# Security Analysis on S-Box of LBlock Algorithm Based on Trace-Driven Cache Timing Attack

*Yu Xi*[1], *Cai Hong-liu*[1], *Chen Cai-sen*[2], *Xiang Yang-xia*[1]
(1. Department of Information Engineering, Academy of Armored Forces Engineering, Beijing, 100072)
(2. Ministry of Science Research, Academy of Armored Forces Engineering, Beijing, 100072)

**Abstract**: Based on the Cache timing attack for lightweight block cipher, this paper mainly analyzes the nonlinear structure characteristics of S-box in cryptographic algorithms. Firstly, the algebraic properties of S-box are analyzed, the truth-table of S-box is derived by structure characteristics, and the relation algebra expression of S-box between inputs and outputs are obtained. Secondly, with reference of encryption process of the LBlock algorithm and the structure of round function F, the operation expression of each round and the algebra expressions of look-up index for S-box are deduced. Finally, based on the principle and model of the Trace-driven Cache timing attack, the kernel expression for key analysis is presented, which is used for LBlock algorithm. The conclusion shows that the LBlock algorithm could be attacked by Cache timing attack.

**Key words**: LBlock Algorithm; Cache Timing Attack; Algebra Expression; S-box; Security Analysis

## 1 Introduction

With the development of information security, lightweight cryptographic algorithms have been used on some devices; including the RFID electronic tag, wireless sensor network, mobile intelligent terminal and so on. In 2011, LBlock algorithm[1] was proposed by Wu Wenling and Zhang Lei, which was lightweight block cipher based on 32-round Feistel. With the round function, plaintext is iterated many times and gets ciphertext, and the round function are generated from main key, the key length is 80 bits and the packet length is 60 bits.

Lightweight cipher algorithm[2] has the advantages of small amount of processing data, low data throughput, and little storage. For algorithm, Robustness and security are improved while not reducing the security. For example, Boolean function is improved and S-box is same, so that resource requirements are reduced to algorithm. According to the iterative structure characteristics of block cipher, traditional safety analysis methods are mainly based on the statistical method of linear analysis[3], the differential cryptanalysis[4], the cube attack[5] and the algebraic attack based on the solution of equations[6], etc. Recently, with the development of the side-channel attack in the field of the cryptanalysis, the attacker may obtain the side-channel information such as power consumption, electromagnetic, timing and so on. The key can be got with side-channel and key correlation, which is the hotspot of the cryptanalysis[7]. Combing with traditional cryptanalysis method in Side-channel attack, the algebra attack and the cube side channel attack are proposed. The cube side channel attack[8] are presented by Shamir, who can gets one bit from the intermediate state of algorithm and gets the key information. In 2009, the cube side channel attack of PRESENT algorithm[9] is verified by Yang and others. Cache behavior is used for the side-channel leaked information, which is proposed by Kocher[10] and Kelsey[11] and becomes new hot spots in the side channel attack. The main idea proposed the idea of taking the behavior information of the high speed memory Cache as the side channel leaked information, the Cache attack has. The main idea of the attack is that attacker acquires the key information from the Cache access behavior in the process of execution of cryptographic algorithms, and key can be got by cache timing information and key relativity analysis, which poses a great threat to the security of the block cipher algorithm with S-box looking-up, such as DES, AES, ARIA algorithm. In addition, the attack can be done with RSA of sliding

Yu Xi(1992—), female, Shaanxi Xi'an, master student on cyber-security; Qian; Cai Hongliu (1960—), female, Shandong Rongcheng, associate professor, master, cyber-security.

window algorithm.

During the Cache timing attack, how to accurately obtain the information of Cache access behavior as well as the correlation analysis with the S box look-up index and the subkey are very important to key analysis. In this paper, based on track driven cache timing attack principle, algebra expressions are analyzed by LBlock algorithm, S-box algebra expression are given, round computation expressions and look-up algebra expressions of S-box are deduced by algorithm and round function results. Subkey expressions are deduced with round key algebra expression and Cache access information and S-box look-up index.

