, $2^{66}$ and $2^{66}$, respectively. The complexities are $2^{26} \times (1 + 2^2 \times \frac{1}{56}) \approx 2^{26}$, $2^{26} \times (1 + 2^{40} \times (\frac{1}{8} + 2^2 \times \frac{1}{64}) \approx 2^{63}$, $2^{66} \times (1 + 2^{40} \times (\frac{1}{9} + 2^2 \times \frac{1}{72}) \approx 2^{103.4}$ and $2^{66} \times (1 + 2^{64} \times (\frac{1}{10} + (2^{40} \times (\frac{1}{10} + 2^2 \times \frac{1}{80})))) \approx 2^{167.3}$, respectively.

In 11-round attack, we add one round at the end of 10-round and check the output $x_R^{(7,8)}$. Then the attacking key bytes are $k^{(1,1)}, k^{(1,2)}, k^{(1,3)}, k^{(1,5)}, k^{(1,8)}, k^{(2,1)}, k^{(8,8)}, k^{(9,1)}, k^{(9,4)}, k^{(9,5)}, k^{(9,6)}, k^{(9,7)}, k^{(10)}$ and $k^{(11)}$.

In key schedule of Camellia, if $k_B$ is given, then $k_A \oplus k_R$ can be gotten by direct computation. So if $k_B$ and $(k_R)_L$ are given, then $(k_A)_L$ is known and if $k_B$

**Table 3.** The Summary of known attacks on Camellia

| Round | $FL/$<br>$FL^{-1}$ | Method | Data | Time<br>128-bit | Time<br>256-bit | Notes |
|---|---|---|---|---|---|---|
| 6 | N/Y | SLA | $2^{18}$ | $2^{20.4}$ | $2^{20.4}$ | This Paper |
| 6 | N/Y | SA | $2^{11.7}$ | $2^{112}$ | $2^{112}$ | [5] |
| 8 | No | TDC | $2^{83.6}$ | $2^{55.6}$ | $2^{63}$ | [8] |
| 8 | No | SLA | $2^{26}$ | $2^{68}$ | $2^{63}$ | This Paper |
| 8 | Yes | ISA | $2^{48}$ | $2^{98}$ | $2^{82}$ | [10] |
| 8 | Yes | SA | $2^{48}$ | — | $2^{116}$ | [17] |
| 9 | No | SLA | $2^{66}$ | $2^{84.8}$ | $2^{103.4}$ | This Paper |
| 9 | No | VSA | $2^{88}$ | $2^{90}$ | $2^{122}$ | [10] |
| 9 | No | DC | $2^{105}$ | $2^{105}$ | $2^{105}$ | [13] |
| 9 | No | CA | $2^{113.6}$ | $2^{121}$ | $2^{175.6}$ | [15] |
| 9 | Yes | ISA | $2^{48}$ | $2^{122}$ | $2^{146}$ | [10] |
| 9 | No | BA | $2^{123.9}$ | — | $2^{169.9}$ | [10] |
| 9 | No | HODC | $2^{21}$ | — | $2^{188}$ | [4] |
| 9 | Yes | SA | $2^{60.5}$ | — | $2^{202}$ | [17] |
| 10 | No | LA | $2^{120}$ | $2^{121}$ | $2^{121}$ | [13] |
| 10 | No | DC | $2^{105}$ | — | $2^{165.7}$ | [13] |
| 10 | No | SLA | $2^{66}$ | — | $2^{167.3}$ | This Paper |
| 10 | No | ICA | $2^{14}$ | — | $2^{207.4}$ | [10] |
| 10 | Yes | ISA | $2^{48}$ | — | $2^{210}$ | [10] |
| 10 | No | CA | $2^{14}$ | — | $2^{239.9}$ | [15] |
| 10 | No | RA | $2^{126.5}$ | — | $2^{240.9}$ | [15] |
| 10 | No | HODC | $2^{21}$ | — | $2^{254.7}$ | [4] |
| 11 | No | LA | $2^{120}$ | — | $2^{181.5}$ | [13] |
| 11 | No | SLA | $2^{66}$ | — | $2^{211.6}$ | This Paper |
| 11 | No | DC | $2^{105}$ | — | $2^{231.5}$ | [13] |
| 11 | No | VSA | $2^{88}$ | — | $2^{250}$ | [10] |
| 11 | N/Y | HODC | $2^{93}$ | — | $2^{255.6}$ | [4] |
| 12 | No | IPDC | $2^{120}$ | — | $2^{181}$ | [16] |
| 12 | No | LA | $2^{120}$ | — | $2^{245.4}$ | [13] |
| 12 | No | SLA | $2^{66}$ | — | $2^{249.6}$ | This Paper |

