Improved Multidimensional Zero-Correlation Linear Cryptanalysis and Applications to LBlock and TWINE

Yanfeng Wang[1,3] and Wenling Wu[1,2]

[1] Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R. China
[2] State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, P.R. China
[3] Graduate University of Chinese Academy of Sciences, Beijing 100049, P.R. China
{wwl,wangyanfeng}@tca.iscas.ac.cn

Abstract. Zero-correlation linear cryptanalysis is a new method based on the linear approximations with correlation zero. In this paper, we propose a new model of multidimensional zero-correlation linear cryptanalysis by taking the equivalent relations of round keys into consideration. The improved attack model first finds out all the longest multidimensional zero-correlation linear distinguishers, then regards the distinguishers with the least independent guessed keys as the optimal distinguishers and finally chooses one optimal distinguisher to recover the secret key of cipher by using the partial-compression technique. Based on the improved attack model, we extend the original 22-round zero-correlation linear attack on LBlock and first evaluate the security of TWINE against the zero-correlation linear cryptanalysis. There are at least 8×8 classes of multidimensional zero-correlation linear distinguishers for 14-round LBlock and TWINE. After determining the corresponding optimal distinguisher, we carefully choose the order of guessing keys and guess each subkey nibble one after another to achieve an attack on 23-round LBlock, an attack on 23-round TWINE-80 and another attack on 25-round TWINE-128. As far as we know, these results are the currently best results on LBlock and TWINE in the single key scenario except the optimized brute force attack.

Keywords: lightweight block cipher, LBlock, TWINE, multidimensional zero-correlation linear cryptanalysis, partial-compression.

1 Introduction

Zero-correlation cryptanalysis[1] is a novel promising attack technique for block ciphers. The distinguishing property used in zero-correlation cryptanalysis is the existence of zero-correlation linear hulls over a part of the cipher. Those linear approximations hold true with probability p equal to $1/2$ and correlation $c = 2p - 1$ equal to 0. The original scheme had the disadvantage of requiring almost the full codebook of data. Bogdanov et.al proposed a framework which

W. Susilo and Y. Mu (Eds.): ACISP 2014, LNCS 8544, pp. 1–16, 2014.

uses several independent zero-correlation linear approximations to reduce data complexity[2]. In a follow-up work at ASIACRYPT'12[3], a multidimensional distinguisher has been constructed for the zero-correlation property, which removed the unnecessary independency assumptions on the distinguishers.

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. Recently, several lightweight block ciphers have been proposed, such as PRESENT[4], LED[5], Piccolo[6], LBlock[7], TWINE[8], etc. To reduce the cost of hardware and to decrease key set-up time, the key schedules of the lightweight ciphers are rather simple. As is known to us, the diffusion of the key schedule plays an important role on the security of the block cipher. In contrast to the serious effort spent on the algorithm design, the aspect of key schedules for block ciphers has attracted comparatively little attention.

In order to take advantage of the simple key schedule algorithm, we introduce an improved model of multidimensional zero-correlation linear cryptanalysis in this paper. In the previous basic attack, the adversary partly encrypts the plaintexts and decrypts the ciphertexts to obtain the values of the corresponding positions determined by the zero-correlation distinguisher. During the above process, attackers need to guess internal subkeys and the sizes of guessed keys are various for different zero-correlation distinguishers. In the improved attack model, we first compute the number of guessed round keys for all possible longest zero-correlation distinguishers and choose the one with least guessed key as the optimal distinguisher. After determining the optimal distinguisher, we finally reduce the complexity of the partial computation by guessing each subkey nibble one after another, which is called partial-compression technique.

To demonstrate the practical impact of our attack model, we apply the improved multidimensional zero-correlation linear attack model to LBlock and TWINE. The attacked round of LBlock against zero-correlation linear cryptanalysis is improved from 22-round to 23-round. As shown in [9], there are 8×8 different classes of zero-correlation linear hulls for 14-round LBlock. We evaluate the sizes of guessed keys for all classes of distinguishers and choose one distinguisher with least independent to attack 23-round LBlock. It cost a time complexity of 2^{76} 23-round LBlock encryptions. Similarly, we also apply the above multidimensional zero-correlation linear cryptanalysis to TWINE block cipher. We first find 8×8 different classes of zero-correlation linear hulls for 14-round TWINE. Then, two different zero-correlation linear distinguishers are chosen for TWINE-80 and TWINE-128 because of their different key schedule algorithms. Based on zero-correlation approximations with dimension 8, we carefully apply the partial-compression technique to present an attack on 23-round TWINE-80 and 25-round TWINE-128. Table 1 outlines the results and compares the results with previous attacks under the single-key model. The security of full-round LBlock and TWINE have been evaluated by biclique cryptanalysis[10,11] but

the biclique cryptanalysis can be regarded as an optimization of brute-force attack. In this paper, we do not discuss such an optimized brute-force attack with a small advantage of a constant factor.

Table 1. Comparisons of Cryptanalysis Results on LBlock and TWINE

Ciphers	Round	Data	Time	Memory	Attacks	Source
LBlock	22	2^{61} CP	2^{70}	2^{63}	Integral	[12]
LBlock	22	2^{58} CP	$2^{79.28}$	2^{68}	Impossible Differential	[13]
LBlock	22	$2^{62.1}$ KP	$2^{71.27}$	2^{64}	Zero-Correlation Linear	[9]
LBlock	23	$2^{62.1}$ KP	2^{76}	2^{60}	Zero-Correlation Linear	Sec.4
TWINE-80	22	2^{62} CP	$2^{68.43}$	$2^{68.43}$	Saturation	[8]
TWINE-80	23	$2^{61.39}$ CP	$2^{76.88}$	$2^{76.88}$	Impossible Differential	[8]
TWINE-80	23	$2^{62.1}$ KP	$2^{72.15}$	2^{60}	Zero-Correlation Linear	Sec.5.1
TWINE-128	23	$2^{62.81}$ CP	$2^{106.14}$	$2^{106.14}$	Saturation	[8]
TWINE-128	24	$2^{52.21}$CP	$2^{115.10}$	$2^{115.10}$	Impossible Differential	[8]
TWINE-128	25	2^{48}CP	2^{122}	2^{125}	Multid Meet-in-the-Middle	[14]
TWINE-128	25	$2^{62.1}$KP	$2^{122.12}$	2^{60}	Zero-Correlation Linear	Sec.5.2

† CP: Chosen Plaintexts, † KP: Known Plaintexts † Multid: Multidimensional

The remainder of this paper is organized as follows. Section 2 presents the general structure of previous multidimensional zero-correlation cryptanalysis. Section 3 proposes the improved model of multidimensional zero-correlation linear cryptanalysis. Section 4 applies the improved zero-correlation linear cryptanalysis to 23-round LBlock. Section 5 shows the key recovery attacks on 23-round TWINE-80 and 25-round TWINE-128. Finally, Section 6 concludes this paper.

