Front. Electr. Electron. Eng. China 2010, 5(4): 482–487
DOI 10.1007/s11460-010-0095-x

RESEARCH ARTICLE

Xiangyang XU, Guangsheng ZHANG

Security research with Square attack to a variant Camellia cipher

Abstract This paper investigates the relation between the choice of S-boxes and Square attack. A variant Camellia, which uses only a single S-box instead of four, is proposed. The security of the variant Camellia against Square attack is studied in detail. Result shows that it needs only 28 chosen plaintexts to recover a byte of the 6th round-key of variant Camellias, while the original Camellia needs either 28 chosen plaintexts to recover a byte of the 6th round-key and a byte of some constant or 216 chosen plaintexts to recover a byte of the 6th round-key. Furthermore, Square attacks on other round-reduced variant Camellia are proposed, and the time complexity of 11-round attack is reduced from 2^{250} to $2^{225.5}$. The weaker variant Camellia indicates that the choice of S-box and the order of different S-boxes have influence on Square attack.

Keywords block cipher, Camellia, Square attack

1 Introduction

Square attack, proposed by Ref. [1], considers the propagation of sums of (many) ciphertexts with special inputs. It was first applied to the Square cipher that is of substitution permutation network structured (SPN-structured). Reference [2] first applied Square attack, employing a different term "saturation attack" to Feistel cipher. The so-called multiset attack, proposed by Ref. [3], is another name of Square attack. In fact, all of these attacks belong to the integral cryptanalysis [4], proposed by Knudsen et al., at FSE 2002.

Integrals exploit the simultaneous relationship between many encryptions, in contrast to differential cryptanalysis where only pairs of encryptions are considered. This feature makes it especially well-suited in analyzing ciphers with primarily bijective components that are not vulnerable to differential and linear cryptanalysis. This feature also makes integral an increasingly popular tool in the recent cryptanalysis works. At FSE 2008, Ref. [5] proposed the bit-pattern-based integral attack that can be seen as a complement of the traditional integral attack proposed in Ref. [4], since the traditional ones can only be applied to byte(word)-oriented ciphers, while the bit-pattern based ones can only be applied to bit-oriented ciphers.

Camellia [6] is a 128-bit block cipher proposed by NTT and Mitsubishi in 2000 and supports 128/192/256-bit keys. The design of Camellia is based on the Feistel structure with an SPN-structured round function, and the number of rounds is 18 for 128-bit key version and 24 for 192/256-bit key version. An FL/FL^{-1} function layer is inserted in every six rounds in order to thwart future unknown attacks. Before the first round and after the last round, there are pre- and post-whitening layers, respectively. Camellia had been submitted to the standardization and the evaluation projects, such as ISO/IEC JTC 1/SC 27, CRYPTREC, and NESSIE. It is one of the winners of the NESSIE project.

Since its publication, Camellia has been widely analyzed. In Ref. [7], the security against truncated differential cryptanalysis is studied, and it has been proved that 11 rounds are enough to make Camellia resilient to the byte-character-based truncated differential attacks. In Ref. [8], empowered by computer aids, security against higher order differential attack was studied. He and Qing found that 6-round Camellia is breakable by Square attack [9]. Reference [10] improved the known result about Square attack. Later, Ref. [11] adopted the equivalent structure of Feistel cipher that improved the known results of Square attack on Camellia. Reference [12] gave an efficient collision attack on Camellia, and later in Ref. [13], some

Received January 23, 2010; accepted May 14, 2010

Xiangyang XU (✉)
Department of Computer Science and Technology, Changsha University, Changsha 410003, China
E-mail: xxy@ccsu.cn

Guangsheng ZHANG
School of Computer, National University of Defense Technology, Changsha 410073, China

nontrivial 8-round impossible differential was given; based on which, Ref. [14] gave an effective attack on Camellia with up to 14 rounds.

To date, there are many ciphers that adopt multi-S-boxes instead of single S-box, and Camellia is one of them. Another example that adopts multi-S-boxes is ARIA [15], which is a 128-bit block cipher designed by a group of Korean experts in 2003. ARIA is an SPN cipher. To make the encryption and decryption alike, the designers of ARIA adopted two S-boxes, which are denoted by S_1 and S_2, as well as their inversions S_1^{-1} and S_2^{-1} to make the cipher involutional.

