The ISC Int'l Journal of Information Security

ISeCure

January 2019, Volume 11, Number 1 (pp. 57–74)

http://www.isecure-journal.org

# Biclique Cryptanalysis of Block Ciphers LBlock and TWINE-80 with Practical Data Complexity☆

Siavash Ahmadi [1,*], Zahra Ahmadian [2], Javad Mohajeri [1], and Mohammad Reza Aref [1]

[1] *Sharif University of Technology, Tehran, Iran*

[2] *Shahid Beheshti University, Tehran, Iran*

ARTICLE INFO.

*Article history:*

**Received:** 30 June 2018

**Revised:** 13 November 2018

**Accepted:** 8 December 2018

**Published Online:** 30 January 2019

*Keywords:*

Lightweight Cryptography, Biclique Cryptanalysis, Partial Matching, Early Abort Technique.

ABSTRACT

In the biclique attack, a shorter biclique usually results in less data complexity, but at the expense of more computational complexity. The early abort technique can be used in partial matching part of the biclique attack in order to slightly reduce the computations. In this paper, we make use of this technique, but instead of slight improvement in the computational complexity, we keep the amount of this complexity the same and reduce the data complexity enormously by a shorter biclique. With this approach, we analyze full-round LBlock, and also LBlock with modified key schedule (which was designed to resist biclique attack) both with data complexity $2^{12}$, while the data complexity of the best biclique attack on the former was $2^{52}$ and for the latter there is no attack on the full-round cipher, so far. Then we propose a new key schedule that is more resistant against biclique cryptanalysis, though the low diffusion of the cipher makes it vulnerable to this attack regardless of the strength of the key schedule. Also using this method, we analyze TWINE-80 with $2^{12}$ data complexity. The lowest data complexity for the prior attack on the TWINE-80 was $2^{60}$. In all the attacks presented in this paper, the computational complexities are slightly improved in comparison to the existing attacks.





## 1 Introduction

Lightweight cryptography is a new domain in cryptography aiming to design and evaluate of cryptographic primitives and protocols tailored for extremely resource constraint devices. In the recent decade there has been an enormous effort specially in symmetric cryptography community at design of lightweight primitives such as Piccolo [2], Present [3], LED [4], Klein [5] block ciphers and Quark [6], Photon [7] and Spongent [8] hash functions.

LBlock is one of these lightweight block ciphers with 64-bit block and 80-bit key sizes [9]. Up to now, the security of LBlock against various attacks has been evaluated and some papers has been presented including Integral attack [10], impossible differential attack [11], zero correlation attack [12], truncated differential attack [13], and related key attack [14]. So far, the only attack which successfully cryptanalyzed full-round LBlock is the biclique attack [15, 16]. The attack proposed by the LBlock designers [15], could reduce the key space about 1.6 bit with $2^{52}$ data. Having concluded the vulnerability of LBlock to biclique

☆ An earlier version of this paper has already been presented in ISCISC'2015.

* Corresponding author.

Email addresses: s_ahmadi@ee.sharif.edu (S. Ahmadi), z_ahmadian@sbu.ac.ir (Z. Ahmadian), mohajer@sharif.edu (J. Mohajeri), aref@sharif.edu (M.R. Aref)

ISSN: 2008-2045 

cryptanalysis is due to some weakness in its key schedule, a modified key schedule is presented to strengthen it against this type of attack.

TWINE is another 64-bit lightweight block cipher that has two versions with 80- and 128-bit key sizes [17]. Apart from designers' evaluations, it received a related key attack on the reduced-round TWINE-128 [14], and some external cryptanalysis using biclique technique on the full-round versions [16, 18]. Here, our focus is on TWINE-80.

Biclique attack has shown to work faster than brute force attack in cryptanalysis of full round version of many block ciphers[19–24], especially those with generalized feistel structure. This paper focuses on this kind of attack on some lightweight block ciphers with emphasis on the data complexity.

### Our Contribution

We explain how to improve the efficiency of biclique attack using the so called *early abort technique* [25] in the matching part. We examined this method on LBlock and TWINE block ciphers and making use of this technique along with the low data complexity biclique attack [22], we can dramatically reduce the data complexity of the attack comparing to the previous biclique attacks, while keeping the computational complexity the same (or slightly better).