2 Notations and Preliminaries

In this section, we introduce the definition of zero-correlation linear approximation[1] and the previous basic methods of multidimensional zero-correlation cryptanalysis.

2.1 Zero-Correlation Linear Approximations

Consider an n-bit block cipher f and let the input of the function be $x \in F_2^n$. A linear approximation (u, v) with an input mask u and an output mask v has probability

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

The value $c_f(u, v) = 2p(u, v) - 1$ is called the correlation of linear approximation (u, v). Note that $p(u, v) = 1/2$ is equivalent to zero correlation $c_f(u, v) = 0$.

Zero-correlation linear cryptanalysis uses linear approximations that the correlations are equal to zero for all keys. The round function of ciphers often makes use of three basic operations: XOR operation, branching operation and a permutation S-box. Linear approximations over these operations obey three major rules(see also [15]):

Lemma 1 *(XOR operation): Either the three linear masks at an XOR $\oplus$ are equal or the correlation over $\oplus$ is exactly zero.*

Lemma 2 *(Branching operation): Either the three linear masks at a branching point $\bullet$ sum up to 0 or the correlation over $\bullet$ is exactly zero.*

Lemma 3 *(S-box permutation): Over an S-box S, if the input and output masks are neither both zero nor both nonzero, the correlation over S is exactly zero.*

In order to find the longest zero-correlation linear approximations, several methods are proposed to find the linear hull with zero-correlation. The matrix method are proposed in [9] by using the miss-in-the-middle technique to establish zero-correlation linear approximations. Given a distinguisher of zero-correlation linear approximation over a part of the cipher, the basic key recovery can be done with a technique similar to that of Matsui's Algorithm 2[15], partially encrypting/decrypting from the plaintext/ciphertext up to the boundaries of the property. This is the key recovery approach used in all zero-correlation attacks so far. In this paper, we aim to improve upon this by exploiting the weakness of the key schedule algorithm and using the partial-compression technique to reduce the computational complexity of attacks.

2.2 Multidimensional Zero-Correlation Linear Cryptanalysis

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[3]. Given m linear approximations

$$\langle u_i, x\rangle + \langle w_i, y\rangle, \quad i = 1, ..., m$$

where x and y are some parts of data in encryption process, one obtains an m-tuples z by evaluating the m linear approximations for a plaintext-ciphertext pair

$$z = (z_1, ..., z_m), \quad z_i = \langle u_i, x\rangle + \langle w_i, y\rangle.$$

For each $z \in \mathbb{F}_2^m$, 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 $\mathbb{F}_2^m$ and increments the counter $V[z]$ of this data value by one. Then the attacker computes the statistic T:

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

The statistic T for the right key guess follows a χ^2-distribution with mean $\mu_0 = l\frac{2^n-N}{2^n-1}$ and variance $\sigma_0^2 = 2l(\frac{2^n-N}{2^n-1})$, while for the wrong key guess it follows a χ^2-distribution with mean $\mu_1 = l$ and variance $\sigma_1^2 = 2l$.

In order to show the relationships between data complexity and success probability, we first denote the type-I error probability (the probability to wrongfully discard the right key) 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

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

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

3 Improved Multidimensional Zero-Correlation Linear Cryptanalysis

In contrast to the serious effort spent on the algorithm design, the aspect of key schedules for block ciphers has attracted comparatively little attention. In this section, we give an improved model of multidimensional zero-correlation linear cryptanalysis by taking advantage of the weakness of key schedule algorithms.

Having the zero-correlation linear distinguisher, the adversary partly encrypts the plaintexts and decrypts the ciphertexts to obtain the values of the corresponding positions determined by the distinguisher. Attackers need to guess internal subkeys during the above process. As mentioned above, a large number of zero-correlation hulls are available for a single block cipher. Moreover, the sizes of guessed keys can vary for different key schedule algorithms and different classes of zero-correlation distinguishers. Thus, the choice and position of the zero-correlation linear hull will influence the result of security evaluation. In order to obtain a better attack on the target cipher, we present an improved model of multidimensional zero-correlation linear cryptanalysis.

Specifically, the following steps are processed to reduce the time complexity of attacks on some R-round block cipher.

1. Find all the longest multidimensional zero-correlation linear distinguishers by using the matrix method or other properties of encryption algorithm. We denote the number of different distinguishers by n and the round number of that by R_d. Obviously, we assume that R_d is always smaller than R.
2. Put the R_d-round distinguisher in the middle of the cipher and calculate the number of related round keys during the process of the partial computation.
   (a) The set of possible cases are noted with $\{(i, R_e), 0 \leq i < n, 0 \leq R_e \leq R - R_d\}$ and the pairs are sorted according to the number of related round keys. In each pair, the parameter i means the indexed number of different distinguishers and R_e means the round number of partial encryption.

Meanwhile, the corresponding round number of partial decryption is $R-R_d-R_e$. Thus, different elements in the set represent different attack schemes.

(b) Save the pairs (i, R_e) with least number of keys in a set S.

The above process is determined by the diffusion of the encryption algorithm and has no relation with the key schedule algorithm.

3. Minimize the set S to an optimal set O by taking the key schedule algorithm into consideration. Having known the position of the corresponding distinguisher, we can determine the realistic round keys for every pair in S. Furthermore, the equivalent relations in round keys can be obtained by carefully analyzing the key schedule algorithm.
   (a) For each element in S, update the number of related keys with the number of independent guessed keys.
   (b) Sort S again and only save the pairs with least guessed keys to O.
4. Choose an arbitrary pair from O to recover the secret key of the R-round cipher. Assume that the dimensional number of the distinguisher is m.
   (a) Allocate a counter $V[z]$ for m-bit z. The vector z is the concatenation of evaluations of m zero-correlation linear approximations.
   (b) Update the counter $V[z]$ by guessing subkeys nibble one after another by using the partial-compression technique.
   (c) For each guessing key k, compute $T_k = \frac{N \cdot 2^m}{(1-2^{-m})} \sum_{z=0}^{2^m-1} \left(\frac{V[z]}{N} - \frac{1}{2^m}\right)^2$.
   (d) If $T_k < \tau$, then the guessed subkey values are possible right subkey candidates.
   (e) Do exhaustive search for all right candidates.