Although many ciphers adopt multi-S-boxes, however, how the multi-S-boxes influence the security of ciphers remains undiscovered. Reference [7] investigated truncated differentials and found that for byte-character-based truncated differentials, the multi-S-boxes case can decrease the truncated differential probabilities, thus making the cipher stronger against truncated differential attack. Reference [16] investigated the security of ARIA against integral attack and suggested that if the cipher adopts only single S-box or different order of the multi-S-boxes, security margins are different. The basic technique of Ref. [16] is a counting method: if different values of a set appear even times, the sum of all element of the correspondence set is zero; in other words, the set is balanced.

This paper focuses on how multi-S-boxes and their order will influence the security of Camellia against Square attack. Our results show that if Camellia adopts single S-box, the security margin will be decreased to design a cipher using multi-S-boxes, the order of these S-boxes should be chosen carefully; otherwise, the security of the ciphers with different orders against Square attack might be compromised.

The rest of this paper is organized as follows: Section 2 briefly describes the Camellia cipher, its variant (Camellia*), and the basis of Square attack. Section 3 focuses on finding Square distinguisher of Camellia*. In Sect. 4, Square attacks on some round-reduced Camellia* are presented. Finally, Sect. 5 concludes the paper.

2 Preliminaries

2.1 Description of Camellia

Camellia is an iterative block cipher with Feistel structure. Let the ith round input and output be (L_{i-1}, R_{i-1}) and (L_i, R_i), then

$$\begin{cases} L_i = F(k_i \oplus L_{i-1}) \oplus R_{i-1}, \\ R_i = L_{i-1}, \end{cases}$$

where F is the round function, and k_i is the round key, which is generated from a master key through the key schedule.

An FL/FL^{-1} function is inserted every six rounds in order to thwart future unknown attack, and the FL function is defined as follows:

$$y_{\mathrm{R}} = \Big((x_{\mathrm{L}} \cap kl_{\mathrm{L}}) <<< 1\Big) \oplus x_{\mathrm{R}},$$
$$y_{\mathrm{L}} = (y_{\mathrm{R}} \cup kl_{\mathrm{R}}) \oplus x_{\mathrm{L}},$$

where $\cap$ is the bit-wise AND operation, while $\cup$ is the bit-wise OR operation.

The round function F function contains three transformations, namely, key-addition, S-function, and P-function. S-function contains four types of nonlinear S-boxes S_1, S_2, S_3, and S_4, where S_2, S_3, and S_4 are variations of S_1. S-function maps $(x_1,x_2,...,x_8) \in \mathbb{F}_{2^8}^8$ to $(y_1,y_2,...,y_8) \in \mathbb{F}_{2^8}^8$, which is defined as

$$(y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8)$$
$$= \Big(S_1(x_1),S_2(x_2),S_3(x_3),S_4(x_4),S_2(x_5),S_3(x_6),S_4(x_7),S_1(x_8)\Big).$$

P-function maps $(y_1,y_2,...,y_8) \in \mathbb{F}_{2^8}^8$ to $(z_1,z_2,...,z_8) \in \mathbb{F}_{2^8}^8$:

$$\begin{aligned} z_1 &= y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8, \\ z_2 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8, \\ z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8, \\ z_4 &= y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7, \\ z_5 &= y_1 \oplus y_2 \oplus y_6 \oplus y_7 \oplus y_8, \\ z_6 &= y_2 \oplus y_3 \oplus y_5 \oplus y_7 \oplus y_8, \\ z_7 &= y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_8, \\ z_8 &= y_1 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7. \end{aligned}$$

Obviously, P is a linear transformation, and it can be easily computed that P^{-1}, the inverse of the P-function, is defined as

$$\begin{aligned} y_1 &= z_2 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8, \\ y_2 &= z_1 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8, \\ y_3 &= z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8, \\ y_4 &= z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7, \\ y_5 &= z_1 \oplus z_2 \oplus z_5 \oplus z_7 \oplus z_8, \\ y_6 &= z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8, \\ y_7 &= z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7, \\ y_8 &= z_1 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8. \end{aligned}$$

Since we assume that the round keys are independent with each other, the key schedule of Camellia is omitted, and we refer to Ref. [15] for more details.

