Multidimensional Zero-Correlation Linear Cryptanalysis on 23-Round LBlock-s

Hong Xu[1,2](✉), Ping Jia[1], Geshi Huang[2], and Xuejia Lai[2]

[1] Zhengzhou Information Science and Technology Institute, Zhengzhou, China
xuhong0504@163.com
[2] Shanghai Jiao Tong University, Shanghai, China

Abstract. LBlock-s is the kernel block cipher of the authentication encryption algorithm LAC submitted to CAESAR competition. The LBlock-s algorithm is almost the same as LBlock except that the former adopts an improved key schedule algorithm with better diffusion property. Using the shifting relation of certain subkeys derived by the new key schedule algorithm, we present a multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s. The time complexity of the attack is about $2^{75.4}$ 23-round encryptions, where $2^{62.3}$ known plaintexts are used and 60 subkey bits are guessed, which is three bits less than that of LBlock. Our research showed that the improved key schedule algorithm did not enhance their ability to protect against zero-correlation linear cryptanalysis, and it is better to use the irregular bit-shifting to disturb the shifting relation between subkeys.

Keywords: LBlock · LBlock-s · Multidimensional zero-correlation linear cryptanalysis · Key schedule

1 Introduction

With the development of communication and electronic applications, the limited-resource devices such as RFID tags and sensor nodes have been used in many aspects of our life. Traditional block cipher is not suitable for this extremely constrained environment. Therefore, research on designing and analyzing lightweight block ciphers has become a hot topic. LBlock [1] is such a kind of a lightweight block cipher presented by Wu *et al.* in ACNS 2011. It employs a variant Feistel structure and consists of 32 rounds. The round function is composed with S-boxes, nibble-wise permutation and bit rotation, and the key schedule algorithm is similar to that of PRESENT [2], one of the lightweight block cipher standards.

The LBlock algorithm has attracted a lot of attention because of its simplicity, efficiency and low cost. In 2012, Liu and Karakoc *et al.* [3,4] presented an impossible differential cryptanalysis on 21 and 22-round LBlock, Minier and Liu *et al.* [5,6] presented a related impossible differential attack on 22-round LBlock, and Sasaki *et al.* [7] presented an integral attack on 22-round LBlock. Later, Wang *et al.* [8] studied the security of LBlock against biclique cryptanalysis and

S. Qing et al. (Eds.): ICICS 2015, LNCS 9543, pp. 97–108, 2016.
DOI: 10.1007/978-3-319-29814-6_9

found the diffusion of the original key schedule algorithm was not enough. They also presented an improved key schedule algorithm and used it in lightweight block cipher LBlock-s, the kernel block cipher of the authentication encryption algorithm LAC [9] submitted to CAESAR competition [10]. Up to now, little research has been done on the cryptanalysis of LBlock-s or the property of the improved key schedule algorithm.

Linear cryptanalysis [11,12] is one of the most prominent cryptanalysis methods against block ciphers. In 2011 and 2012, Bogdanov *et al.* [13–15] proposed the method of zero-correlation linear cryptanalysis and used it in the cryptanalysis of many block ciphers such as AES, CLEFIA, TEA and XTEA etc. Deferent with linear cryptanalysis which uses linear approximations with correlation far from zero, the zero-correlation linear cryptanalysis used linear approximations with correlation zero to reduce the key space. For block cipher with Feistel-structure, Soleimany and Nyberg proposed the matrix method [16] to automatic search for longest linear approximations with correlation zero, and found 64 classes of zero-correlation linear approximations for 14-round LBlock. Based on this, they also proposed a general zero-correlation linear cryptanalysis on 22-round LBlock-type block cipher without using the property of the key schedule algorithm. Later in ACISP 2014, Wang *et al.* [17] further presented an improved multidimensional zero-correlation linear cryptanalysis on 23-round LBlock using the special property of the key schedule algorithm, the time complexity was about 2^{76} 23-round encryptions, 2^{62} known plaintexts were used, and totally 63 subkey bits were guessed.

In this paper, we will further evaluate the security of LBlock-s against zero-correlation linear cryptanalysis. From a deeply research on the new improved key schedule algorithm we find that there still exists some simple shifting relations between some subkeys of neighboring rounds. Using these properties, by selecting proper zero-correlation linear approximations, we can also present a multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s. The time complexity of the attack is about $2^{75.4}$ 23-round encryptions, where $2^{62.3}$ known plaintexts are used, and 60 subkey bits are guessed, which is three bits less than that of LBlock. The results showed that the improved key schedule algorithm did not enhance their ability to protect against zero-correlation linear cryptanalysis, and it was better to use the irregular bit-shifting to disturb the shifting relation between subkeys.