In all cases (e.g. LBlock, LBlock with modified key schedule, and TWINE-80), our attacks require $2^{12}$ plaintext/ciphertext pairs. We show that the modified key schedule presented by the designers in [15] still suffers from the same weakness as with the original key schedule and we could analyze LBlock with modified key schedule with computational complexity of $2^{78.74}$, and data complexity of $2^{12}$. To the best of our knowledge, it is the first attack on the full-round LBlock with modified key schedule. At the end, we propose another key schedule which resolves this problem and increases the resistance of the LBlock against biclique cryptanalysis and still preserve it as a lightweight block cipher. A summary of the previous attacks on full-round LBlock and TWINE-80, as well as our attack, is listed in Table 1.

This paper follows this procedure: Section 2 presents the improved biclique attack. Section 3 presents a brief description of LBlock and TWINE-80. We apply our attacks on LBlock and LBlock with modified key schedule in Section 4. Also, a new lightweight key schedule algorithm for LBlock is proposed to enforce it against biclique attack. We apply our attack to TWINE-80 in Section 5, and we conclude our work in Section 6.

## 2 Biclique Attack with Early Abort Technique

Biclique cryptanalysis was proposed in [19] as a successful attack for cryptanalysis of full round AES. Moreover, the cryptanalytic results on a large number of block ciphers shows that this is a generally applicable attack. Our approach enjoys an improvement in the matching part which dominates the computational complexity of biclique cryptanalysis. We use the early abort technique in partial matching part to avoid additional computations which are not necessary. Early abort technique was first introduced in improving the impossible differential attack [25]. Almost all the biclique attacks can be improved by this technique to a greater and lesser extent. Better results are observed for the block ciphers which have lower diffusion in the data processing part of the algorithm.

The details of biclique attack can be found in [19] and it is summarized in the other attacks such as [22]. We briefly explain it here with emphasis on how to make use of early abort technique in the partial matching part. In the biclique attack and also in the improved version of it, the biclique can be constructed either in the plaintext or ciphertext side. In this section, we explain the details of improved biclique attack in the case that the biclique is constructed in the plaintext side.

**Key partitioning.** First divide the master key $K$ into three disjoint sets of $d$, $d$ and $n-2d$ bits, namely $K^f$, $K^b$ and $K^g$, respectively. For any constant value of $K^g$, we can define a group of keys in which the keys only differ in $K^f$ and $K^b$. All keys in a group are shown by $K[i,j]$ where $K^f = j$ and $K^b = i$ for $0 \leq i,j \leq 2^d - 1$. Then, we repeat the other steps for each group. We also define the differences $\nabla_i^K = K[0,0] \oplus K[i,0]$ and $\Delta_j^K = K[0,0] \oplus K[0,j]$.

**Biclique constructing.** The 3-tuple $[\{P_i\},\{S_j\},\{K[i,j]\}]$ is called a $d$-dimensional biclique with length $l$, if:

$$\forall i,j \in \{0,1,...,2^d-1\} : P_i \xrightarrow[0,l-1]{K[i,j]} S_j, \qquad (1)$$

where $\{P_i\}$ is a set of $2^d$ plaintexts, $\{S_j\}$ is a set of $2^d$ internal states and $\xrightarrow[a,b]{K[i,j]}$ denotes the encryption with key $K[i,j]$ from round $a$ to round $b$ ($\xleftarrow[a,b]{K[i,j]}$ stands for decryption)(see Figure 1).

The most common method for constructing the biclique, namely Independent Biclique method [19], is as follows:

Step 1. Choose a random plaintext $P_0$ and compute $S_0$ as $P_0 \xrightarrow[0,l-1]{K[0,0]} S_0$.