To evaluate the influence of four S-boxes and different order of these S-boxes being used, we analyze the case where only single S-box is used, and this variant is all Camellia* whose S-function is replaced by

$$(y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8) = \Big(S(x_1),S(x_2),S(x_3),S(x_4),S(x_5),S(x_6),S(x_7),S(x_8)\Big),$$

where S is one of S_1, S_2, S_3, and S_4, and the FL/FL^{-1} is omitted. Other parts of Camellia and Camellia* are the same.

2.2 Basis of Square attack

The following definitions are essential when applying an integral attack.

Let a Λ-set be a set of 256 states that are all different in some of the state bytes (the active) and all equal in the other state bytes (the passive). We have

$$\forall x = (x_1,x_2,...,x_n),\ y = (y_1,y_2,...,y_n) \in \Lambda: \begin{cases} x_i \neq y_i, & \text{if } x_i \text{ is active,} \\ x_i = y_i, & \text{else.} \end{cases}$$

Let Γ-set (balanced set) be a set of 256 states that are all equal to zero in summation (the balanced). We have

$$\sum_{x\in\Gamma} x = 0.$$

Applying the S-function or key-addition on a Λ-set results in a Λ-set with the positions of the active bytes unchanged. The result set of applying P-function to a Λ-set is not always a Λ-set but always a Γ-set.

In practice, if a balanced set comes with a nonlinear transformation, the finding process is stopped. Thus, the determination of the property of balanced set after it passed through a nonlinear transformation is very important in finding integral distinguishers. Reference [16] determined the property of balanced set after it passes through a nonlinear by determining that different values in the set appear even times; thus, the corresponding set is a balanced one.

3 4.5-round Square distinguisher of Camellia*

Let the input and output of the ith round be (L_{i-1}, R_{i-1}) and (L_i, R_i), respectively, and the output of S-function and P-function be Z_i and Y_i, respectively. Let $X_{i,j}$ denote the jth byte of X_i, where X can represent L, R or Z, Y.

Assume that the input to Camellia* is

$$\begin{cases} P_{\mathrm{L}} = (c,c,c,c,c,c,c,c), \\ P_{\mathrm{R}} = (x,c,c,c,c,c,c,c), \end{cases}$$

where c denotes some constant value in $\mathbb{F}_{2^8}$ (which are not necessarily equal to each other at different positions). Thus

$$Z_2 = \Big(S(x \oplus t_1) \oplus t_2,c,c,c,c,c,c,c\Big),$$

where t_1 and t_2 are some unknown constants in $\mathbb{F}_{2^8}$. Let $f(x) = S(x \oplus t_1) \oplus t_2$. Since $S(x)$ is a one-to-one map, so is $f(x)$. After the P-function, we have

$$Y_2 = \Big(f(x) \oplus \alpha_1, f(x) \oplus \alpha_2, f(x) \oplus \alpha_3, \alpha_4, f(x) \oplus \alpha_5, \alpha_6, \alpha_7, f(x) \oplus \alpha_8\Big),$$

where $\alpha_1,\alpha_2,...,\alpha_8$ are some unknown constants.

Similarly, we have

$$Z_3 = \Big(S\Big(f(x) \oplus \beta_1\Big), S\Big(f(x) \oplus \beta_2\Big), S\Big(f(x) \oplus \beta_3\Big), \beta_4, S\Big(f(x) \oplus \beta_5\Big), \beta_6, \beta_7, S\Big(f(x) \oplus \beta_8\Big)\Big),$$

where $\beta_1,\beta_2,...,\beta_8$ are also some unknown constants.

Based on above, we can compute the expression of Y_3 and $L_3 = R_4$. Since each byte of L_3 is a sum of some active bytes and each byte of L_3 is balanced, this supports Ref. [7]'s claim as the 4-round Square distinguisher of Camellia.

After computing the expression of L_3, we can find that the 8th byte of L_3 satisfies

$$L_{3,8} = S\Big(f(x) \oplus \beta_1\Big) \oplus S\Big(f(x) \oplus \beta_5\Big) \oplus \gamma,$$

where γ is a constant.