In the following sections, these new improvements will be illustrated with applications to block ciphers LBlock and TWINE.

4 Application to LBlock

In this section, we will evaluate the security of LBlock against multidimensional zero-correlation linear cryptanalysis by using the above improved model and give an attack on 23-round LBlock. We first give a brief description of LBlock and then show the properties of zero-correlation linear distinguishers for 14-round LBlock. Finally, a key recovery attack on 23-round LBlock is given.

4.1 A Brief Description of LBlock

Encryption Algorithm. The general structure of LBlock is a variant of Feistel Network, which is depicted in Figure 1. The number of iterative rounds is 32. The round function of LBlock includes three basic functions: AddRoundKey AK, confusion function S and diffusion function P. The confusion function S consists of eight 4×4 S-boxes in parallel. The diffusion function P is defined as a permutation of eight 4-bit words.

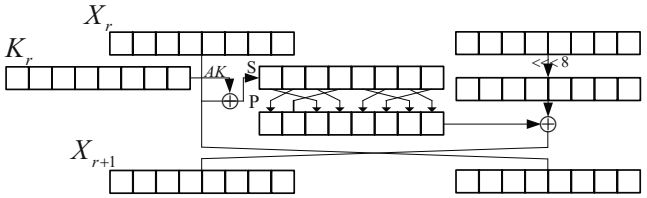

Fig. 1. Round function of LBlock block cipher

Key Schedule Algorithm. To reduce the cost of hardware and to decrease key set-up time, the key schedule of LBlock is rather simple. The 80-bit master key MK is stored in a key register and represented as $MK = k_0k_1...k_{79}$. At round i, the leftmost 32 bits of current contents of register MK are output as the round key K_i, i.e., $K_i = k_0k_1...k_{31}$. The key schedule of LBlock can be shown as follows:

1. $K_0 = MK[0-31]$
2. For $i \leftarrow 1$ to 31
   (a) $MK = MK <<< 29$
   (b) $MK[0-3] = s_9(MK[0-3])$
   $MK[4-7] = s_8(MK[4-7])$
   (c) $MK[29-33] = MK[29-33] \oplus [i]_2$
   (d) $K_i = MK[0-31]$

4.2 Zero-Correlation Linear Approximations of 14-Round LBlock

If an incompatible pair of linear masks can be shown for each linear trail in a linear hull, the correlation of the linear hull is zero. As studied in [9], there are 8×8 different classes of zero-correlation linear hulls for 14-round LBlock and the characteristics can be summarized as the following property:

Property 1. For 14-round LBlock, if the input mask a of the first round locates at the left branch and the output mask b of the last round locates in the right branch, then the correlation of the linear approximation is zero, where $a, b \in F_2^4$, $a \neq 0$ and $b \neq 0$.

To distinguish the 64 different zero-correlation hulls, we express them with two integers as (la, lb), where $0 \leq la \leq 7$ and $8 \leq lb \leq 15$.

4.3 Key Recovery for 23-Round LBlock

In order to attack 23-round LBlock, we follows the improved attack model of multidimensional zero-correlation cryptanalysis.

Step 1. As noted before, $R = 23$ and $R_d = 14$ for block cipher LBlock. We need to choose a distinguisher from the set $\{((la, lb), R_e), 0 \leq R_e \leq 9\}$.

Step 2. After calculating the number of related keys, the original set is reduced to $S = \{((la, lb), R_e), 4 \leq R_e \leq 5\}$.

Step 3. For every element in S, compute the least number of guessed keys. The least number of guessed keys is 63. Meanwhile, only four choices are left in the optimal set and $O = \{((1, 14), 4), ((2, 14), 4), ((3, 14), 4), ((6, 14), 4)\}$.

Step 4. Finally, we select $((1, 14), 4)$ to give an attack on 23-round LBlock. Because $R_e = 4$, we put the 14-round zero-correlation linear hull in rounds 4 to 17 and attack LBlock from round 0 to round 22 (Figure 2).

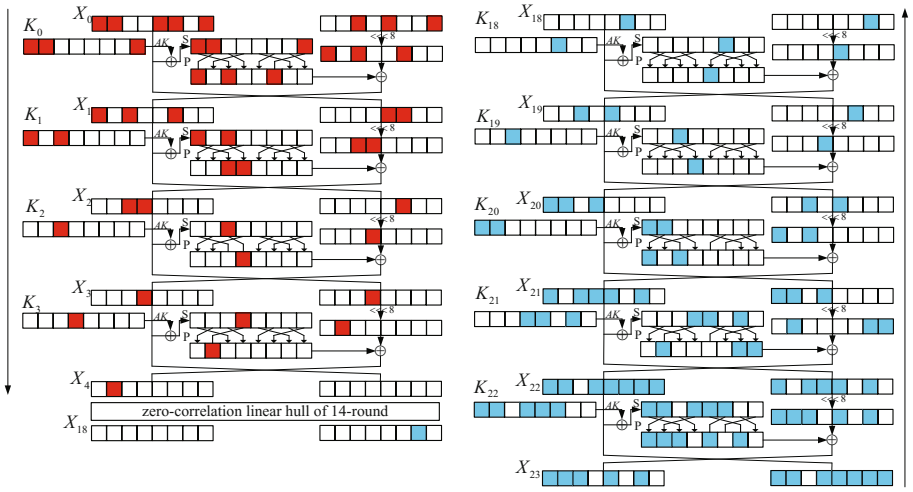

Fig. 2. Attack on 23-Round LBlock

After collecting sufficient plaintext-ciphertext pairs, we guess corresponding subkeys for the first four rounds and the last five rounds to estimate the statistic T. If we directly guess the subkeys bits involved in the key recovery process, then the time complexity will be greater than exhaustive search. Therefore, in order to reduce the time complexity, we first express the two target values by using the related round keys and plaintexts or ciphertexts, then use the partial-compression technique to reduce the time complexity significantly.