**Table 1**. A comparison of our attacks with the previous biclique attacks on LBlock and TWINE

| Block Cipher | Rounds | Computations | Data | Memory | Biclique Length | Reference |
|---|---|---|---|---|---|---|
| LBlock | Full(32) | $2^{78.76}$ | $2^{64}$ | $2^4$ | 9 | [16] |
| | Full(32) | $2^{78.4}$ | $2^{52}$ | $2^4$ | 8 | [15] |
| | Full(32) | $2^{78.4}$ | $2^{12}$ | $2^4$ | 5 | This paper |
| LBlock* | Full(32) | $2^{78.74}$ | $2^{12}$ | $2^4$ | 5 | This paper |
| TWINE-80 | Full(36) | $2^{79.10}$ | $2^{60}$ | $2^8$ | 8 | [16] |
| | Full(36) | $2^{78.73}$ | $2^{12}$ | $2^4$ | 5 | This paper |

* With modified key schedule.

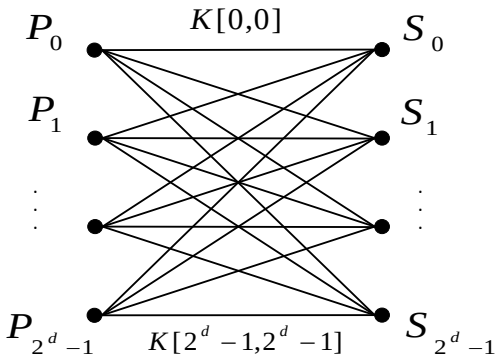



**Figure 1**. $d$-dimensional biclique in plaintext side

Step 2. Compute $P_i$ as $P_i \xleftarrow[0,l-1]{K[i,0]} S_0$ for all $i \in \{1,\ldots,2^d-1\}$.

Step 3. Compute $S_j$ as $P_0 \xrightarrow[0,l-1]{K[0,j]} S_j$ for all $j \in \{1,\ldots,2^d-1\}$.

It can be shown that (1) is satisfied for the 3-tuple $[\{P_i\},\{S_j\},\{K[i,j]\}]$, if the related key differential characteristic of $\Delta_j^K$ in forward direction does not share any active nonlinear component with the related key differential characteristic of $\nabla_i^K$ in backward direction within rounds 0 to $l-1$.

**Partial matching with early abort technique.** Partial matching with precomputation and recomputation is the procedure in which all the keys in a group are tested in an efficient way [19]. In the cases that biclique is constructed at the plaintext side, partial matching is performed at the ciphertext side.

In conventional biclique attack, one intermediate variable, V, is selected in an appropriate position between round l and the last round. In improved version, enjoying the early abort technique, we choose two smaller intermediate variables, namely $V^{(1)}$ and $V^{(2)}$. In forward direction, we partially encrypt $S_j$ under key $K[0,j]$ to derive the first matching variable in forward direction ($\overrightarrow{V_{0,j}^{(1)}}$), and also save all the intermediate states associated to this computations. Similarly, in backward direction, we partially decrypt $C_i$ under key $K[i,0]$ to derive the first matching variables in backward direction ($\overleftarrow{V_{i,0}^{(1)}}$), and again save all the intermediate states associated to this computation.

Now suppose that we want to check $K[i,j]$. In forward direction, for finding $\overrightarrow{V_{i,j}^{(1)}}$ by encrypting $S_j$ under key $K[i,j]$, $i \neq 0$, we only need to recompute those bytes that are influenced by $K^b$ when $i$ changes and $\overrightarrow{V_{i,j}^{(1)}}$ depends on, while the other bytes are not recomputed. Similarly, in backward direction, for finding $\overleftarrow{V_{i,j}^{(1)}}$ by decrypting $C_i$ under key $K[i,j]$, $j \neq 0$, we only need to recompute bytes that are influenced by $K^f$ when $j$ changes and $\overleftarrow{V_{i,j}^{(1)}}$ depends on. If $\overrightarrow{V_{i,j}^{(1)}} \neq \overleftarrow{V_{i,j}^{(1)}}$, key $K[i,j]$ is rejected, otherwise we continue as follows. We continue encrypting and recompute those parts that $\overrightarrow{V_{i,j}^{(2)}}$ depends on, in forward direction. Also, we continue decrypting and recompute those parts that $\overleftarrow{V_{i,j}^{(2)}}$ depends on, in backward direction. Now, if $\overrightarrow{V_{i,j}^{(2)}} = \overleftarrow{V_{i,j}^{(2)}}$ key $K[i,j]$ is stored as a right candidate key. The memory required for the attack is bounded to $2^d$ intermediate states of the encryption algorithm.