Let $f(x) \oplus \beta_1 = y$, thus

$$L_{3,8} = S(y) \oplus S(y \oplus \beta_1 \oplus \beta_5) \oplus \gamma.$$

If $\beta_1 \oplus \beta_5 = 0$, $L_{3,8} = \gamma$ is a constant; if $\beta_1 \oplus \beta_5 \neq 0$, we have

$$S(y) \oplus S(y \oplus \beta_1 \oplus \beta_5) \oplus \gamma = S(y^*) \oplus S(y^* \oplus \beta_1 \oplus \beta_5) \oplus \gamma,$$

where $y^* = y \oplus \beta_1 \oplus \beta_5 \neq y$. Since $L_3 = R_4$, the following theorem holds.

Theorem 1 Assuming Camellia* is defined as above, if all the bytes of the left half of the input to Camellia* are fixed, and in the right half, all the bytes are fixed except the first one is active, then all the bytes of the right half of the output of the 4th round are balanced. Besides, the times that different values appear at the 8th byte, i.e., $Z_{4,8}$, are even integers.

According to Theorem 1, the times that different values of $L_{3,8}$ appear are even integers. Because the S-box is a bijective map, the times that different values of $Z_{4,8}$ appear are even integers. Thus, $Z_{4,8}$ is a balanced byte. Also, because $Z_{4,8}$ is the output of S-box, rather than a full round, the distinguisher shown in Theorem 1 is called a 4.5-round Square distinguisher of Camellia*.

In the original Camellia, we have

$$R_{4,8} = S_1(y) \oplus S_2(y \oplus \beta_1 \oplus \beta_5) \oplus \gamma,$$

by which we can only determine that $R_{4,8}$ is a balanced byte. If one wants to determine whether the times that different values of $R_{4,8}$ appear is even or odd, it is enough that the S-boxes at positions 1 and 5 are the same.

Reference [8] evaluated the security of Camellia against higher order differential attacks. According to the definition of higher order differences and by aid of computers, some higher order differences of round-reduced Camellia were found. In fact, the result of Theorem 1 will also be found by computers.

The results in this section show that, when a cipher adopts multi-S-boxes, in order to improve the immunity against Square attack, the designers must choose the order of the S-boxes carefully.

We can simply denote the Square distinguisher shown in Theorem 1 by ($P_{R,1}$, $Z_{4,8}$), which means that if only $P_{R,1}$ is active and other bytes are constants, $Z_{4,8}$ is a balanced byte. By the same techniques, we can find the following Square distinguishers of Camellia*: ($P_{R,2}$, $Z_{4,5}$), ($P_{R,3}$, $Z_{4,6}$), and ($P_{R,4}$, $Z_{4,7}$). Details of the proofs are omitted.

4 Square attacks on Camellia*

4.1 Square attack on 6-round Camellia*

To apply a 6-round Square attack, we adopt the method that has been used in Ref. [8] (See Fig. 1).

First, we have

$$P_L \oplus Y_2 \oplus Y_4 \oplus Y_6 = C_L.$$

Thus,

$$P_L \oplus C_L = Y_2 \oplus Y_4 \oplus Y_6 = P(Z_2 \oplus Z_4 \oplus Z_6),$$

which means that

$$P^{-1}(P_L \oplus C_L) = Z_2 \oplus Z_4 \oplus Z_6.$$

Thus, we have

$$\begin{aligned}\sum_{P_{R,1}} P^{-1}(P_L \oplus C_L)_8 &= \sum_{P_{R,1}} P^{-1}(C_L)_8 \\ &= \sum_{P_{R,1}} (Z_2 \oplus Z_4 \oplus Z_6)_8 \\ &= \sum_{P_{R,1}} Z_{2,8} \oplus \sum_{P_{R,1}} Z_{4,8} \oplus \sum_{P_{R,1}} Z_{6,8} \\ &= \sum_{P_{R,1}} Z_{6,8},\end{aligned}$$

according to which we have the following attack on 6-round Camellia*.