## 2 LBlock algorithm analysis

### 2.1 Overview of LBlock algorithm

The block length of LBlock is 64-bit, and the key length is 80-bit. It employs a variant Feistel structure and consists of 32 rounds. The specification of LBlock consists of three parts: encryption algorithm, decryption algorithm and key scheduling.

The encryption algorithm of LBlock consists of a 32-bit iterative structure which is a variant of Feistel network. Where $M = X_1 \| X_0$, $M$ is a 64-bit plaintext, and encryption can be expressed as follows.

(1) For $i = 2, 3, \cdots, 33$

$X_i = F(X_{i-1}, K_{i-1}) \oplus (X_{i-2} \lll 8)$

(2) where $C = X_{32} \| X_{33}$, $C$ is 64-bit ciphertext.

The encryption procedure is illustrated in Figure 1.

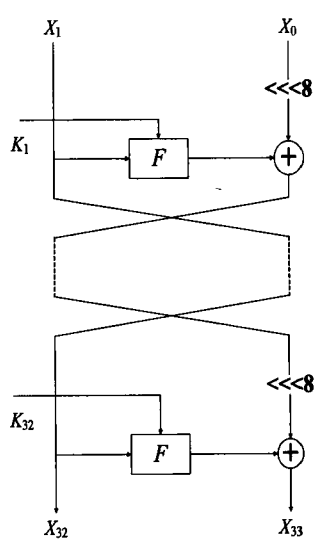


**Figure 1 Encryption procedure of LBlock**

Specifically, the components used in each round are defined as follows.

(1) Round function $F$

The round function $F$ is defined as follows, where $S$ and $P$ denote the confusion and diffusion functions which will be defined later.

$$F(X, K_i) = P(S(X \oplus K_i)) \in \{0,1\}^{32}$$

(2) Confusion function $S$

Confusion function $S$ denotes the non-linear layer of round function $F$, and it consists of eight 4-bit S-boxes $S_i$ in parallel.

$$S: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$

$$Y = Y_7 \| Y_6 \| Y_5 \| Y_4 \| Y_3 \| Y_2 \| Y_1 \| Y_0 \rightarrow Z$$
$$= Z_7 \| Z_6 \| Z_5 \| Z_4 \| Z_3 \| Z_2 \| Z_1 \| Z_0$$

$$Z_7 = s_7(Y_7), Z_6 = s_6(Y_6), Z_5 = s_5(Y_5), Z_4 = s_4(Y_4)$$
$$Z_3 = s_3(Y_3), Z_2 = s_2(Y_2), Z_1 = s_1(Y_1), Z_0 = s_0(Y_0)$$

The contents of eight 4-bit S-boxes are listed in Table 1.

**Table 1 Contents of the *S*-boxes used in LBlock**

| S box | The value of the table element |
|---|---|
| $S_0$ | 14,9,15,0,13,4,10,11,1,2,8,3,7,6,12,5 |
| $S_1$ | 4,11,14,9,15,13,0,10,7,12,5,7,2,8,1,3 |
| $S_2$ | 1,14,7,12,15,13,0,6,11,5,9,3,2,4,8,10 |
| $S_3$ | 7,6,8,11,0,15,3,14,9,10,12,13,5,2,4,1 |
| $S_4$ | 14,5,15,0,7,2,12,13,1,8,4,9,11,10,6,3 |
| $S_5$ | 2,13,11,12,15,14,0,9,7,10,6,3,1,8,4,5 |
| $S_6$ | 11,9,4,14,0,15,10,13,6,12,5,7,3,8,1,2 |
| $S_7$ | 13,10,15,0,14,4,9,11,2,1,8,3,7,5,12,6 |
| $S_8$ | 8,7,14,5,15,13,0,6,11,12,9,10,2,4,1,3 |
| $S_9$ | 11,5,15,0,7,2,9,13,4,8,1,12,14,10,3,6 |

(3) Diffusion function $P$

Diffusion function $P$ is defined as a permutation of eight 4-bit words, and it can be expressed as the following equations.

$$P: \{0,1\}^{32} \rightarrow \{0,1\}^{32}$$

$$Z = Z_7 \| Z_6 \| Z_5 \| Z_4 \| Z_3 \| Z_2 \| Z_1 \| Z_0 \rightarrow U$$
$$= U_7 \| U_6 \| U_5 \| U_4 \| U_3 \| U_2 \| U_1 \| U_0$$

$$Z_7 = U_6, Z_6 = U_4, Z_5 = U_7, Z_4 = U_5$$
$$Z_3 = U_2, Z_2 = U_0, Z_1 = U_3, Z_0 = U_1$$

Figure 2 illustrates the structure of round function $F$ in detail.