**Rechecking the candidate keys.** Finally, we test the candidate keys by a valid $(P,C)$ pair to filter out all the wrong keys and find the correct key.

The total scheme of the improved biclique cryptanalysis of a block cipher is shown in Figure 2. Dashed line in the matching part represent the second matching procedure (using $V_{i,j}^{(2)}$) while the bold line are the first matching filtering (using $V_{i,j}^{(1)}$).

The efficiency of early abort technique does not depend on the key schedule algorithm in any case. So, it can generally improve all the biclique attacks no matter what the key schedule is, though this attack is more efficient on those which have lower dimension (e.g. four), and have the matching variable that can

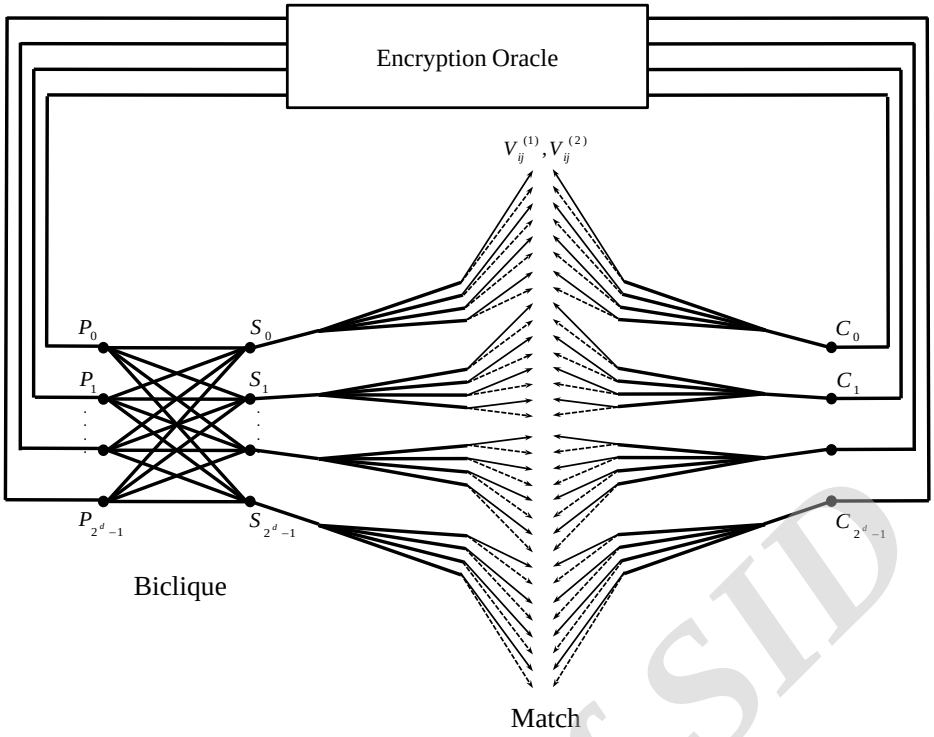



**Figure 2**. Improved biclique cryptanalysis

be divided into two separate parts which depend on separate intermediate variables, each. The improvement gained by early abort technique can be used in two directions. In first approach, it can directly reduce the computational complexity of the attack with no improvement in data complexity. In the second approach it can be used to extend the matching rounds and consequently reduce the biclique length which can be taken as an opportunity to reduce the data complexity.

In this paper we choose the second approach for cryptanalysis of LBlock [9], LBlock with modified key schedule [15], and TWINE-80 [17], inspiring by the algorithm proposed for low data complexity biclique attack in [22], we found the two differentials in a way that the resulted attack has extremely less data complexity than the existing ones whilst the computational complexity is also improved slightly.

## 3 Brief Description of LBlock and TWINE

### 3.1 LBlock and the Modified Key Schedule Version

**Notations.** These are the notations used in this paper.
$K$: Master key.
$K_i$: Subkey of round $i$.
$k_i$: $i^{th}$ bit of master key $K$ counting from right.
$\lll n$: $n$-bit left rotation.
$X_i^L$, $X_i^R$: Left and right half of the state of round $i$ containing 8 nibbles each.