Step 1 Choose plaintexts with the following form where c is some constant not necessarily equal to each other at different positions, and x takes all value of $\mathbb{F}_{2^8}$:

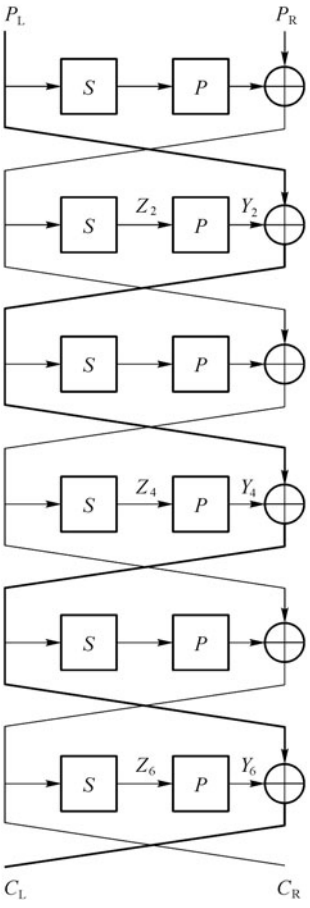

Fig. 1 Square attack on 6-round Camellia*

$$\begin{cases} P_L = (c,c,c,c,c,c,c,c), \\ P_R = (x,c,c,c,c,c,c,c), \end{cases}$$

the corresponding ciphertexts are denoted by ($C_L(x)$, $C_R(x)$). Then, compute

$$\text{sum} = \sum_x \left(P^{-1}\left(C_L(x)\right)\right)_8.$$

Step 2 Guess $k_{6,8}$ of the 6th round-key and compute

$$\text{sum}^* = \sum_x S(C_{R,8} \oplus k_{6,8}).$$

If $\text{sum}^* = \text{sum}$, keep $k_{6,8}$ as a candidate of the right subkey; otherwise, it is rejected.

Step 3 If necessary, repeat Steps 1 and 2 until the value of $k_{6,8}$ is uniquely determined.

For a wrong key, with probability 2^{-8}, $\text{sum}^* = \text{sum}$ holds. Thus, after choosing a structure of plaintexts, there are $(2^8-1)\times 2^{-8} \approx 1$ wrong keys that can pass the test. To uniquely determine the correct key, two structures are sufficient. Therefore, the data complexity of the above attack is $2\times 2^8 = 2^9$ chosen plaintexts. Accordingly, the time complexity of the attack is about $2^8\times 2^8 + 2\times 2^8$ times

lookup tables, and since there are 6×8 S-boxes in 6-round Camellia*, the time complexity is about $(2^8\times2^8+2\times2^8)/(6\times8)\approx2^{10.4}$ encryptions. Since the structure must be stored, the space complexity of the attack is 2^8 plaintext/ciphertext pairs.

4.2 Square attack on 7-round Camellia*

The 7-round attack is based on the 6-round attack with additional one round at the beginning.

Step 1 Choose plaintexts with the left half being

$$P_{\mathrm{L}}=(x,c,c,c,c,c,c,c),$$

where c is some constant not necessarily equal to each other at different positions; guess a value for $k_{1,1}$, and compute

$$P_{\mathrm{R}}=P\Big(S(x\oplus k_{1,1}),c,c,c,c,c,c,c\Big).$$

Then, compute the corresponding ciphertext of (P_{L}, C_{R}), say, (C_{L}, C_{R}), and last, compute

$$\mathrm{sum}=\sum_x (P^{-1}C_{\mathrm{L}})_8.$$

Step 2 Guess a value for $k_{7,8}$, then compute

$$\mathrm{sum}^*=\sum_x S(C_{\mathrm{R},8}\oplus k_{7,8}).$$

If $\mathrm{sum}^*=\mathrm{sum}$, put ($k_{1,1}$, $k_{6,8}$) as a candidate of the right keys; otherwise, it is rejected.

Step 3 If necessary, repeat Steps 1 and 2 until the value of ($k_{1,1}$, $k_{6,8}$) is uniquely determined.

If $k_{1,1}$ is the correct value, the output of the first round is

$$\begin{cases} L_1=(c,c,c,c,c,c,c,c),\\ R_1=(y,c,c,c,c,c,c,c),\end{cases}$$

thus the 6-round attack can be applied to the following 6-round cipher. Because a wrong value for $k_{7,8}$ can pass the test with probability 2^{-8}, three different structures of P_{L} will be needed to uniquely determine ($k_{1,1}$, $k_{6,8}$). Thus, the data complexity of the attack is $2^{17.6}$ chosen plaintexts, time complexity is $(2\times2^8\times2^8\times2^8+2^8\times2^8+2\times2^8)/(8\times7)\approx2^{19.2}$ encryptions, space complexity of the attack is 2^8 plaintext/ciphertext pairs, and 2^8 keys are candidates after analyzing the first structure.