*Note 1.* BA: Boomerang Attack; CA: Collision Attack; DC: Differential Attack; HODC: High Order Differential Attack; ICA: Improved Collision Attack; IPDC: Impossible Differential Attack; LA: Linear Attack; RA: Rectangle Attack; SA: Square Attack; TDC: Truncated Differential Attack; VSA: Variant Square Attack;

and $(k_R)_R$ are given, then $(k_A)_R$ is known. In 192-and 256-Camellia, the third round key is $(k_R)_L$ and the 11th round key is $(k_A)_L$. The first two round keys are $(k_B)_L$ and $(k_B)_R$.

To improve the attack, we use chosen ciphertext attack, in which we select the ciphertext set $\{C_L \| C_R\}_\iota$ same as the plaintext $\{P_L \| P_R\}_\iota$ in 11-round chosen plaintext attack. Then, the attacking key bytes become $k^{(11,1)}$, $k^{(11,2)}$, $k^{(11,3)}$, $k^{(11,5)}$, $k^{(11,8)}$, $k^{(10,1)}$,$k^{(4,8)}$, $k^{(3,1)}$, $k^{(3,4)}$, $k^{(3,5)}$, $k^{(3,6)}$, $k^{(3,7)}$, $k^{(2)}$ and $k^{(1)}$. From $k^{(2)}$,$k^{(1)}$,

$k^{(11)}$ and $k^{12}$, we can get $k^{(3)}$ and $k^{(4)}$. In fact, 24 bits of $k^{(3,1)}$, $k^{(3,4)}$, $k^{(3,5)}$, $k^{(3,6)}$, $k^{(3,7)}$ can be get from $k^{(2)}$,$k^{(1)}$ and key bytes $k^{(11,1)}$, $k^{(11,2)}$, $k^{(11,3)}$, $k^{(11,5)}$ and $k^{(11,8)}$. Then the chosen ciphertext in 11-round attack is $2^{66}$ and the complexity is $2^{66} \times (1 + 2^{64} \times (\frac{1}{11} + 2^{64} \times (\frac{1}{11} + 2^{16} \times (\frac{1}{11} + 2^{8} \times \frac{1}{88})))) \approx 2^{211.6}$.

12-round attack adds one round at the beginning of 11-round selected plaintext attack and uses select ciphertext attack. So the selected ciphertext is same as 11-round chosen ciphertext attack and the guessing key bytes are $k^{(12,1)}$,$k^{(12,2)}$, $k^{(12,3)}$, $k^{(12,5)}$,$k^{(12,8)}$, $k^{(11,1)}$,$k^{(5,8)}$, $k^{(4,1)}$, $k^{(4,4)}$, $k^{(4,5)}$,$k^{(4,6)}$, $k^{(4,7)}$,$k^{(3)}$, $k^{(2)}$ and $k^{(1)}$. The $k^{(5)}$ is same as part of $k^{(11)}$ and $k^{12}$. From $k^{(2)}$, $k^{(1)}$, $k^{(12,1)}$,$k^{(12,2)}$, $k^{(12,3)}$, $k^{(12,5)}$,$k^{(12,8)}$ and $k(11,1)$, we can get 46 bits of $k^{(4,1)}$, $k^{(4,4)}$, $k^{(4,5)}$,$k^{(4,6)}$, $k^{(4,7)}$ and $k^{(3)}$. $k^{(5)}$ can be get from $k^{(1)}$,$k^{(2)}$ and $k^{(3)}$. Then, the 12-round attack requires $2^{66}$ ciphertext and the complexity is $2^{66} \times (1 + 2^{64} \times (\frac{1}{12} + 2^{64} \times (\frac{1}{12} + 2^{43} \times (\frac{1}{12} + 2^{16} \times (\frac{1}{12} + 1 \times \frac{1}{96}))))) \approx 2^{249.6}$.