The remainder of this paper is organized as follows. Section 2 presents a brief description of LBlock-s. Section 3 introduces the definition of zero-correlation linear approximation and presents the basic methods of multidimensional zero-correlation linear cryptanalysis. Section 4 presents the multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s. Finally, Sect. 5 concludes this paper.

2 A Brief Description of LBlock-s

2.1 Notation

Throughout this paper we use the following notations:
- P, C : the 64-bit plaintext and the 64-bit ciphertext;

- K_r : the r-th round subkey;
- X_r: the left half of the r-th round input;
- X_0 : the right half of the first round input;
- $Y|Z$: the concatenation of Y and Z;
- Y_i^j : the j-th 4-bit word of Y_i (where $0 \leq j \leq 7$, and the leftmost index is 7);
- $Y \lll i$: left rotation of Y by i bits;
- $[i]_2$: binary form of an integer i.

2.2 Overview of LBlock-s

LBlock-s is the kernel block cipher of the authentication encryption algorithm LAC submitted to CAESAR competition. Similar to LBlock, the general structure of LBlock-s is a variant of Feistel Network, which is depicted in Fig. 1. The number of iterative rounds is 32.

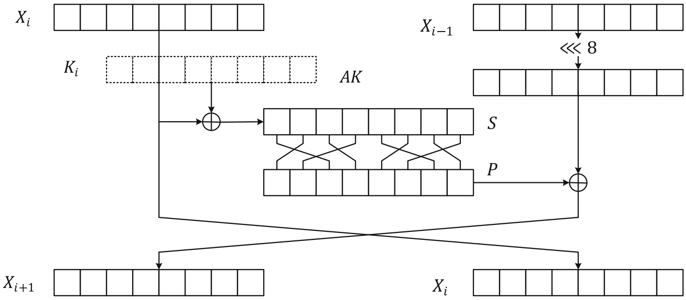

Fig. 1. Round function of LBlock-s block cipher

The round function of LBlock-s includes three basic functions: round subkey addition AK, confusion function S and diffusion function P. The nonlinear layer S consists of 8 identical 4-bit S-boxes in parallel (8 different S-boxes are used in LBlock, see reference [1]). The diffusion function P is defined as a permutation of eight 4-bit nibbles.

Encryption Algorithm. Let $P = (X_1, X_0)$ be a 64-bit plaintext. For $i = 1, 2, \ldots, 32$, do

$$X_{i+1} = P(S(X_i \oplus K_i)) \oplus (X_{i-1} \lll 8)$$

Then the 64-bit ciphertext C is (X_{32}, X_{33}).

The decryption process is the inverse of the encryption process, that is, input 64-bit ciphertext (X_{32}, X_{33}), and output 64-bit plaintext $P = (X_1, X_0)$.

Key Schedule Algorithm. The 80-bit master key K is stored in a key register and denoted as $K = k_{79}k_{78} \ldots k_0$. Output the leftmost 32 bits of register K as subkey K_1.

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

1. $K \lll 24$
2. $[k_{55}k_{54}k_{53}k_{52}] = S[k_{79}k_{78}k_{77}k_{76}] \oplus [k_{55}k_{54}k_{53}k_{52}]$
   $[k_{31}k_{30}k_{29}k_{28}] = S[k_{75}k_{74}k_{73}k_{72}] \oplus [k_{31}k_{30}k_{29}k_{28}]$
   $[k_{67}k_{66}k_{65}k_{64}] = [k_{71}k_{70}k_{69}k_{68}] \oplus [k_{67}k_{66}k_{65}k_{64}]$
   $[k_{51}k_{50}k_{49}k_{48}] = [k_{11}k_{10}k_{9}k_{8}] \oplus [k_{51}k_{50}k_{49}k_{48}]$
3. $[k_{54}k_{53}k_{52}k_{51}k_{50}] = [k_{54}k_{53}k_{52}k_{51}k_{50}] \oplus [i]_2$
4. Output the leftmost 32 bits of current content of register K as round subkey K_{i+1}.

The original key schedule of LBlock used the shift $K \lll 29$, and only two nibbles are updated using two S-boxes (see reference [1] or appendix), so the diffusion is not enough as shown by Wang *et al.* in [8]. Thus in the design of LBlock-s, this improved key schedule was adopted.