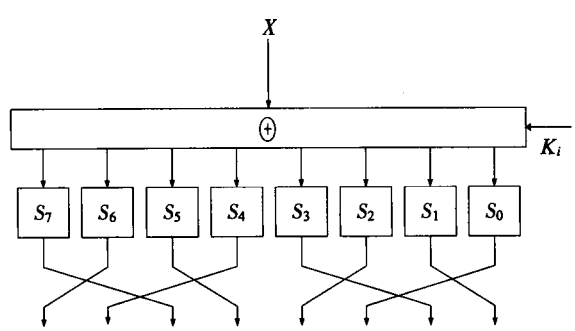


**Figure 2 Round function F**

According to the figure of the round function $F$, corresponding to 8 $S$ boxes, the 4-bit plaintext is as a set of the left 32-bit $X_i$, and it can be expressed from left to right as: $a_{i,7}$, $a_{i,6}$, $a_{i,5}$, $a_{i,4}$, $a_{i,3}$, $a_{i,2}$, $a_{i,1}$, $a_{i,0}$; In proportion, the round subkey $K_i$ also can be divided 4-bit to a set and expressed from left to right as: $K_{i,7}$, $K_{i,6}$, $K_{i,5}$, $K_{i,4}$, $K_{i,3}$, $K_{i,2}$, $K_{i,1}$, $K_{i,0}$.

Assuming that the right 32-bit plaintext is full of 0, take $S_7$ as example, the look-up index in the first round is $a_{1,7}\oplus K_{1,7}$, and the look-up index in the second round is $a_{2,7}\oplus K_{2,7}$.

As the encryption procedure of LBlock algorithm, the left 32-bit value $X_i$ each round can be expressed as:

$$X_i = P(S(X_{i-1},K_{i-1}))\oplus(X_{i-2}\lll 8)$$

therefore,

$$X_2 = P(S(X_1,K_1))\oplus(X_0\lll 8) = P(S(X_1,K_1))$$

As the figure of the the round function $F$ as shown, the output of the $S_6$ in the first round is corresponding to the input of the $S_7$ in the second round, it can be expressed as: $a_{2,7}=S_6(a_{1,6}\oplus K_{1,6})$.

So we can concluded that the look-up index of $S_7$ in the second round is $S_6(a_{1,6}\oplus K_{1,6})\oplus K_{2,7}$.

In a conclusion about the analysis above as following:

Assuming that the right 32-bit plaintext is full of 0, the look-up index of $S_7$ in the first round is $a_{1,7}\oplus K_{1,7}$, and the look-up index of $S_7$ in the second round is $S_6(a_{1,6}\oplus K_{1,6})\oplus K_{2,7}$.

This conclusion is also the key factors of getting the bit of related-key through analyzing the S box look-up index.

## 2.2 Key Scheduling

The 80-bit master key $K$ is stored in a key register and denoted as:

$$K = k_{79}k_{78}\cdots k_0$$

(1) Output the leftmost 32 bits of current content of register $K$ as round subkey $K_1$;

(2) For $i = 1, 2, \cdots, 31$, update the key register $K$ as follows:

a. $K\lll 29$;

b. $[k_{79}k_{78}k_{77}k_{76}] = S_9[k_{79}k_{78}k_{77}k_{76}]$, $[k_{75}k_{74}k_{73}k_{72}] = S_8[k_{75}k_{74}k_{73}k_{72}]$;

c. $[k_{50}k_{49}k_{48}k_{47}k_{46}]\oplus[i]_2$;

d. Output the leftmost 32 bits of current content of register $K$ as round subkey $K_{i+1}$.