This attack is valid even if an FL/FL^{-1} is inserted.

In fact, if there is no FL/FL^{-1} transformation, $(P^{-1}C_{\mathrm{L}})_8$, we only need to know five bytes of $(C_{\mathrm{L}})_8$, thus when FL/FL^{-1} is added, we need to guess another 5×8 bits of k_{l} and 8 bits of k_{r}, where k_{l} and k_{r} stand for the left and right halves of the correspondence subkey. Therefore, the number of structures must satisfy

$$(2^{3\times8}\times2^{5\times8}\times2^8-1)\times(2^{-8})^N<1,$$

which tells that $N=9$ is enough. Therefore, the data complexity is $2^{16}\times9\approx2^{19.1}$ chosen plaintexts, and the time complexity is $2^{18.2}\times2^{6\times8}=2^{66.2}$ encryptions.

4.3 Square attack on 11-round Camellia*

The 11-round attack is based on the 6-round attack with additional two rounds at the beginning and three rounds at the end. In the two rounds at the beginning, it needs to guess six bytes subkeys; and in the three rounds at the end, it needs to guess 22 bytes subkeys.

Step 1 Guess a value for $k_{2,1}$, and

$$P_{\mathrm{L}}=\Big(S(x\oplus k_{2,1}),S(x\oplus k_{2,1}),S(x\oplus k_{2,1}),c,S(x\oplus k_{2,1}),c,c,S(x\oplus k_{2,1})\Big),$$

then guess $k_{1,1}$, $k_{1,2}$, $k_{1,3}$, $k_{1,5}$, $k_{1,8}$ and compute

$$P_{\mathrm{R}}=P\Big(S\Big(S(x\oplus k_{2,1})\oplus k_{1,1}\Big),S\Big(S(x\oplus k_{2,1})\oplus k_{1,2}\Big),S\Big(S(x\oplus k_{2,1})\oplus k_{1,3}\Big),c,S\Big(S(x\oplus k_{2,1})\oplus k_{1,5}\Big),c,c,S\Big(S(x\oplus k_{2,1})\oplus k_{1,8}\Big)\Big).$$

Step 2 Guess all bytes of the 11th round-key (eight bytes) and compute (L_{10}, R_{10}), then guess all bytes of the 10th round-key (eight bytes) and compute ($L_{9,8}$, R_9); guess $k_{9,1}$, $k_{9,4}$, $k_{9,5}$, $k_{9,6}$, $k_{9,7}$ and compute ($L_{8,(1,4,5,6,7)}$, $R_{8,8}$); guess $k_{8,8}$ and check whether the following equation holds:

$$\sum_x S(R_{8,8}\oplus k_{8,8})=\sum_x(L_{8,1}\oplus L_{8,4}\oplus L_{8,5}\oplus L_{8,6}\oplus L_{8,7}).$$

If the equation does not hold, the combination of the correspondence subkeys is a wrong one.

Step 3 If necessary, repeat Steps 1 and 2 until the combination of the subkeys is uniquely determined.

To uniquely determine the candidates, it needs 29 different structures of P_{L}. Thus, the data complexity of the attack is $29\times2^8\times2^{40}\approx2^{52.9}$ chosen plaintexts; the time complexity is $(2^8\times2^8\times2^{40}\times2^{22}\times8+\cdots)/(8\times11)\approx2^{225.5}$ encryptions; and the space complexity is 2^{216}.

5 Conclusion

This paper primarily investigated the relationship between the order of S-boxes and immunity of ciphers against Square attack. Results in this paper show that, if Camellia adopts only a single S-box instead of four S-boxes, the security of Camellia against Square attack decreased dramatically. Also, if the order of the four S-boxes is changed, the security of Camellia against Square attack is also decreased. See Table 1 for the comparison of these

Table 1 Square attack on Camellia and Camellia*

attack	rounds	data	time	source
Camellia	6	2^{56}	2^{56}	Ref. [10]
Camellia	6	$2^{9.6}$	2^{18}	Ref. [11]
Camellia*	6	2^{9}	$2^{10.4}$	Sect. 4.1
Camellia	7	$2^{58.3}$	$2^{80.2}$	Ref. [10]
Camellia	7	$2^{26.8}$	$2^{33.5}$	Ref. [11]
Camellia*	7	$2^{17.6}$	$2^{19.2}$	Sect. 4.2
Camellia	11	$2^{84.8}$	2^{250}	Ref. [11]
Camellia*	11	$2^{52.9}$	$2^{225.5}$	Sect. 4.3

results. In the design of a cipher, multi-S-boxes can improve the security of the cipher, given that one can carefully chooses the order of the S-boxes being used.