3 Zero-Correlation Linear Approximation

Consider a function $f : F_2^n \rightarrow F_2^m$, and let the input of the function be $x \in F_2^n$. A linear approximation with an input mask u and an output mask v is the following function:

$$x \rightarrow u \cdot x \oplus v \cdot f(x).$$

The linear approximation has probability

$$p(u; v) = Pr_{x \in F_2^n}(u \cdot x \oplus v \cdot f(x) = 0),$$

and its correlation is defined as follows:

$$c_f(u; v) = 2p(u; v) - 1.$$

In linear cryptanalysis we are interested in the linear approximation with correlation far from zero. The number of known plaintexts needed in the linear cryptanalysis is inversely proportional to the squared correlation. Zero-correlation linear cryptanalysis uses linear approximations such that the correlation is equal to zero for all keys. Particularly for multidimensional zero-correlation linear cryptanalysis, if $2^m - 1$ zero-correlation approximations of dimension m is used, then by reference [15] the number of required distinct plaintexts is about $2^{n+2-m/2}$. Next we will review the process of multidimensional zero-correlation linear cryptanalysis in more detail.

For most ciphers, a large number of zero-correlation approximations are available. To remove the statistical independence for multiple zero-correlation linear approximations, the zero-correlation linear approximations available are treated as a linear space spanned by m different zero-correlation linear approximations such that all $l = 2^m - 1$ non-zero linear combinations of them have zero correlation [15]. Thus we can describe a cipher E as a cascade of three parts: $E = E_2 \circ E_1 \circ E_0$, and assume there exists m independent linear approximations (u_i, w_i) for E_1 such that all $l = 2^m - 1$ nonzero linear combinations of them have correlation zero. The E_0 and E_2 are the encryption function added before or after E_1.

For each key candidate, the adversary encrypts the plaintexts for the beginning rounds E_0 and obtain some parts of data x, and decrypts the corresponding ciphertexts for the final rounds E_2 and obtain some parts of data y, then obtain a m-tuple

$$z = (z_1, \dots, z_m), \text{where } z_i = \langle u_i, x\rangle + \langle w_i, y\rangle,$$

by evaluating the m linear approximations for a plaintext-ciphertext pair.

For each $z \in F_2^n$, the attacker allocates a counter $V[z]$ and initializes it to value zero. Then for each distinct plaintext, the attacker computes the corresponding data in F_2^m and increments the counter $V[z]$ of this data value by one. Then the attacker computes the statistic T:

$$T = \sum_{z=0}^{2^m-1} \frac{(V(z) - N2^{-m})^2}{N2^{-m}(1-2^{-m})} = \frac{N2^m}{1-2^{-m}} \sum_{z=0}^{2^m-1} \left(\frac{V(z)}{N} - \frac{1}{2^m}\right)^2$$

The value T for right key guess follows a χ^2-distribution with mean $\mu_0 = l \cdot (2^n - N)/(2^n - 1)$ and variance $\sigma_0^2 = 2l(\frac{2^n-N}{2^n-1})^2$ while for the wrong key guess the distribution is a χ^2-distribution with mean $\mu_1 = l$, and variance $\sigma_1^2 = 2l$. Denote the type-I error probability (the probability to wrongfully discard the right key, that is, the success probability) with α and the type-II error probability (the probability to wrongfully accept a random key as the right key) with β. We consider the decision threshold $\tau = \mu_0 + \sigma_0 z_{1-\alpha} = \mu_1 - \sigma_1 z_{1-\beta}$, then the number of known plaintexts N should be about

$$N = \frac{2^n(z_{1-\alpha} + z_{1-\beta})}{\sqrt{l/2} + z_{1-\alpha}}$$

where $z_p = \Phi^{-1}(p)$ for $0 < p < 1$ and Φ is the cumulative function of the standard normal distribution.

4 Multidimensional Zero-Correlation Linear Cryptanalysis on 23-round LBlock-s

Using the miss-in-the-middle technique, Soleimany and Nyberg proposed the matrix method [16] to automatic search for the longest linear approximations with correlation zero, and found 64 classes of zero-correlation linear approximations with the form $(\Gamma_a, 0) \rightarrow_{14r} (0, \Gamma_b)$ for 14-round LBlock, where Γ_a, Γ_b contains exactly one nonzero nibble. Based on this, they also proposed a general zero-correlation linear cryptanalysis on 22-round LBlock-type block cipher without using the property of the key schedule algorithm. Recently, Wang *et al.* [17] further presented an improved multidimensional zero-correlation linear cryptanalysis on 23-round LBlock using the special property of the key schedule algorithm, the time complexity was about 2^{76} 23-round encryptions, where 2^{62} known plaintexts were used, and totally 63 subkey bits were guessed.