As the same method, we can generate each round subkey, which is applied to calculated.

# 3 The nonlinear characteristic analysis of $S$-box in LBlock algorithm

## 3.1 The deduction of the truth-table of S-box

The input and output of $S$ box of LBlock algorithm are both 4-bit binary number. Assume that the input $X = x_3x_2x_1x_0$, of which the $x_3$ is the highest bit and the $x_0$ is the lowest bit, the output $Y = y_3y_2y_1y_0$, of which the $y_3$ is the highest bit and the $y_0$ is the lowest bit. According to contents of the S-boxes used in LBlock as Table 1 shown, take $S_0$ as example, when the input $X(x_3x_2x_1x_0)=0000$, the output $Y(y_3y_2y_1y_0)=1110$, the truth-table of $S_0$ can be got as shown in Table 2.

**Table 2 The truth-table of $S_0$**

| Item | The corresponding relation of value between $X$ and $Y$ | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $X(x_3x_2x_1x_0)$ | 0000 | 0001 | 0010 | 0011 | 0100 | 0101 | 0110 | 0111 |
| $Y(y_3y_2y_1y_0)$ | 1110 | 1001 | 1111 | 0000 | 1101 | 0100 | 1010 | 1011 |
| $X(x_3x_2x_1x_0)$ | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |
| $Y(y_3y_2y_1y_0)$ | 0001 | 0010 | 1000 | 0011 | 0111 | 0110 | 1100 | 0101 |

As the Table 2 shown, the truth-table of the output $y_0$, $y_1$, $y_2$, $y_3$ respectively can be obtained, which are corresponding to $X(x_3x_2x_1x_0)$ (from 0000 to 1111) in $S_0$ of the LBlock algorithm as shown in Table 3.

**Table 3 The truth-table of the output $y_0$, $y_1$, $y_2$, $y_3$ in $S_0$ of the LBlock algorithm**

| Output in $S_0$ | The truth of output $y$ |
|---|---|
| $y_0$ | 0110100110011001 |
| $y_1$ | 1010001101011100 |
| $y_2$ | 1010110000001111 |
| $y_3$ | 1110101100100010 |

Suppose that the Boolean function relations of output $Y(y_3y_2y_1y_0)$ and input $X(x_3x_2x_1x_0)$ in S box of the LBlock algorithm as follows:

$$y_i = f_i(x_3,x_2,x_1,x_0)$$

Among them, $i = 0, 1, 2, 3$, take $S_0$ as example, according to the truth-table of the output $y_0$, $y_1$, $y_2$, $y_3$ in $S_0$ of the LBlock algorithm to solve the Boolean function expressions, take $y_0$ as example, there are 8 terms of the value with "1" in truth-table are 8, it can be expressed as:

$$y_0 = \sum_j m_j = m_{0001}\oplus m_{0010}\oplus m_{0100}\oplus m_{0111}\oplus m_{1000}\oplus m_{1011}\oplus m_{1100}\oplus m_{1111} \quad (1)$$

Among them, $j = x_3x_2x_1x_0$, and 8 terms of the value with "1" are $m_{0001}$, $m_{0010}$, $m_{0100}$, $m_{0111}$, $m_{1000}$,

$m_{1100}$, $m_{1111}$. 8 terms can be expanded one by one, take $m_{0001}$ as example, meanwhile $j = x_3x_2x_1x_0 = 0001$, make the term of the value with "1" indicated as $x_i$ and the term of the value with "0" indicated as $\overline{x_i}$[12], so $m_{0001} = \overline{x_3}\,\overline{x_2}\,\overline{x_1}\,\overline{x_0}$, then put into the equation:

$$m_{0001} = (x_3 \oplus 1)(x_2 \oplus 1)(x_1 \oplus 1)x_0$$

Expand it,

$$m_{0001} = x_3x_2x_1x_0 \oplus x_3x_2x_0 \oplus x_3x_1x_0 \oplus x_2x_1x_0 \oplus x_3x_0 \oplus x_2x_0 \oplus x_1x_0 \oplus x_0$$