As shown in Figure 2, the nibble X_4^1 is affected by 32 bits of plaintext X_0 and 28 bits of round keys and the expression can be shown as:

$$X_4^1 = X_0^5 \oplus S(X_0^{12} \oplus S(X_0^0 \oplus K_0^0) \oplus K_1^2) \oplus S(X_0^{15} \oplus S(X_0^7 \oplus K_0^7) \oplus S(X_0^4 \oplus S(X_0^{10} \oplus S(X_0^1 \oplus K_0^1) \oplus K_1^0) \oplus K_2^2) \oplus K_3^3)$$

Similarly, the nibble X_{18}^{14} is affected by 48 bits of ciphertext X_{23} and 48 bits of round keys:

$$\begin{aligned}X_{18}^{14} = X_{23}^{0} \oplus S(X_{23}^{9} \oplus K_{22}^{1}) \oplus S(X_{23}^{14} \oplus S(X_{23}^{2} \oplus S(X_{23}^{8} \oplus K_{22}^{0}) \oplus K_{21}^{4}) \oplus K_{20}^{0}) \oplus \\ S(X_{23}^{9} \oplus S(X_{23}^{1} \oplus S(X_{23}^{11} \oplus K_{22}^{3}) \oplus K_{21}^{3}) \oplus S(X_{23}^{6} \oplus S(X_{23}^{12} \oplus K_{22}^{4}) \oplus \\ S(X_{23}^{15} \oplus S(X_{23}^{4} \oplus S(X_{23}^{13} \oplus K_{22}^{5}) \oplus K_{21}^{6}) \oplus K_{20}^{1}) \oplus K_{19}^{2}) \oplus K_{18}^{5})\end{aligned}$$

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

$K_0^7 \Rightarrow K_1^0[0-2]$, $K_{21}^3 \Rightarrow K_{18}^5[0-2]$, $K_{21}^4 \Rightarrow K_{18}^5[3]$, $K_{22}^0 \Rightarrow K_{19}^2[0-2]$, $K_{22}^1 \Rightarrow K_{19}^2[3]$ and $K_{20}^0 \Rightarrow K_{22}^5[2-3]$.

Assuming that N known plaintexts are used, the partial encryption and decryption using the partial-compression technique are proceeded as in Table 2. The second column stands for the subkey nibbles that have to be guessed in each step. 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 possible value of $x_i (1 \le i \le 13)$, 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 more clear, we explain some steps in Table 2 in detail.

Step 4.1. We allocate the 60-bit counter $N_1[x_1]$ and initialize it to zero. We then guess 17-bit keys and partially encrypt N plaintexts to compute x_1, and increment the corresponding counter.

The guessed keys are $K_0^1, K_0^7, K_1^0[3]$ and K_{22}^0, K_{21}^4. Because $K_0^7[1-3]$ are equivalent to $K_1^0[0-2]$, K_1^0 are all known. As shown in Figure 2, the values of $X_4^1|X_{18}^{14}$ are affected by 32 bits of plaintext and 48 bits of ciphertext. They are represented by

$$\begin{aligned}x_0 = X_0^5|X_0^{12}|X_0^0|X_0^{15}|X_0^7|X_0^4|X_0^{10}|X_0^1|X_{23}^0|X_{23}^9|X_{23}^{14}|X_{23}^2|X_{23}^8|X_{23}^1|X_{23}^{11}| \\ X_{23}^6|X_{23}^{12}|X_{23}^{15}|X_{23}^4|X_{23}^{13}.\end{aligned}$$

As the following three equations

$$\begin{aligned}X_1^5 &= X_0^{15} \oplus S(X_0^7 \oplus K_0^7) \\ X_2^2 &= X_0^4 \oplus S(X_0^{10} \oplus S(X_0^1 \oplus K_0^1) \oplus K_1^0) \\ X_{21}^8 &= X_{23}^{14} \oplus S(X_{23}^2 \oplus S(X_{23}^8 \oplus K_{22}^0) \oplus K_{21}^4)\end{aligned}$$

are true for LBlock, the 80-bit x_0 can be reduced to 60-bit x_1 after guessing the 17 bits keys. Update the expressions of X_4^1 and X_{18}^{14}:

$$X_4^1 = X_0^5 \oplus S(X_0^{12} \oplus S(X_0^0 \oplus K_0^0) \oplus K_1^2) \oplus S(X_1^5 \oplus S(X_2^2 \oplus K_2^2) \oplus K_3^3)$$

$$\begin{aligned}X_{18}^{14} = X_{23}^{0} \oplus S(X_{23}^{9} \oplus K_{22}^{1}) \oplus S(X_{21}^{8} \oplus K_{20}^{0}) \oplus S(X_{23}^{9} \oplus S(X_{23}^{1} \oplus S(X_{23}^{11} \oplus K_{22}^{3}) \\ \oplus K_{21}^{3}) \oplus S(X_{23}^{6} \oplus S(X_{23}^{12} \oplus K_{22}^{4}) \oplus S(X_{23}^{15} \oplus S(X_{23}^{4} \oplus S(X_{23}^{13} \oplus K_{22}^{5}) \\ \oplus K_{21}^{6}) \oplus K_{20}^{1}) \oplus K_{19}^{2}) \oplus K_{18}^{5})\end{aligned}$$

Step 4.2. We first allocate 56-bit counter $N_2[x_2]$ and initialize them to zero. We then guess 4-bit K_{20}^0 and partially decrypt x_1 to compute x_2 and add the corresponding $N_1[x_1]$ to $N_2[x_2]$. During the above process, A is defined as $X_{23}^0 \oplus S(X_{21}^8 \oplus K_{20}^0)$. Meanwhile, the expression of X_{18}^{14} is update as:

$$X_{18}^{14} = A \oplus S(X_{23}^9 \oplus K_{22}^1) \oplus S(X_{23}^9 \oplus S(X_{23}^1 \oplus S(X_{23}^{11} \oplus K_{22}^3) \oplus K_{21}^3) \oplus S(X_{23}^6 \oplus S(X_{23}^{12} \oplus K_{22}^4) \oplus S(X_{23}^{15} \oplus S(X_{23}^4 \oplus S(X_{23}^{13} \oplus K_{22}^5) \oplus K_{21}^6) \oplus K_{20}^1) \oplus K_{19}^2) \oplus K_{18}^5).$$