**Specifications.** LBlock is a 64-bit lightweight block cipher with a 80-bit key. It has a Fiestel structure and 32 rounds (Figure 3). The workflow of LBlock is as follows.

LBlock Algorithm

(1) $X_0^L||X_0^R = \text{Input}$
(2) For $i = 0$ to 31
$X_{i+1}^L = (X_i^R \lll 8) \oplus Permutation(Sboxes(X_i^L \oplus K_i))$
$X_{(i+1)}^R = X_i^L$
(3) $\text{Output} = X_{32}^L||X_{32}^R$

where *Permutation* layer is a byte-wise permutation and *Sboxes* layer containing 8 different $4 \times 4$ Sboxes. So far, LBlock security has been analyzed extensively [9–14], most of which are applied on reduced variant of the cipher. In [15] the designers of LBlock presented the first biclique attack on this algorithm and designed a modified key schedule to overcome their new discovered shortcomings in the original design.

**Key schedule.** The key schedule of LBlock composed of a 29-bit left rotation, applying two Sboxes, and adding round number for each round. In modified version, designers use a 24-bit left rotation as well as two XORs to increase the key schedule diffusion.

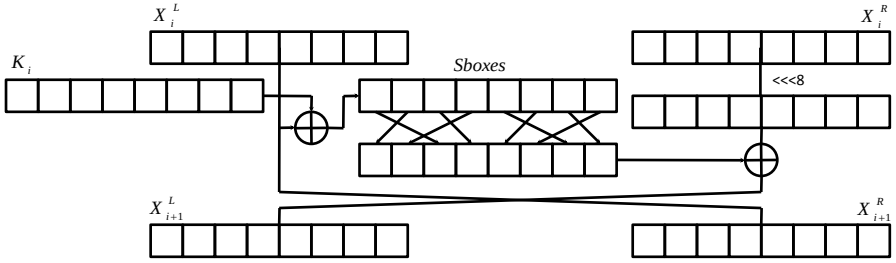



**Figure 3**. One round encryption of LBlock

The key schedule and modified key schedule of LBlock is as follows.

- Key schedule:
  (1) $K \lll 29$
  (2) $[k_{79}k_{78}k_{77}k_{76}] = s9[k_{79}k_{78}k_{77}k_{76}]$
  (3) $[k_{75}k_{74}k_{73}k_{72}] = s8[k_{75}k_{74}k_{73}k_{72}]$
  (4) $[k_{50}k_{49}k_{48}k_{47}k_{46}] = [k_{50}k_{49}k_{48}k_{47}k_{46}] \oplus [i]_2$
  (5) Output the leftmost 32 bits of current content of register $K$ as round subkey $K_{i+1}$

- Modified key schedule:
  (1) $K \lll 24$
  (2) $[k_{55}k_{54}k_{53}k_{52}] = s9[k_{79}k_{78}k_{77}k_{76}] \oplus [k_{55}k_{54}k_{53}k_{52}]$
  (3) $[k_{31}k_{30}k_{29}k_{28}] = s8[k_{75}k_{74}k_{73}k_{72}] \oplus [k_{31}k_{30}k_{29}k_{28}]$
  (4) $[k_{67}k_{66}k_{65}k_{64}] = [k_{71}k_{70}k_{69}k_{68}] \oplus [k_{67}k_{66}k_{65}k_{64}]$
  (5) $[k_{51}k_{50}k_{49}k_{48}] = [k_{11}k_{10}k_9k_8] \oplus [k_{51}k_{50}k_{49}k_{48}]$
  (6) $[k_{54}k_{53}k_{52}k_{51}k_{50}] = [k_{54}k_{53}k_{52}k_{51}k_{50}] \oplus [i]_2$
  (7) Output the leftmost 32 bits of the register $K$ as round subkey $K_{i+1}$

For more details, refer to [9].