As the same way,

$$m_{0010} = x_3x_2x_1x_0 \oplus x_3x_2x_1 \oplus x_3x_1x_0 \oplus x_2x_1x_0 \oplus x_3x_1 \oplus x_2x_1 \oplus x_1x_0 \oplus x_1$$

$$m_{0100} = x_3x_2x_1x_0 \oplus x_3x_2x_1 \oplus x_3x_2x_0 \oplus x_2x_1x_0 \oplus x_3x_2 \oplus x_2x_1 \oplus x_2x_0 \oplus x_2$$

$$m_{0111} = x_3x_2x_1x_0 \oplus x_2x_1x_0$$

$$m_{1000} = x_3x_2x_1x_0 \oplus x_3x_2x_1 \oplus x_3x_2x_0 \oplus x_3x_1x_0 \oplus x_3x_2 \oplus x_3x_1 \oplus x_3x_0 \oplus x_3$$

$$m_{1011} = x_3x_2x_1x_0 \oplus x_3x_1x_0$$

$$m_{1100} = x_3x_2x_1x_0 \oplus x_3x_2x_1 \oplus x_3x_2x_0 \oplus x_3x_2$$

$$m_{1111} = x_3x_2x_1x_0$$

Add up and divide out the term of the value with "0" to acquire the $y_0$, the other three output $y_1$, $y_2$, $y_3$ can be acquired with the same way.

In a conclusion about the analysis above as following:

Setting the input of S box $X = x_3x_2x_1x_0$ and the output $Y = y_3y_2y_1y_0$, resulted can be got by the truth-table of the LBlock algorithms in $S_0$, as follows:

$$y_0 = x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_2x_3$$

$$y_1 = 1 \oplus x_0 \oplus x_2 \oplus x_0x_2 \oplus x_1x_2 \oplus x_3$$

$$y_2 = 1 \oplus x_0 \oplus x_0x_2 \oplus x_1x_2 \oplus x_3 \oplus x_0x_3 \oplus x_2x_3 \oplus x_0x_2x_3 \oplus x_1x_2x_3$$

$$y_3 = 1 \oplus x_0x_1 \oplus x_0x_2 \oplus x_3 \oplus x_1x_3 \oplus x_0x_2x_3$$

The algebraic expressions of other $S$ box ($S_1 \cdots S_9$) can be obtained in the same method.

### 3.2 The algebraic expressions of round subkey

According to the key scheduling algorithm described in chapter 2.2 and the algebraic expressions between input and output of S box derived in chapter 3.1, the algebraic expression of each round key of LBlock algorithm can be obtained.

The 80-bit master key $K$ is stored in a key register and denoted as:

$$K = k_{79}k_{78}\cdots k_0$$

The second round subkey $K_2$ can be expressed as:

$$\begin{aligned}K_2 = \{&1 \oplus k_{47} \oplus k_{49} \oplus k_{47}k_{49} \oplus k_{48}k_{49} \oplus k_{50},\\ &k_{47} \oplus k_{48} \oplus k_{49} \oplus k_{50} \oplus k_{49}k_{50},\\ &1 \oplus k_{47} \oplus k_{47}k_{49} \oplus k_{48}k_{49} \oplus k_{50} \oplus k_{47}k_{50} \oplus k_{49}k_{50}\\ &\oplus k_{47}k_{49}k_{50} \oplus k_{48}k_{49}k_{50},\\ &1 \oplus k_{47}k_{48} \oplus k_{47}k_{49} \oplus k_{50} \oplus k_{48}k_{50} \oplus k_{47}k_{49}k_{50},\\ &1 \oplus k_{43} \oplus k_{43}k_{45} \oplus k_{44}k_{45} \oplus k_{43}k_{46} \oplus k_{45}k_{46}\\ &\oplus k_{43}k_{45}k_{46} \oplus k_{44}k_{45}k_{46},\\ &k_{43} \oplus k_{44} \oplus k_{43}k_{44} \oplus k_{45} \oplus k_{43}k_{45} \oplus k_{44}k_{46}\\ &\oplus k_{45}k_{46} \oplus k_{43}k_{45}k_{46},\\ &k_{43} \oplus k_{44} \oplus k_{45} \oplus k_{46} \oplus k_{45}k_{46},\\ &k_{43} \oplus k_{45} \oplus k_{43}k_{45} \oplus k_{44}k_{45} \oplus k_{46},\\ &k_{42}, k_{41}, k_{40}, k_{39}, k_{38}, k_{37}, k_{36}, k_{35}, k_{34}, k_{33}, k_{32}, k_{31},\\ &k_{30}, k_{29}, k_{28}, k_{27}, k_{26}, k_{25}, k_{24}, k_{23}, k_{22}, k_{21}, k_{20}, k_{19}\}\end{aligned}$$