Since the general structure of LBlock-s is the same as LBlock, it also has such 14-round zero-correlation linear approximations of the form $(\varGamma_a, 0) \rightarrow_{14r} (0, \varGamma_b)$ for 14-round LBlock, where $\varGamma_a, \varGamma_b$ run through all $l = 2^8 - 1$ nonzero values, they form a linear space spanned by 8 different zero-correlation linear approximations such that all $l = 2^8 - 1$ non-zero linear combinations of them have zero correlation. When used directly to present a multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s, 76 bits of subkey will be guessed and the total time complexity will be greater than exhaustive search. So we must try to find some dependence between subkey bits and use them to reduce the time complexity. Fortunately, by careful discussion we really find some dependence between subkey bits, for example, we have

$$K_i^0 = K_{i+1}^6, K_i^1 = K_{i+1}^7.$$

Using these relations, by selecting proper zero-correlation linear approximations, we can present a multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s.

Let E_1 be the encryption function of 14-round LBlock-s with zero-correlation linear approximations of the form $(\varGamma_a, 0) \rightarrow_{14r} (0, \varGamma_b)$, we add r_{in} rounds before E_1 and r_{out} rounds after E_1, then obtain a $(r_{in} + 14 + r_{out})$-round encryption function $E = E_2 \circ E_1 \circ E_0$. Let $Site_{in}$ and $Site_{out}$ be the position of nonzero nibbles of $\varGamma_a$ and $\varGamma_b$, where $0 \leq Site_{in}, Site_{out} \leq 7$.

In order to fully use the dependence of subkey bits to reduce the complexity, we use the improved multidimensional zero-correlation linear cryptanalysis method proposed by Wang *et al.* in [17] and search for linear approximations and (r_{in}, r_{out}) with least number of guessed keys. The least number of guessed keys is 60, where $r_{in} = 5$, $r_{out} = 4$, and the corresponding choices for $(Site_{in}, Site_{out})$ are as follows:

$$(Site_{in}, Site_{out}) \in \{(6,6), (6,4), (6,2), (6,0)\}.$$

We select $(Site_{in}, Site_{out}) = (6,6)$ to give an attack on 23-round LBlock-s, that is, we use the linear approximations of the form $(0u000000, 00000000) \rightarrow_{14r} (00000000, 0w000000)$. As $r_{in} = 5$, and $r_{out} = 4$, we put the 14-round zero-correlation linear approximations in round 6 to 19 and attack LBlock-s from round 1 to 23 (Fig. 2).

After collecting sufficient plaintext-ciphertext pairs, we guess corresponding subkeys for the first five rounds and the last four rounds to evaluate the statistic T. Using the dependence of subkeys bits and using the partial compression technique we can reduce the time complexity significantly and present an efficient zero-correlation linear attack on 23-round LBlock-s.

As shown in Fig. 2, the nibble X_6^6 is affected by 48 bits of plaintext (X_1, X_0) and 48 bits of round keys and the expression can be shown as:

$$\begin{aligned} X_6^6 = & X_0^0 \oplus S(X_1^0 \oplus K_1^0) \oplus S(X_1^3 \oplus S(X_0^5 \oplus S(X_1^6 \oplus K_1^6) \oplus K_2^7) \oplus K_3^5) \oplus \\ & S(X_1^0 \oplus S(X_0^6 \oplus S(X_1^1 \oplus K_1^1) \oplus K_2^0) \oplus S(X_0^1 \oplus S(X_1^2 \oplus K_1^2) \oplus \\ & S(X_1^5 \oplus S(X_0^4 \oplus S(X_1^4 \oplus K_1^4) \oplus K_2^6) \oplus K_3^7) \oplus K_4^5) \oplus K_5^4) \end{aligned}$$