Table 2. Partial encryption and decryption on 23-round LBlock

Step	Guess	Time	Obtained States	Size
4.1	$K_0^1, K_0^7, K_1^0[3]$ K_{22}^0, K_{21}^4	$N \cdot 2^{17} \cdot 5$	$x_1 = X_0^5 \vert X_0^{12} \vert X_0^0 \vert X_1^5 \vert X_2^2 \vert X_{23}^0 \vert X_{23}^9 \vert X_{21}^8 \vert$ $X_{23}^1 \vert X_{23}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{23}^4 \vert X_{23}^{13}$	2^{60}
4.2	K_{20}^0	$2^{60} \cdot 2^{17+4}$	$x_2 = X_0^5 \vert X_0^{12} \vert X_0^0 \vert X_1^5 \vert X_2^2 \vert A \vert X_{23}^9 \vert X_{23}^1 \vert$ $X_{23}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{23}^4 \vert X_{23}^{13}$	2^{56}
4.3	$K_{22}^5[0,1]$	$2^{56} \cdot 2^{21+2}$	$x_3 = X_0^5 \vert X_0^{12} \vert X_0^0 \vert X_1^5 \vert X_2^2 \vert A \vert X_{23}^9 \vert$ $X_{23}^1 \vert X_{23}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{22}^{14}$	2^{52}
4.4	K_2^2	$2^{52} \cdot 2^{23+4}$	$x_4 = X_0^5 \vert X_0^{12} \vert X_0^0 \vert X_3^3 \vert A \vert X_{23}^9 \vert X_{23}^1 \vert X_{23}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{22}^{14}$	2^{48}
4.5	K_0^0	$2^{48} \cdot 2^{27+4}$	$x_5 = X_0^5 \vert X_1^2 \vert X_3^3 \vert A \vert X_{23}^9 \vert X_{23}^1 \vert X_{23}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{22}^{14}$	2^{44}
4.6	K_1^2	$2^{44} \cdot 2^{31+4}$	$x_6 = X_3^{11} \vert X_3^3 \vert A \vert X_{23}^9 \vert X_{23}^1 \vert X_{23}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{22}^{14}$	2^{40}
4.7	K_3^3	$2^{40} \cdot 2^{35+4}$	$x_7 = X_4^1 \vert A \vert X_{23}^9 \vert X_{23}^1 \vert X_{23}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{22}^{14}$	2^{36}
4.8	K_{22}^3	$2^{36} \cdot 2^{39+4}$	$x_8 = X_4^1 \vert A \vert X_{23}^9 \vert X_{22}^{11} \vert X_{23}^6 \vert X_{23}^{12} \vert X_{23}^{15} \vert X_{22}^{14}$	2^{32}
4.9	K_{22}^4	$2^{32} \cdot 2^{43+4}$	$x_9 = X_4^1 \vert A \vert X_{23}^9 \vert X_{22}^{11} \vert X_{22}^8 \vert X_{23}^{15} \vert X_{22}^{14}$	2^{28}
4.10	K_{21}^6	$2^{28} \cdot 2^{47+4}$	$x_{10} = X_4^1 \vert A \vert X_{23}^9 \vert X_{22}^{11} \vert X_{22}^8 \vert X_{21}^9$	2^{24}
4.11	K_{20}^1	$2^{24} \cdot 2^{51+4}$	$x_{11} = X_4^1 \vert A \vert X_{23}^9 \vert X_{22}^{11} \vert X_{20}^{10}$	2^{20}
4.12	$K_{22}^1(K_{19}^2)$	$2^{20} \cdot 2^{55+4} \cdot 2$	$x_{12} = X_4^1 \vert B \vert C \vert X_{22}^{11}$	2^{16}
4.13	$K_{21}^3(K_{18}^5)$	$2^{16} \cdot 2^{59+4} \cdot 2$	$x_{13} = X_4^1 \vert X_{18}^{14}$	2^8

† $A = X_{23}^0 \oplus S(X_{21}^8 \oplus K_{20}^0)$ † $B = A \oplus S(X_{23}^9 \oplus K_{22}^1)$ † $C = X_{23}^9 \oplus S(X_{20}^{10} \oplus K_{19}^2)$

Because the following steps are similar to the above two steps, we do not explain in details. Besides, we note that the numbers of guessed keys in Step 12 and Step 13 are both 4-bit. However, the numbers of known keys are both 8 bit, that is because the key in the $'()'$ can be obtained by using the relations of round keys.

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 8 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 $T_k = \frac{N \cdot 2^8}{(1-2^{-8})} \sum_{z=0}^{2^8-1} \left(\frac{V[z]}{N} - \frac{1}{2^8}\right)^2$.
4. If $T_k < \tau$, then the guessed subkey values are possible right subkey candidates.
5. Do exhaustive search for all right candidates.

Complexity. We set $\alpha = 2^{-2.7}, \beta = 2^{-9}$, then $z_{1-\alpha} \approx 1, z_{1-\beta} \approx 2.88$. Since $n = 64$ and $l = 255$, then according to equation 2, the data complexity N is about $2^{62.1}$. Now we evaluate the time complexity of the key recovery on 23-round LBlock. We first sum the cost of step 1 to step 14 in the process of partial computation and the result is about $2^{81} \cdot 6$ S-box access, which is about $2^{81} \cdot 6 \cdot 1/8 \cdot 1/23 \approx 2^{76}$ 23-round LBlock encryptions. The number of remaining key candidates is about $2^{80} \cdot \beta \approx 2^{71}$. The total time complexity is $2^{76} + 2^{71} \approx 2^{76}$ 23-round LBlock encryptions.

All in all, the data complexity of our attack on 23-round LBlock is $2^{62.1}$ known plaintexts, the time complexity is 2^{76} 23-round LBlock encryptions and the memory requirements are about 2^{60} bytes.

5 Application to TWINE

In this section, we apply the improved multidimensional zero-correlation linear attack model to TWINE block cipher and give attacks on 23-round TWINE-80 and 25-round TWINE-128.

5.1 A Brief Description of TWINE

Encryption Algorithm. Round function of TWINE consists of eight identical 4-bit S-boxes and a diffusion layer π, which is depicted in Figure 3. This round function is iterated for 36 times for both TWINE-80 and TWINE-128, where the diffusion layer of the last round is omitted.

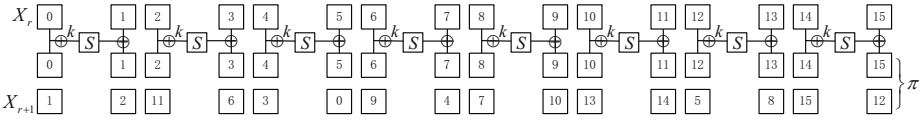

Fig. 3. Round function of TWINE block cipher

Key Schedule Algorithm. The key schedule of TWINE is quite simple. S-boxes, XOR operations and a series of constants are used in the key schedule. Due to the page limit, see the specific key schedule algorithms for both key lengths in Reference [8].

5.2 Zero-Correlation Linear Approximations of 14-Round TWINE

We find that there are at least 8×8 zero-correlation linear hulls for 14-round TWINE and the characteristics can be summarized as the following property:

Property 2. For 14-round TWINE, if the input mask a of the first round locates at the even nibble and the output mask b of the last round locates in the odd

nibble, then the correlation of the linear approximation is zero, where $a, b \in F_2^4$, $a \neq 0$ and $b \neq 0$.