in the same way, subkey $K_3$ is obtained in the third round, and so on.

## 4 The key analysis of the trace driven Cache timing attack based on the feature of S-Box index

### 4.1 The principle of the trace driven Cache timing attack and the feature of S-Box index

The trace drive Cache attack is a very effective side channel[13] analysis technology. The principle is that the same S box always be accessed repeatedly in the implementation of the encryption procedure, which produce the Cache hit and Cache miss can be used to speculate the key. During the S-box access, the required element is in the Cache as Cache hit while the required element is not in the Cache as Cache miss. In the case of Cache miss, the processor will load the whole memory block of the element into one Cache line.

In the experiment, Cache is cleaned firstly, thus the first time of looking-up S box may produce a Cache miss. When the second time of looking-up, it may produce a Cache hit or Cache miss. If it produce a Cache hit, the required element is in the Cache line which loaded memory block after the first time looking-up table. And every time a look-up index are used, the highest 2 bits of index is corresponding to Cache line, while the lowest 2 bits is corresponding to the address in the Cache line, namely the highest 2 bits of twice look-up index are equal.

In conclusion, as following:

Supposing the look-up index of S box is expressed as $Y$, the highest 2 bits is expressed as $\langle Y \rangle$, if the twice look-up index of S box is $Y_1$, $Y_2$ and the second time of looking-up produce a Cache hit, so that $\langle Y_1 \rangle = \langle Y_2 \rangle$.

### 4.2 The correlation analysis between the key and S box of LBlock algorithm

In this section, with three conclusions above

mentioned, the correlation analysis[14] are make between the key and S box of LBlock algorithm with constructing the Cache hit of S box in LBlock algorithm encryption.

Assuming that the right 32-bit plaintext of the first round is full of 0, and randomly select the highest 4-bit plaintext $a_{i,7}$ and the second highest 4-bit plaintext $a_{i,6}$ to make a Cache hit in second round of looking-up $S_7$. Based on section 2.1 and 4.1, formulas are derived that:

$$S_6(a_{1,6}\oplus K_{1,6})\oplus K_{2,7} = a_{1,7}\oplus K_{1,7} \quad (2)$$

namely,

$$S_6(a_{1,6}\oplus k_{75}k_{74}k_{73}k_{72})\oplus k_{50}k_{49}k_{48}k_{47} = a_{1,7}\oplus k_{79}k_{78}k_{77}k_{76}$$

Therein, the highest 2 bits of look-up index of $S_7$ is correlative with 10 bits key: $k_{79}$, $k_{78}$, $k_{75}$, $k_{74}$, $k_{73}$, $k_{72}$, $k_{50}$, $k_{49}$, $k_{48}$, $k_{47}$. And the highest bit of look-up index of $S_7$ is correlative with 9 bits key: $k_{79}$, $k_{75}$, $k_{74}$, $k_{73}$, $k_{72}$, $k_{50}$, $k_{49}$, $k_{48}$, $k_{47}$, while the second highest bit of look-up index of $S_7$ is correlative with 9 bits key: $k_{78}$, $k_{75}$, $k_{74}$, $k_{73}$, $k_{72}$, $k_{50}$, $k_{49}$, $k_{48}$, $k_{47}$. In this case, we select 12 sets of plaintexts, composed to 12 sets of equations, to acquire the unique solution, which may restore the 10 bits key related to the highest 2 bits of look-up index of $S_7$. In conclusion, there are times of the discriminant algorithm to restore the 10 bits key: $k_{79}$, $k_{78}$, $k_{75}$, $k_{74}$, $k_{73}$, $k_{72}$, $k_{50}$, $k_{49}$, $k_{48}$, $k_{47}$.