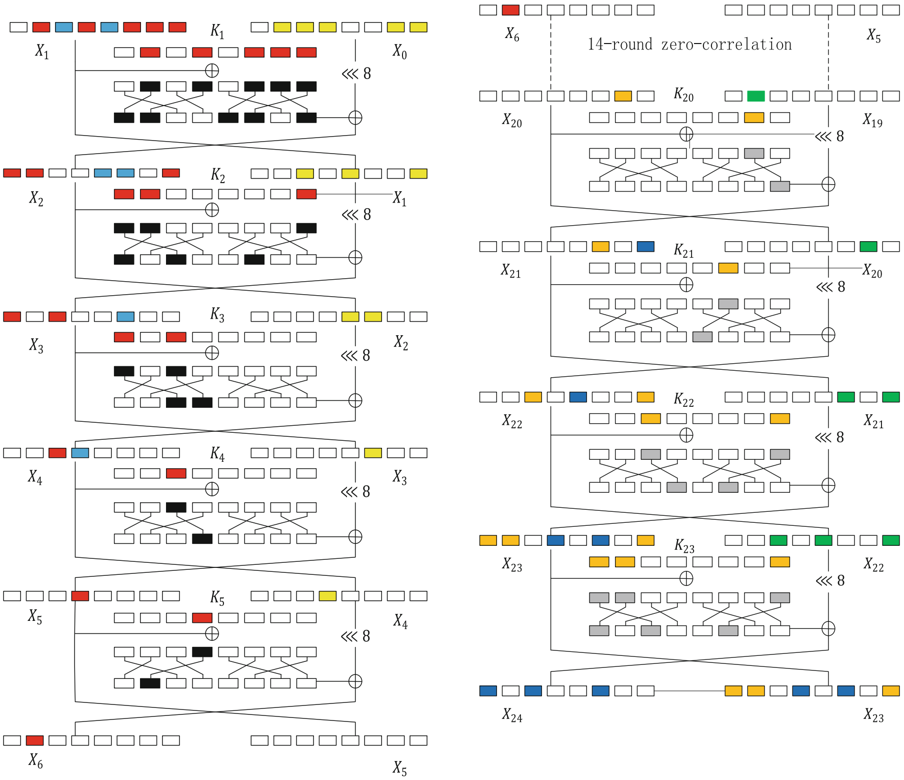

Fig. 2. Attack on 23-round LBlock-s

Similarly, the nibble X_{19}^6 is affected by 32 bits of ciphertext (X_{23}, X_{24}) and 28 bits of round keys and the expression can be shown as:

$$\begin{aligned} X_{19}^6 = & X_{23}^2 \oplus S(X_{24}^2 \oplus S(X_{23}^0 \oplus K_{23}^0) \oplus K_{22}^0) \oplus S(X_{24}^5 \oplus S(X_{23}^7 \oplus K_{23}^7) \oplus \\ & S(X_{23}^4 \oplus S(X_{24}^7 \oplus S(X_{23}^6 \oplus K_{23}^6) \oplus K_{22}^5) \oplus K_{21}^2) \oplus K_{20}^1) \end{aligned}$$

After analyzing the key schedule of LBlock-s, we find the following relations in the round keys:

$$K_2^7 = K_1^1, K_2^6 = K_1^0, K_5^4 = K_1^0 \oplus K_1^1, K_{23}^6 = K_{22}^0.$$

Thus the number of bits need to be guessed can be reduced from 76 to 60.

Assuming that N known plaintexts are used, the partial encryption and decryption using the partial-compression technique are proceeded as in Table 1.

The second column in Table 1 stands for the subkey nibbles that have to be guessed in each step, and the third column denotes the time complexity of corresponding step measured in S-box access. In each step, we save the values of the Obtained States during the encryption and decryption process. For each