To distinguish the 64 different zero-correlation hulls, we express the distinguisher as (l_a, l_b), where $0 \leq l_a \leq 14$ is an even integer and $1 \leq l_b \leq 15$ is an odd integer.

5.3 Key Recovery for 23-Round TWINE-80

Step 1. As noted before, $R = 23$ and $R_d = 14$ for block cipher TWINE-80. The original set is $\{((l_a, l_b), R_e), 0 \leq R_e \leq 9\}$.

Step 2. After analyzing the encryption algorithm, the candidates are reduced to $S = \{((l_a, l_b), R_e), 4 \leq R_e \leq 5\}$.

Step 3. Only one element $\{((2, 9), 4)\}$ is left in the optimal set O. The size of the guessed keys is reduced from 76 bits to 60 bits.

Step 4. We use $((2, 9), 4)$ to give an attack on 23-round TWINE-80. By puting these 14-round zero-correlation linear approximations in rounds 4 to 17, we can attack TWINE-80 from round 0 to round 22. Similarly, we first express the two target values and then guess the keys one nibble after another to reduce the time complexity of partial computation. The nibble X_4^2 is affected by 32 bits of plaintext X_0 and 28 bits of round keys and the expression can be shown as:

$$X_4^2 = X_0^{12} \oplus S(X_0^{15} \oplus S(X_0^{14} \oplus K_0^7) \oplus K_1^7) \oplus S(X_0^7 \oplus S(X_0^6 \oplus K_0^3) \oplus S(X_0^0 \oplus S(X_0^3 \oplus S(X_0^2 \oplus K_0^1) \oplus K_1^2) \oplus K_2^6) \oplus K_3^5)$$

Similarly, the nibble X_{18}^9 is affected by 48 bits of ciphertext X_{23} and 48 bits of round keys:

$$X_{18}^9 = X_{23}^8 \oplus S(X_{23}^3 \oplus K_{22}^3) \oplus S(X_{23}^5 \oplus S(X_{23}^{12} \oplus S(X_{23}^7 \oplus K_{22}^2) \oplus K_{21}^0) \oplus K_{20}^1) \oplus S(X_{23}^3 \oplus S(X_{23}^{10} \oplus S(X_{23}^{15} \oplus K_{22}^6) \oplus K_{21}^4) \oplus S(X_{23}^2 \oplus S(X_{23}^9 \oplus K_{22}^5) \oplus S(X_{23}^1 \oplus S(X_{23}^6 \oplus S(X_{23}^{13} \oplus K_{22}^4) \oplus K_{21}^5) \oplus K_{20}^7) \oplus K_{19}^6) \oplus K_{18}^4)$$

The following relations exist in the related round keys:

$$K_3^5 \Longleftrightarrow K_0^3, K_2^6 \Longleftrightarrow K_0^1, K_{21}^0 \Longleftrightarrow K_{18}^4 \text{ and } K_{20}^1 \Longleftrightarrow K_{22}^6.$$

Assuming that N known plaintexts are used, the partial encryption and decryption using the partial-compression technique are proceeded as in Table 3. Finally, attackers compute the statistic T_k for every guessed k and do exhaustive search for all right candidates. The process can be referred to that of LBlock.

Complexity. We also set $\alpha = 2^{-2.7}, \beta = 2^{-9}$, then $z_{1-\alpha} \approx 1, z_{1-\beta} \approx 2.88$. Since $n = 64$ and $l = 255$, the data complexity N is about $2^{62.1}$. The complexity of partial computation is about $2^{76} \cdot 8$ S-box access, which is about $2^{76} \cdot 8 \cdot 1/8 \cdot$

Table 3. Partial encryption and decryption on 23-round TWINE-80

Step	Guess	Time	Obtained States	Size
4.1	$K_3^5(K_0^3)$, $K_2^6(K_0^1), K_1^2$	$N \cdot 2^{12} \cdot 5$	$x_1 = A\|X_0^{15}\|X_0^{14}\|X_{23}^8\|X_{23}^3\|X_{23}^5\|X_{23}^{12}\|$ $X_{23}^7\|X_{23}^{10}\|X_{23}^{15}\|X_{23}^2\|X_{23}^9\|X_{23}^1\|X_{23}^6\|X_{23}^{13}$	2^{60}
4.2	K_0^7	$2^{60} \cdot 2^{16}$	$x_2 = A\|X_1^{14}\|X_{23}^8\|X_{23}^3\|X_{23}^5\|X_{23}^{12}\|X_{23}^7\|X_{23}^{10}\|$ $X_{23}^{15}\|X_{23}^2\|X_{23}^9\|X_{23}^1\|X_{23}^6\|X_{23}^{13}$	2^{56}
4.3	K_1^7	2^{76}	$x_3 = X_4^2\|X_{23}^8\|X_{23}^3\|X_{23}^5\|X_{23}^{12}\|X_{23}^7\|X_{23}^{10}\|$ $X_{23}^{15}\|X_{23}^2\|X_{23}^9\|X_{23}^1\|X_{23}^6\|X_{23}^{13}$	2^{52}
4.4	K_{22}^2	2^{76}	$x_4 = X_4^2\|X_{23}^8\|X_{23}^3\|X_{23}^5\|X_{22}^5\|X_{23}^{10}\|X_{23}^{15}\|X_{23}^2\|X_{23}^9\|X_{23}^1\|X_{23}^6\|X_{23}^{13}$	2^{48}
4.5	K_{21}^0	2^{76}	$x_5 = X_4^2\|X_{23}^8\|X_{23}^3\|X_{21}^1\|X_{23}^{10}\|X_{23}^{15}\|X_{23}^2\|X_{23}^9\|X_{23}^1\|X_{23}^6\|X_{23}^{13}$	2^{44}
4.6	$K_{22}^6(K_{20}^1)$	$2^{76} \cdot 2$	$x_6 = X_4^2\|B\|X_{23}^3\|X_{22}^{13}\|X_{23}^2\|X_{23}^9\|X_{23}^1\|X_{23}^6\|X_{23}^{13}$	2^{36}
4.7	K_{22}^5	2^{72}	$x_7 = X_4^2\|B\|X_{23}^3\|X_{22}^{13}\|X_{22}^{11}\|X_{23}^1\|X_{23}^6\|X_{23}^{13}$	2^{32}
4.8	K_{22}^4	2^{72}	$x_8 = X_4^2\|B\|X_{23}^3\|X_{22}^{13}\|X_{22}^{11}\|X_{23}^1\|X_{22}^9$	2^{28}
4.9	K_{21}^5	2^{72}	$x_9 = X_4^2\|B\|X_{23}^3\|X_{22}^{13}\|X_{22}^{11}\|X_{21}^{11}$	2^{24}
4.10	K_{20}^7	2^{72}	$x_{10} = X_4^2\|B\|X_{23}^3\|X_{22}^{13}\|X_{20}^{15}$	2^{20}
4.11	K_{22}^3	2^{72}	$x_{11} = X_4^2\|X_{20}^3\|X_{23}^3\|X_{22}^{13}\|X_{20}^{15}$	2^{20}
4.12	K_{21}^4	2^{76}	$x_{12} = X_4^2\|X_{20}^3\|X_{21}^9\|X_{20}^{15}$	2^{16}
4.13	K_{19}^6	2^{76}	$x_{13} = X_4^2\|X_{18}^9$	2^8