In the same way, the 8 bits key are got: $k_{67}$, $k_{66}$, $k_{65}$, $k_{64}$, $k_{46}$, $k_{45}$, $k_{44}$, $k_{43}$, analyzing the highest 2 bits of look-up index of $S_6$ in the first and second round of LBlock algorithm encryption.

Further analysis of the highest 2 bits of look-up index of other S box, we ultimately restore the 49 bits key, specifically situations of every time the key corresponding to the highest 2 bits of look-up index of S box as shown in Table 4.

**Table 4 The key corresponding to the highest 2 bits of look-up index of S box in the second round**

| S box | The key corresponding to the highest 2 bits of look-up index | Number of the keys |
|---|---|---|
| $S_7$ | $k_{79}, k_{78}, k_{75}, k_{74}, k_{73}, k_{72}, k_{50}, k_{49}, k_{48}, k_{47}$ | 10 |
| $S_6$ | $k_{67}, k_{66}, k_{65}, k_{64}, k_{46}, k_{45}, k_{44}, k_{43}$ | 8 |
| $S_5$ | $k_{77}, k_{76}, k_{71}, k_{70}, k_{42}, k_{41}$ | 6 |
| $S_4$ | $k_{69}, k_{68}, k_{38}, k_{37}$ | 4 |
| $S_3$ | $k_{63}, k_{62}, k_{59}, k_{58}, k_{57}, k_{56}, k_{34}, k_{44}$ | 8 |
| $S_2$ | $k_{51}, k_{30}, k_{29}$ | 3 |
| $S_1$ | $k_{61}, k_{60}, k_{55}, k_{54}, k_{26}, k_{25}$ | 6 |
| $S_0$ | $k_{53}, k_{52}, k_{22}, k_{21}$ | 4 |

If every time the number of the sets of chosen-plaintexts is more than the number of the bits of key related look-up index of S box by 2. From Table 4, there are 12 + 10 + 8 + 6 + 10 + 5 + 8 + 6 = 65 sets of chosen-plaintexts and approximately $12 \times 2^{10} + 10 \times 2^8 + 8 \times 2^6 + 6 \times 2^4 + 10 \times 2^8 + 5 \times 2^3 + 8 \times 2^6 + 6 \times 2^4 \approx 2^{14.18}$ times of the discriminant operation.

There are 32 rounds which each with 8 S boxes in LBlock algorithm, and at the same time, there are 2 S boxes participated at most each criterion operation. So once discriminant algorithm can be regarded as $2/(32 \times 8) = 1/128$ times of LBlock encryption operations. Above all, there are totally about $2^{7.18}$ times of LBlock encryption arithmetic to restore the 49 bits key in Table 4.

In the same method, analyzing the look-up index of S box in the third and fourth round, the more related keys are got, as shown in Table 5.

Based on the above analysis, there are 5 + 8 + 4 + 6 + 6 + 4 + 4 + 4 = 41 sets of chosen-plaintexts and $2^6$ times of LBlock encryption arithmetic at most to restore the remaining 6 bits key with exhaustion method, ignoring the discriminant time.

In conclusion, there are totally 106 sets of chosen-plaintexts in the whole attack andapproximately $2^{7.18} + 2^6 \approx 2^{7.71}$ times of LBlock encryption operations to restore all the key.

All in all, The LBlock algorithm exists the possibility of being attacked by Cache timing attack.