Table 1. Partial encryption and decryption on 23-round LBlock-s

Steps	Guessed subkeys	Time (S-box accesses)	Obtained States	Size
1	$K_1^{1,4,6}, K_2^6, K_2^7(K_1^1)$	$N \cdot 2^{16} \cdot 5$	$x_1 = X_0^0 \vert X_1^0 \vert X_3^5 \vert X_2^0 \vert X_0^1 \vert X_1^2 \vert X_3^7 \vert X_{23}^2 \vert X_{24}^2 \vert X_{23}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{60}
2	$K_2^0, K_1^0(K_2^6)$	$2^{60} \cdot 2^{16+4} \cdot 2$	$x_2 = X_2^2 \vert X_3^5 \vert X_3^2 \vert X_0^1 \vert X_1^2 \vert X_3^7 \vert X_{23}^2 \vert X_{24}^2 \vert X_{23}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{56}
3	K_1^2	$2^{56} \cdot 2^{20+4}$	$x_3 = X_2^2 \vert X_3^5 \vert X_3^2 \vert X_2^3 \vert X_3^7 \vert X_{23}^2 \vert X_{24}^2 \vert X_{23}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{52}
4	K_3^5	$2^{52} \cdot 2^{24+4}$	$x_4 = X_4^4 \vert X_3^2 \vert X_2^3 \vert X_3^7 \vert X_{23}^2 \vert X_{24}^2 \vert X_{23}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{48}
5	K_3^7	$2^{48} \cdot 2^{28+4}$	$x_5 = X_4^4 \vert X_3^2 \vert X_4^5 \vert X_{23}^2 \vert X_{24}^2 \vert X_{23}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{44}
6	K_4^5	$2^{44} \cdot 2^{32+4}$	$x_6 = X_4^4 \vert X_5^4 \vert X_{23}^2 \vert X_{24}^2 \vert X_{23}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{40}
7	$K_5^4(K_1^0 \oplus K_1^1)$	$2^{40} \cdot 2^{36+0}$	$x_7 = X_6^6 \vert X_{23}^2 \vert X_{24}^2 \vert X_{23}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{36}
8	K_{23}^0	$2^{36} \cdot 2^{36+4}$	$x_8 = X_6^6 \vert X_{23}^2 \vert X_{22}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{24}^7 \vert X_{23}^6$	2^{32}
9	$K_{22}^0(K_{23}^6)$	$2^{32} \cdot 2^{40+4} \cdot 2$	$x_9 = X_6^6 \vert X_{21}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{23}^4 \vert X_{22}^5$	2^{24}
10	K_{22}^5	$2^{24} \cdot 2^{44+4}$	$x_{10} = X_6^6 \vert X_{21}^0 \vert X_{24}^5 \vert X_{23}^7 \vert X_{21}^2$	2^{20}
11	K_{23}^7	$2^{20} \cdot 2^{48+4}$	$x_{11} = X_6^6 \vert X_{21}^0 \vert X_{22}^3 \vert X_{21}^2$	2^{16}
12	K_{21}^2	$2^{16} \cdot 2^{52+4}$	$x_{12} = X_6^6 \vert X_{21}^0 \vert X_{20}^1$	2^{12}
13	K_{20}^1	$2^{12} \cdot 2^{56+4}$	$x_{13} = X_6^6 \vert X_{19}^6$	2^8

possible value of $x_i (1 \leq i \leq 13)$, the counter $N_i[x_i]$ will record how many plaintext-ciphertext pairs can produce the corresponding intermediate state x_i. The counter size for each x_i is shown in the last column.

To be clear, we explain some steps in Table 1 in detail.

Step 1. We allocate the 60-bit counter $N_1[x_1]$ and initialize it to zero. We then guess 16-bit keys and partially encrypt N plaintexts to compute x_1, and increment the corresponding counter.

Since $K_2^7 = K_1^1$, we only need to guess 16 bits of subkeys $K_1^{1,4,6}, K_2^6$. As shown in Fig. 2, the nibble X_6^6 is affected by 42 bits of plaintext (X_1, X_0). They are represented by

$$\begin{aligned} x_0 = & X_0^0|X_1^0|X_1^3|X_0^5|X_1^6|X_0^6|X_1^1|X_0^1|X_1^2|X_1^5|X_0^4|X_1^4| \\ & X_{23}^2|X_{24}^2|X_{23}^0|X_{24}^5|X_{23}^7|X_{23}^4|X_{24}^7|X_{23}^6 \end{aligned}$$

Since the following three equations

$$X_2^0 = X_0^6 \oplus S(X_1^1 \oplus K_1^1),$$

$$X_3^5 = X_1^3 \oplus S(X_0^5 \oplus S(X_1^6 \oplus K_1^6) \oplus K_2^7),$$
$$X_3^7 = X_1^5 \oplus S(X_0^4 \oplus S(X_1^4 \oplus K_1^4) \oplus K_2^6)$$

are true for LBlock-s, then the 80-bit x_0 can be reduced to 60-bit x_1 :

$$x_1 = X_0^0|X_1^0|X_3^5|X_2^0|X_0^1|X_1^2|X_3^7|X_{23}^2|X_{24}^2|X_{23}^0|X_{24}^5|X_{23}^7|X_{23}^4|X_{24}^7|X_{23}^6$$

after guessing 16 bits subkeys $K_1^{1,4,6}, K_2^6$. Update the expressions of X_6^6 as follows:

$$\begin{aligned}X_6^6 =& X_0^0 \oplus S(X_1^0 \oplus K_1^0) \oplus S(X_3^5 \oplus K_3^5) \oplus S(X_1^0 \oplus S(X_2^0 \oplus K_2^0)\oplus \\ & S(X_0^1 \oplus S(X_1^2 \oplus K_1^2) \oplus S(X_3^7 \oplus K_3^7) \oplus K_4^5) \oplus K_5^4)\end{aligned}$$

Step 2. We allocate the 56-bit counter $N_2[x_2]$ and initialize it to zero. We then guess 4-bit subkeys K_2^0 and partially encrypt x_0 to compute x_1 and add the corresponding $N_1[x_1]$ to $N_2[x_2]$.