Acknowledgements This work was supported by the Planned Science and Technology Project of Hunan Province of China (No. 2010FJ4079) and A Project Supported by Scientific Research Fund of Hunan Provincial Education Department.

References

1. Daemen J, Knudsen L R, Rijmen V. The block cipher Square. In: Proceedings of the 4th International Workshop on Fast Software Encryption. Lecture Notes in Computer Science, 1997, 1267: 149–165
2. Lucks S. The saturation attack—a bait for Twofish. In: Proceedings of the 8th International Workshop on Fast Software Encryption. Lecture Notes in Computer Science, 2002, 2355: 1–15
3. Biryukov A, Shamir A. Structural cryptanalysis of SASAS. In: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. Lecture Notes in Computer Science, 2001, 2045: 395–405
4. Knudsen L R, Wagner D. Integral cryptanalysis. In: Proceedings of the 9th International Workshop on Fast Software Encryption. Lecture Notes in Computer Science, 2002, 2365: 112–127
5. Reza Z'aba M, Raddum H, Henricksen M, Dawson E. Bit-pattern based integral attack. In: Proceedings of the 15th International Workshop on Fast Software Encryption. Lecture Notes in Computer Science, 2008, 5086: 363–381
6. Aoki K, Ichikawa T, Kanda M, Matsui M, Moriai S, Nakajima J, Tokita T. Camellia: a 128-bit block cipher suitable for multiple platforms—design and analysis. In: Proceedings of the 7th Annual International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, 2001, 2012: 39–56
7. Kanda M, Matsumoto T. Security of Camellia against truncated differential cryptanalysis. In: Proceedings of the 8th International Workshop on Fast Software Encryption. Lecture Notes in Computer Science, 2002, 2355: 286–299
8. Hatano Y, Sekine H, Kaneko T. Higher order differential attack of Camellia (II). In: Proceedings of the 9th Annual International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, 2003, 2595: 129–146
9. He Y P, Qing S H. Square attack on reduced Camellia cipher. In: Proceedings of the 3rd International Conference on Information and Communications Security. Lecture Notes in Computer Science, 2001, 2229: 238–245
10. Yeom Y, Park S, Kim I. On the security of Camellia against the Square attack. In: Proceedings of the 9th International Workshop on Fast Software Encryption. Lecture Notes in Computer Science, 2002, 2365: 89–99
11. Lei D, Chao L, Feng K Q. New observation on Camellia. In: Proceedings of the 12th International Workshop on Selected Areas in Cryptography. Lecture Notes in Computer Science, 2006, 3897: 51–64
12. Wu W L, Feng D G. Collision attack on reduced-round Camellia. Science in China, Series F: Information Sciences, 2005, 48(1): 78–90
13. Wu W L, Zhang W T, Feng D G. Impossible differential cryptanalysis of reduced-round ARIA and Camellia. Journal of Compute Science and Technology, 2007, 22(3): 449–456
14. Lu J Q, Kim J, Keller N, Dunkelman O. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In: Proceedings of the Cryptopgraphers' Track at the RSA Conference on Topics in Cryptology. Lecture Notes in Computer Science, 2008, 4964: 370–386
15. Kwon D, Kim J, Park S, Sung S H, Sohn Y, Song J H, Yeom Y, Yoon E-J, Lee S, Lee J, Chee S, Han D, Hong J. New block cipher: ARIA. In: Proceedings of the 6th International Conference on Information Security and Cryptology. Lecture Notes in Computer Science, 2004, 2971: 432–445
16. Li P, Sun B, Li C. Integral cryptanalysis of ARIA. In: Proceedings of Information Security and Cryptology—Inscrypt 2009. 2009