### 5.3 The Influences of $FL/FL^{-1}$ Function

If $FL/FL^{-1}$ layer is included, the properties of XORing of sBoxes can not pass the $FL/FL^{-1}$ layer, so the attack is possible only by adding the rounds at the end of 6-round basic attack and guessing more key bytes of $FL/FL^{-1}$ layer. Then the attack is only possible for 7-round 128-Camellia and 9-round 256-Camellia.

## 6 Conclusions

The Square like attack is possible for the XORing of active Sboxes has some special properties. The rotation of key schedule of Camellia influence the security of Camellia. Table.3 gives a summary of known attacks on Camellia.

## Acknowledgments

The work is supported in part by NSFC 60573028 and by NUDT FBR JC07-02-02. We thank the anonymous reviewers for their very helpful comments.

## References

1. Aoki, K., Ichikawa, T., Kanda, M., et al.: Camellia: A 128-Bit block cipher suitable for multiple platforms-design and analysis. In: Ito, T., Abadi, M. (eds.) TACS 1997. LNCS, vol. 1281, pp. 39–56. Springer, Heidelberg (1997)
2. Daemen, J., Knudsen, L.R., Rijmen, V.: The block cipher SQUARE. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 149–165. Springer, Heidelberg (1997)
3. Daemen, J., Rijmen, V.: The Design of Rijndael, AES - The Advanced Encryption Standard. Springer, Heidelberg (2002)
4. Hatano, Y., Sekine, H., Kaneko, T.: Higher order differential attack of Camellia (II). In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, Springer, Heidelberg (2003)

5. He, Y., Qing, S.: Square attack on reduced Camellia cipher. In: Qing, S., Okamoto, T., Zhou, J. (eds.) ICICS 2001. LNCS, vol. 2229, pp. 238–245. Springer, Heidelberg (2001)
6. Kanda, M., Matsumoto, T.: Security of Camellia against truncated differential cryptanalysis. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, Springer, Heidelberg (2002)
7. Kawabata, T., Kaneko, T.: A study on higher order differential attack of Camellia.: The 2nd open NESSIE workshop (2001)
8. Lee, S., Hong, S., Lee, S., Lim, J., Yoon, S.: Truncated differential cryptanalysis of Camellia. In: Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 32–38. Springer, Heidelberg (2002)
9. Ledig, H., Muller, F., Valette, F.: Enhancing collision attacks. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, Springer, Heidelberg (2004)
10. Lei, D., Chao, L., Feng, K.: New observation on Camellia. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 51–64. Springer, Heidelberg (2006)
11. NTT Information Sharing Platform Laboratories: Internationally standardized encryption algorithm form Japan ”Camellia”, avaliable at `http://info.isl.ntt.co.jp/crypt/camellia/dl/Camellia20061108v4_eng.pdf`
12. Shirai, T., Kanamaru, S., Abe, G.: Improved upper bounds of differential and linear characteristic probability for Camellia. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, Springer, Heidelberg (2002)
13. Shirai, T.: Differential, linear, boomerang and rectangle cryptanalysis of reduced-round Camellia. In: Proceedings of 3rd NESSIE workshop (November 2002)
14. Sugita, M., Kobara, K., Imai, H.: Security of reduced version of the block cipher Camellia against truncated and impossible differential cryptanalysis. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 193–207. Springer, Heidelberg (2001)
15. Wu, W., Feng, D., Chen, H.: Collision attack and pseudorandomness of reduced-round Camellia. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 256–270. Springer, Heidelberg (2004)
16. Wu, W., Zhang, W., Feng, D.: Impossible differential cryptanalyssi of ARIA and Camellia, JCST
17. Yeom, Y., Park, S., Kim, I.: On the security of Camellia against the Square attack. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 89–99. Springer, Heidelberg (2002)