Since the subkey $K_1^0 = K_2^6$ is known, and the following two equations

$$X_2^2 = X_0^0 \oplus S(X_1^0 \oplus K_1^0),$$
$$X_3^2 = X_1^0 \oplus S(X_2^0 \oplus K_2^0)$$

are true for LBlock-s, then the 60-bit x_1 can be reduced to 56-bit x_2 :

$$x_2 = X_2^2|X_3^5|X_3^2|X_0^1|X_1^2|X_3^7|X_{23}^2|X_{24}^2|X_{23}^0|X_{24}^5|X_{23}^7|X_{23}^4|X_{24}^7|X_{23}^6$$

after guessing 4 bits subkeys. Update the expressions of X_6^6 as follows:

$$X_6^6 = X_2^2 \oplus S(X_3^5 \oplus K_3^5) \oplus S(X_3^2 \oplus S(X_0^1 \oplus S(X_1^2 \oplus K_1^2) \oplus S(X_3^7 \oplus K_3^7) \oplus K_4^5) \oplus K_5^4)$$

The following steps are similar to the above two steps, and we do not explain in details. The cost of step 1 to step 13 in the process of partial computation is about 2^{83} S-box access, which is about $2^{83} \cdot 1/8 \cdot 1/23 \approx 2^{75.4}$ 23-round LBlock-s encryptions.

Next we will discuss in detail the data complexity and total time complexity of the attack.

As $(0u000000, 00000000) \rightarrow_{14r} (00000000, 0w000000)$ is the selected zero-correlation linear approximations, where $u, w \in F_2^4$. When u, w run through all $l = 2^8 - 1$ nonzero values, they form a linear space of dimension 8, so we can choose 8 independent linear masks with $(u_i, w_i) \in \{(1,0), (2,0), (4,0), (8,0), (0,1), (0,2), (0,4), (0,8)\}$, and calculate the 8-bit tuple

$$z = (z_1, \ldots, z_8), \text{where } z_i = \langle u_i, X_6^6\rangle + \langle w_i, X_{19}^6\rangle.$$

Then evaluate the statics $T_k = \frac{N2^8}{1-2^{-8}} \sum_{z=0}^{2^8-1} (\frac{V(z)}{N} - \frac{1}{2^8})^2$ and make decision for each guessing key k.

Similar as in [17], let the type-I error probability $\alpha = 2^{-2.7} \approx 0.154$ and the type-II error probability $\beta = 2^{-9} \approx 0.002$, then $z_{1-\alpha} \approx 1, z_{1-\beta} \approx 2.88$. Since $n = 64$ and $l = 2^8 - 1 = 255$, then from $N = \frac{2^n(z_{1-\alpha}+z_{1-\beta})}{\sqrt{l/2}+z_{1-\alpha}}$ we know the data complexity N is about $2^{62.3}$, and the decision threshold is $\tau = \mu_0 + \sigma_0 z_{1-\alpha}$.

To recover the secret key, the following steps are performed:

1. Allocate a counter $V[z]$ for 8-bit z.
2. For 2^8 values of x_{13} :
   (a) Evaluate all eight basis zero-correlation masks on x_{13} and get z.
   (b) Update the counter $V[z]$ by $V[z] = V[z] + N_{13}[x_{13}]$.
3. For each guessing key k, compute $T_k = \frac{N2^8}{1-2^{-8}} \sum_{z=0}^{2^8-1} (\frac{V(z)}{N} - \frac{1}{2^8})^2$.
4. If $T_k < \tau$, then the guessed subkey values are possible right subkey candidates.
5. Do exhaustive search for all right candidates.

Complexity. The cost of step 1 to step 13 in the process of partial computation is about $2^{75.4}$ 23-round LBlock-s encryptions. Since the type-II error probability $\beta = 2^{-9}$), the number of remaining key candidates is about $2^{80} \cdot \beta = 2^{71}$. Thus the total time complexity is $2^{75.4} + 2^{71} \approx 2^{75.4}$ 23-round LBlock-s encryptions. The data complexity is $2^{62.3}$ known plaintexts, and the memory requirements are about 2^{60} bytes.

5 Conclusions

The security of LBlock-s against multidimensional zero-correlation linear cryptanalysis is evaluated. By choosing proper zero-correlation linear approximations, we present a multidimensional zero-correlation linear cryptanalysis on 23-round LBlock-s using the shifting relation of certain subkeys derived by the new key schedule algorithm. The complexity is almost as that of LBlock. Our research showed that the improved key schedule algorithm did not enhance their ability to protect against zero-correlation linear cryptanalysis, and it is better to use the irregular bit-shifting to disturb the shifting relation between subkeys.