**Table 5 The key corresponding to the highest 2 bits of look-up index of S box in the fourth round**

| S box | The key corresponding to the highest 2 bits of look-up index | Number of the keys |
|---|---|---|
| $S_7$ | $k_{20}, k_{19}, k_{18}$ | 3 |
| $S_6$ | $k_{36}, k_{35}, k_{17}, k_{16}, k_{15}, k_{14}$ | 6 |
| $S_5$ | $k_{13}, k_{12}$ | 2 |
| $S_4$ | $k_{40}, k_{39}, k_9, k_8$ | 4 |
| $S_3$ | $k_{28}, k_{27}, k_5, k_4$ | 4 |
| $S_2$ | $k_1, k_0$ | 2 |
| $S_1$ | $k_{32}, k_{31}$ | 2 |
| $S_0$ | $k_{24}, k_{23}$ | 2 |

## 5 Conclusion

In this paper, based on the trace drive Cache timing attack, features about S-box of LBlock algorithm are studied by LBlock algorithm. At first, the nonlinear algebraic expressions of S-box are derived, expressions for each round and algebraic expressions for S-box look-up index are deduced by encryption and round function $F$. Then, based on features of S-box look-up, the main

expression of the key are propose, which demonstrates that the LBlock algorithm exists the possibility of the cache timing attack and provides a valuable reference to security analysis on other lightweight cryptographic algorithms.

**Acknowledgments**

The authors would like to thank anonymous reviewers for their valuable comments. This research was supported by the National Natural Science Foundation of China under Grant No. 61402528.

## References

[1] Wu Wenling, Zhang Lei. LBlock: A lightweight block cipher [C]//Proceedings of the 9th International Conference on Applied Cryptography and Network Security. Berlin, Germany: Springer-Verlag, 2011: 327-344.

[2] Wu Wenling, Fan Weijie, Zhang Lei. The research progress of lightweight block cipher [J]. The development reports of China cryptography, 2010, 140: 159.

[3] Matsui M. Linear cryptanalysis method for DES cipher [C]//Advances in Cryptology-EUROCRYPT'93. Springer Berlin Heidelberg, 1994: 386-397.

[4] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems [C]// In CRYPTO 1990, volume 537 of LNCS, pages 2-21. Springer, 1990.

[5] Dinur I, Shamir A. Cube attacks on tweakable black box polynomials [M]//Advances. in Cryptology-EUROCRYPT 2009. Springer Berlin Heidelberg, 2009: 278-299.

[6] ALBRECHT M. Alorithmic algebraic techniques and their application to block cipher cryptanalysis [D]. Royal Holloway: University of London, 2010.

[7] Guo Shize, Wang Tao, Zhao Xinjie. The principle and methods of the side channel cryptanalysis [M]. Beijing: Science Press, 2014.

[8] Li Zhenqi, Zhang Bin, Yao Yuan, et al. Cube cryptanalysis of LBlock with noisy leakage [C]// Proceedings of the 15th International Conference on Information Security and Cryptology. Berlin, Germany: Springer-Verlag, 2012: 141-155.

[9] Bogdanov A, Kundsen L R, Leander G, et al. PRESENT: An ultra-lightweight block cipher [C]//Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Germany: Springer-Verlag, 2007: 450-466.

[10] Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems [C]// Advances in Cryptology-CRYPTO 1996, LNCS 1109, 1996: 104-113.

[11] Kelsey J, Schneier B, Wagner D, et al. Side channel cryptanalysis of product ciphers [C]// Peoceeding of the 5th European Symposium on Research in Computer Security-ESORICS 1998, LNCS 1485, 1998: 97-110.

[12] Wen Qiaoyan, Niu Xinxi, Yang Yixian. The Boolean function in modern cryptography [M]. Beijing: Science Press, 2000.

[13] Page D. Theoretical use of cache memory as a cryptanalytic side-channel [DB/OL]. (2002-11-11) http://eprint. iacr. org /2002 /169. pdf.

[14] Zhu Xiliang, Wei Yongzhuang. The study of the trace driven cache timing attack against LBlock algorithm [J]. Computer Engineering, 2015, 47(5): 153-158.

[15] Peng Changyong, Zhu Yuefei, Gu Chunxiang, et al. The polynomial representation and completeness analysis on 1 ~ 5 round of LBlock algorithm [J]. Computer Engineering, 2012, 38(9): 155-157.