† $A = X_0^{12} \oplus S(X_0^7 \oplus S(X_0^6 \oplus K_0^3) \oplus S(X_0^0 \oplus S(X_0^3 \oplus S(X_0^2 \oplus K_0^1) \oplus K_1^2) \oplus K_2^6) \oplus K_3^5)$
† $B = X_{23}^8 \oplus S(X_{21}^1 \oplus K_{20}^1)$

$1/23 \approx 2^{71.48}$ 23-round TWINE-80 encryptions. The number of remaining key candidates is about $2^{80} \cdot \beta \approx 2^{71}$. Thus, the total time complexity is $2^{71.48} + 2^{71} \approx 2^{72.15}$ 23-round TWINE-80 encryptions. Meanwhile, the memory requirements are about 2^{60} bytes.

5.4 Key Recovery for 25-Round TWINE-128

Step 1. $R = 25$ and $R_d = 14$ for block cipher TWINE-128 and the original set equals to $\{((l_a, l_b), R_e), 0 \leq R_e \leq 11\}$.

Step 2. When encrypting 5 or 6 rounds, the number of guessed keys is minimal(124 bits) and $S = \{((l_a, l_b), R_e), 5 \leq R_e \leq 6\}$.

Step 3. After deleting the equivalent keys for every element in S, we find that only the cases in $O = \{((l_a, l_b), 5), ((l_a^*, l_b^*), 6),\ l_a \in \{0, 4, 12, 14\}, l_b = 9, l_a^* \in \{0, 4, 10, 14\}, l_b^* = 11\}\}$ needs to guess 112-bit keys.

Step 4. The distinguisher $((4, 9), 5)$ is chosen to attack 25-round TWINE-128. Firstly, express X_5^4 by using subkeys and plaintexts and X_{19}^9 by using subkeys and ciphertexts.

$$X_5^4 = X_0^{13} \oplus S(X_0^{12} \oplus K_0^6) \oplus S(X_0^4 \oplus S(X_0^9 \oplus S(X_0^8 \oplus K_0^4) \oplus K_1^3) \oplus K_2^4) \oplus S(X_0^{12} \oplus S(X_0^{15} \oplus S(X_0^{14} \oplus K_0^7) \oplus K_1^7) \oplus S(X_0^7 \oplus S(X_0^6 \oplus K_0^3) \oplus S(X_0^0 \oplus S(X_0^3 \oplus S(X_0^2 \oplus K_0^1) \oplus K_1^2) \oplus K_2^6) \oplus K_3^5) \oplus K_4^1)$$

$$X_{19}^9 = X_{25}^{13} \oplus S(X_{25}^4 \oplus S(X_{25}^1 \oplus K_{24}^1) \oplus K_{23}^3) \oplus S(X_{25}^{12} \oplus S(X_{25}^7 \oplus K_{24}^2) \oplus S(X_{25}^{15} \oplus S(X_{25}^8 \oplus S(X_{25}^3 \oplus K_{24}^3) \oplus K_{23}^2) \oplus K_{22}^0) \oplus K_{21}^1) \oplus S(X_{25}^4 \oplus S(X_{25}^1 \oplus K_{24}^1) \oplus S(X_{25}^9 \oplus S(X_{25}^{14} \oplus S(X_{25}^{11} \oplus K_{24}^7) \oplus K_{23}^6) \oplus K_{22}^4) \oplus S(X_{25}^1 \oplus S(X_{25}^6 \oplus S(X_{25}^{13} \oplus K_{24}^4) \oplus K_{23}^5) \oplus S(X_{25}^0 \oplus S(X_{25}^5 \oplus K_{24}^0) \oplus S(X_{25}^3 \oplus S(X_{25}^{10} \oplus S(X_{25}^{15} \oplus K_{24}^6) \oplus K_{23}^4) \oplus K_{22}^5) \oplus K_{21}^7) \oplus K_{20}^6) \oplus K_{19}^4)$$

Meanwhile, the following equivalent relations exist in the related round keys of TWINE-128:

$$K_4^1 \Longleftrightarrow K_1^3, K_{24}^2 \Longleftrightarrow K_{20}^6 \text{ and } K_{24}^6 | K_{24}^7 \Rightarrow K_{19}^4.$$

The partial encryption and decryption are similarly proceeded as in Table 4.