### 3.2 TWINE-80

**Notations.** These are the notations used in this paper.
$K$: Master key.
$K[i]$: $i^{th}$ nibble of the master key $K$.
$K[i, j, ..., k]$: Concatenation of nibbles $i$,$j$,...,$k$ of the master key $K$.
$RK^i$: $i^{th}$ round key which is equal to $RK_0^i||RK_1^i||...||RK_7^i$.
$RK_j^i$: $j^{th}$ nibble of $i^{th}$ 32-bit subkey counting from left ($RK^i = RK_0^i||RK_1^i||...||RK_7^i$).
$\lll n$: $n$-bit left rotation.

**Specifications.** TWINE is a 64-bit lightweight block cipher with generalized feistel structure. It has two versions TWINE-80 and 128 working with 80- and 128-bit key length, respectively. The only difference of these two versions is in the key schedule algorithms. It has 36 rounds, each consists of eight F-functions and one permutation. F-function is composed of a key addition layer, followed by a sbox layer (Figure 5).

Figure 4 shows one round encryption of TWINE.

**Key schedule.** The Key schedule of TWINE-80 is as follows.

- Key schedule of TWINE-80.
  (1) $RK^0 = K[1, 3, 4, 6, 13, 14, 15, 16]$
  (2) for $i = 1$ to 35
  $K[1] = K[1] \oplus S(K[0])$
  $K[4] = K[4] \oplus S(K[16])$
  $K[7] = K[7] \oplus (0||CON_H^i)$
  $K[19] = K[19] \oplus (0||CON_L^i)$
  $K[0, 1, 2, 3] = K[0, 1, 2, 3] \lll 4$
  $K = K \lll 16$
  $RK^i = K[1, 3, 4, 6, 13, 14, 15, 16]$

$CON^i = CON_H^i||CON_L^i$ is the $i^{th}$ round constant. Our attacks are independent of Sboxes lookup tables and constant values. The interested readers can refer to [17] for more details.

## 4 Improved Biclique Cryptanalysis of LBlock

### 4.1 Attack on LBlock

**Attack specifications.** Let $K^f = k_{25}k_{24}k_{23}k_{22}$ and $K^b = k_9k_8k_7k_6$. As it can be seen in Figure A.1 of Appendix A, $\Delta_j^K$ and $\nabla_i^K$ differentials have not any shared active bits in key schedule, and so the differential effect of each can be computed independently.

Now we construct a 5-round 4-dimensional biclique for rounds 0 to 4. Thus, the intermediate state $S$ refers to the output state of round 4. As it can be seen in Figure 6, the differential characteristic of $\Delta_j^K$ difference of master key in forward direction does not share any active Sboxes with the differential characteristic of $\nabla_i^K$ difference of master key in backward direction within the first five rounds. So the biclique could be constructed here.

The $8^{th}$ nibble of $X_{18}^R$ is chosen as the first matching

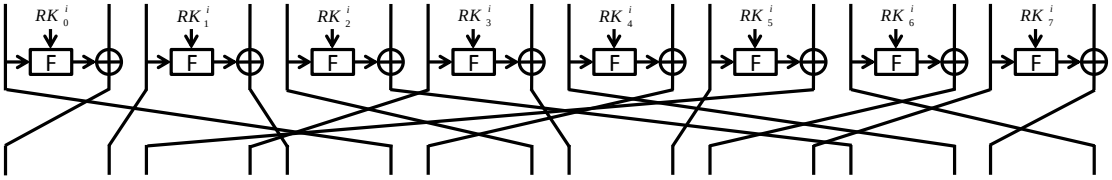



**Figure 4**. One round encryption of TWINE

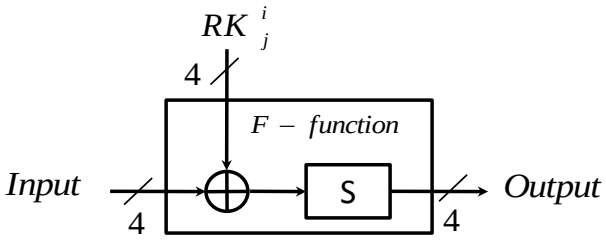



**Figure 5**. TWINE F-Function

variable $V_{i,j}^{(1)}$, and the $3^{th}$ nibble of $X_{18}^{R}$ is chosen as the second matching variable $V_{i,j}^{(2)}$.