Acknowledgements. We thank the anonymous reviewers for their careful reading of our paper and helpful comments. This research was supported by the National Natural Science Foundation of China (Nos. 61100200, 61170235, 61309017, 61472251) and China Postdoctoral Science Foundation (No. 2014T70417).

Appendix. Key Schedule of LBlock

The 80-bit master key K is stored in a key register and denoted as $K = k_{79}k_{78}\dots k_0$. Output the leftmost 32 bits of register K as subkey K_1.

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

1. $K \lll 29$
2. $[k_{79}k_{78}k_{77}k_{76}] = S_8[k_{79}k_{78}k_{77}k_{76}]$
   $[k_{75}k_{74}k_{73}k_{72}] = S_9[k_{75}k_{74}k_{73}k_{72}]$
3. $[k_{50}k_{49}k_{48}k_{47}k_{46}] = [k_{50}k_{49}k_{48}k_{47}k_{46}] \oplus [i]_2$
4. Output the leftmost 32 bits of current content of register K as round subkey K_{i+1}.

References

1. Wu, W., Zhang, L.: LBlock: a lightweight block cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344. Springer, Heidelberg (2011)
2. Bogdanov, A.A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
3. Liu, Y., Gu, D., Liu, Z., Li, W.: Impossible differential attacks on reduced-round LBlock. In: Ryan, M.D., Smyth, B., Wang, G. (eds.) ISPEC 2012. LNCS, vol. 7232, pp. 97–108. Springer, Heidelberg (2012)
4. Karakoç, F., Demirci, H., Harmancı, A.E.: Impossible differential cryptanalysis of reduced-round LBlock. In: Askoxylakis, I., Pöhls, H.C., Posegga, J. (eds.) WISTP 2012. LNCS, vol. 7322, pp. 179–188. Springer, Heidelberg (2012)
5. Minier, M., Naya-Plasencia, M.: A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock. Inf. Process. Lett. **112**, 624–629 (2012)
6. Liu, S., Gong, Z., Wang, L.: Improved related-key differential attacks on reduced-round LBlock. In: Chim, T.W., Yuen, T.H. (eds.) ICICS 2012. LNCS, vol. 7618, pp. 58–69. Springer, Heidelberg (2012)
7. Sasaki, Y., Wang, L.: Comprehensive study of integral analysis on 22-round LBlock. In: Kwon, T., Lee, M.-K., Kwon, D. (eds.) ICISC 2012. LNCS, vol. 7839, pp. 156–169. Springer, Heidelberg (2013)
8. Wang, Y., Wu, W., Yu, X., Zhang, L.: Security on LBlock against Biclique cryptanalysis. In: Lee, D.H., Yung, M. (eds.) WISA 2012. LNCS, vol. 7690, pp. 1–14. Springer, Heidelberg (2012)
9. Zhang, L., Wu, W., Wang, Y.: LAC: a lightweight authenticated encryption cipher. In: Submission to CAESAR, version 1, 15 March 2014. http://competitions.cr.yp.to/round1/lacv1.pdf
10. CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, January 2013–December 2017. http://competitions.cr.yp.to/caesar.html
11. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
12. Nyberg, K.: Linear approximation of block ciphers. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 439–444. Springer, Heidelberg (1995)
13. Bogdanov, A., Rijmen, V.: Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Des. Codes Cryptogr. **70**(3), 369–383 (2014). https://eprint.iacr.org/2011/123
14. Bogdanov, A., Wang, M.: Zero correlation linear cryptanalysis with reduced data complexity. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 29–48. Springer, Heidelberg (2012)
15. Bogdanov, A., Leander, G., Nyberg, K., Wang, M.: Integral and multidimensional linear distinguishers with correlation zero. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 244–261. Springer, Heidelberg (2012)
16. Soleimany, H., Nyberg, K.: Zero-correlation linear cryptanalysis of reduced-round LBlock. Des. Codes Cryptogr. **73**(2), 683–698 (2014). https://eprint.iacr.org/2012/570
17. Wang, Y., Wu, W.: Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE. In: Susilo, W., Mu, Y. (eds.) ACISP 2014. LNCS, vol. 8544, pp. 1–16. Springer, Heidelberg (2014)

18. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 158–178. Springer, Heidelberg (2014)
19. Boura, C., Naya-Plasencia, M., Suder, V.: Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and SIMON. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 179–199. Springer, Heidelberg (2014)