Table 4. Partial encryption and decryption on 25-round TWINE-128

Step	Guess	Time	Obtained States	Size
4.1	$K_{24}^{0-4,6,7}, K_{22}^{4,5}, K_{23}^{2-6}, K_{21}^7$	$N \cdot 2^{60} \cdot 17$	$x_1 = A \vert X_{23}^5 \vert X_{23}^0 \vert X_0^{15} \vert X_0^{14} \vert X_0^{13} \vert X_0^{12} \vert X_0^9 \vert X_0^8 \vert X_0^7 \vert X_0^6 \vert X_0^4 \vert X_0^3 \vert X_0^2 \vert X_0^0$	2^{60}
4.2	K_{22}^0	2^{124}	$x_2 = A \vert X_{22}^1 \vert X_0^{15} \vert X_0^{14} \vert X_0^{13} \vert X_0^{12} \vert X_0^9 \vert X_0^8 \vert X_0^7 \vert X_0^6 \vert X_0^4 \vert X_0^3 \vert X_0^2 \vert X_0^0$	2^{56}
4.3	K_{21}^1	2^{124}	$x_3 = X_{19}^9 \vert X_0^{15} \vert X_0^{14} \vert X_0^{13} \vert X_0^{12} \vert X_0^9 \vert X_0^8 \vert X_0^7 \vert X_0^6 \vert X_0^4 \vert X_0^3 \vert X_0^2 \vert X_0^0$	2^{52}
4.4	K_0^4	2^{124}	$x_4 = X_{19}^9 \vert X_0^{15} \vert X_0^{14} \vert X_0^{13} \vert X_0^{12} \vert X_1^6 \vert X_0^7 \vert X_0^6 \vert X_0^4 \vert X_0^3 \vert X_0^2 \vert X_0^0$	2^{48}
4.5	K_1^3	2^{124}	$x_5 = X_{19}^9 \vert X_0^{15} \vert X_0^{14} \vert X_0^{13} \vert X_0^{12} \vert X_2^8 \vert X_0^7 \vert X_0^6 \vert X_0^3 \vert X_0^2 \vert X_0^0$	2^{44}
4.6	K_0^7	2^{124}	$x_6 = X_{19}^9 \vert X_1^{14} \vert X_0^{13} \vert X_0^{12} \vert X_2^8 \vert X_0^7 \vert X_0^6 \vert X_0^3 \vert X_0^2 \vert X_0^0$	2^{40}
4.7	K_0^3	2^{124}	$x_7 = X_{19}^9 \vert X_1^{14} \vert X_0^{13} \vert X_0^{12} \vert X_2^8 \vert X_1^8 \vert X_0^3 \vert X_0^2 \vert X_0^0$	2^{36}
4.8	K_0^1	2^{124}	$x_8 = X_{19}^9 \vert X_1^{14} \vert X_0^{13} \vert X_0^{12} \vert X_2^8 \vert X_1^8 \vert X_1^4 \vert X_0^0$	2^{32}
4.9	K_1^2	2^{124}	$x_9 = X_{19}^9 \vert X_1^{14} \vert X_0^{13} \vert X_0^{12} \vert X_2^8 \vert X_1^8 \vert X_2^{12}$	2^{28}
4.10	K_2^6	2^{124}	$x_{10} = X_{19}^9 \vert X_1^{14} \vert X_0^{13} \vert X_0^{12} \vert X_2^8 \vert X_3^{10}$	2^{24}
4.11	K_2^4	2^{124}	$x_{11} = X_{19}^9 \vert B \vert X_1^{14} \vert X_0^{12} \vert X_3^{10}$	2^{20}
4.12	K_1^7, K_3^5	$2^{128} \cdot 3$	$x_{12} = X_{19}^9 \vert C \vert X_0^{12}$	2^{12}
4.13	K_0^6	2^{124}	$x_{13} = X_{19}^9 \vert X_5^4$	2^8

† $A = X_{23}^7 \oplus S(X_{23}^6 \oplus S(X_{23}^{13} \oplus K_{22}^4) \oplus S(X_{23}^{11} \oplus S(X_{23}^2 \oplus S(X_{23}^9 \oplus K_{22}^5) \oplus K_{21}^7) \oplus K_{20}^6) \oplus K_{19}^4)$
† $B = X_0^{13} \oplus S(X_2^8 \oplus K_2^4)$
† $C = B \oplus S(X_0^{12} \oplus S(X_1^{14} \oplus K_1^7) \oplus S(X_3^{10} \oplus K_3^5) \oplus K_4^1)$

Complexity. We set $\alpha = 2^{-2.7}, \beta = 2^{-9}$, then $z_{1-\alpha} \approx 1, z_{1-\beta} \approx 2.88$. Since $n = 64$ and $l = 255$, then according to equation 2, the data complexity N is

also about $2^{62.1}$. The total time complexity is $2^{121.95} + 2^{119} \approx 2^{122.12}$ 25-round TWINE-128 encryptions and the memory requirements are about 2^{60} bytes to store counter in Step 4.1.

6 Conclusion

In this paper, we first present an improved model of multidimensional zero-correlation linear cryptanalysis by taking the key schedule algorithm into consideration. Besides, partial-compression technique is used to reduce the time complexity, which is similar to the partial-sum technique of integral attack. In order to illustrate the improved attack model, we evaluate the security of LBlock and TWINE block cipher against zero-correlation linear cryptanalysis. Based on 14-round zero-correlation distinguishers, we presented attacks on 23-round LBlock, 23-round TWINE-80 and 25-round TWINE-128. In terms of the number of attacked rounds, the result on LBlock is better than any previously published results in the single key model up to now. While the previous attack on TWINE-80 and TWINE-128, which can break the same number of rounds, uses chosen plaintexts, our attacks assume only the known plaintexts and the attack on TWINE-80 is of the less time complexity and memory. As discussed above, we conclude that the diffusion of the key schedule algorithms influence the security of block ciphers against zero-correlation linear cryptanalysis. Moreover, the results reveal a criterion of designing the key schedule algorithm. Specifically, designers should avoid equivalent subkeys when partly encrypting or decrypting ciphers to obtain a single nibble.

Acknowledgments. We thank the anonymous reviewers for their useful comments that help to improve the paper. The research presented in this paper is supported by the National Basic Research Program of China (No. 2013CB338002) and National Natural Science Foundation of China (No. 61272476, No.61232009 and No. 61202420).

References

1. Bogdanov, A., Rijmen, V.: Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Designs, Codes and Cryptography 70(3), 369–383 (2014)
2. Bogdanov, A., Wang, M.Q.: Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 29–48. Springer, Heidelberg (2012)
3. Bogdanov, A., Leander, G., Nyberg, K., Wang, M.Q.: 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)
4. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., 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)

5. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
6. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: An Ultra-Lightweight Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 342–357. Springer, Heidelberg (2011)
7. 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)
8. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: A Lightweight Block Cipher for Multiple Platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013)
9. Soleimany, H., Nyberg, K.: Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock. Cryptology ePrint Archive, `https://eprint.iacr.org/2012/570`
10. 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)
11. Çoban, M., Karakoç, F., Boztaş, Ö.: Biclique Cryptanalysis of TWINE. In: Pieprzyk, J., Sadeghi, A.-R., Manulis, M. (eds.) CANS 2012. LNCS, vol. 7712, pp. 43–55. Springer, Heidelberg (2012)
12. 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)
13. 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)
14. Boztaş, Ö., Karakoç, F., Çoban, M.: Multidimensional Meet-in-the-middle Attacks on Reduced-Round TWINE-128. In: Avoine, G., Kara, O. (eds.) LightSec 2013. LNCS, vol. 8162, pp. 55–67. Springer, Heidelberg (2013)
15. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) Advances in Cryptology - EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)