### Complexities

**Data complexity.** Figure 6 shows that there are three active nibbles in the plaintext for each biclique. So the data complexity of this attack is bounded by $2^{12}$.

**Computational complexity.** We only consider the number of Sbox computations as the component with dominate computational complexity in LBlock and ignore the other linear components. LBlock have $32 \times 8 = 256$ Sboxes for encryption and $2 \times 31 = 62$ Sboxes for key schedule. A single 32-round encryption of LBlock is regarded as the unit of computation which is equivalent to 256+62=318 Sbox computations.

As we can see in Figure A.1, there are 9 active Sboxes for $\nabla_i^K$ and 6 active Sboxes for $\Delta_j^K$ in the key schedule, and also they do not shared any active Sboxes. So, the normalized computational complexity of key schedules in a group of keys is:

$$C_{keyschedule} = \frac{62 + 9 \times (2^4 - 1) + 6 \times (2^4 - 1)}{318} = 2^{-0.14} \quad (2)$$

To compute $S_j$ in a biclique, 30 Sboxes should be calculated once (the light gray nibbles) and 10 Sboxes should be calculated $2^4$ times (the dark gray nibbles) (see Figure 6, left). Also, for computing $P_i$, we have to recompute 3 Sboxes $2^4 - 1$ times (see Figure 6, right). So, the normalized computational complexity of the biclique constructing is:

$$C_{biclique} = \frac{30 + 10 \times 2^4 + 3 \times (2^4 - 1)}{318} = 2^{-0.44} \quad (3)$$

In forward direction of partial matching (rounds 5 to 17) for each $S_j$, 20 Sboxes should be calculated once and 47 Sboxes should be calculated $2^4$ times to obtaining the first matching variable ($\overrightarrow{V_{i,j}^{(1)}}$). (see Figure 7, left; The computation of the nibbles in white is not required). Also, in backward direction (rounds 31 to 18) for each $C_i$, 29 Sboxes should be calculated once and 54 Sboxes should be calculated $2^4$ times to obtain the first matching variable ($\overleftarrow{V_{i,j}^{(1)}}$) (see Figure 7, right). If $\overrightarrow{V_{i,j}^{(1)}} = \overleftarrow{V_{i,j}^{(1)}}$, we have to obtain $\overrightarrow{V_{i,j}^{(2)}}$ and $\overleftarrow{V_{i,j}^{(2)}}$, which need to calculate 5 Sboxes in forward direction and 9 Sboxes in backward direction (the gridded nibbles), respectively. The probability of the correctness of $\overrightarrow{V_{i,j}^{(1)}} = \overleftarrow{V_{i,j}^{(1)}}$ is equal to $2^{-4}$ for each wrong key guess, so for each group of keys, we need to calculate these additional Sboxes $2^4$ times. Hence, the computational complexity for checking all the keys in a group normalized to a full-round encryption of LBlock is:

$$C_{forward} = \frac{2^4 \times (20 + 47 \times 2^4) + 5 \times 2^4}{318} = 2^{5.29} \quad (4)$$

$$C_{backward} = \frac{2^4(29 + 54 \times 2^4) + 9 \times 2^4}{318} = 2^{5.50} \quad (5)$$

$$C_{match} = C_{forward} + C_{backward} = 2^{6.4} \quad (6)$$

By using the two 4-bit matching variables, the probability of accepting a wrong key is $2^{-8}$. Also, we check $2^8$ keys in each group. So, the computational complexity of rechecking false keys is:

$$C_{recheck} = 2^8 \times 2^{-8} = 1 \quad (7)$$

Since all steps are executed for each group, the total computational complexity of the attack is:

$$C_{total} = 2^{72} \times (C_{keyschedule} + C_{biclique} + C_{match} + C_{recheck}) = 2^{72} \times (2^{-0.14} + 2^{-0.44} + 2^{6.4} + 1) = 2^{78.4} \quad (8)$$

The computational complexity of the attack is summarized in Table 2.

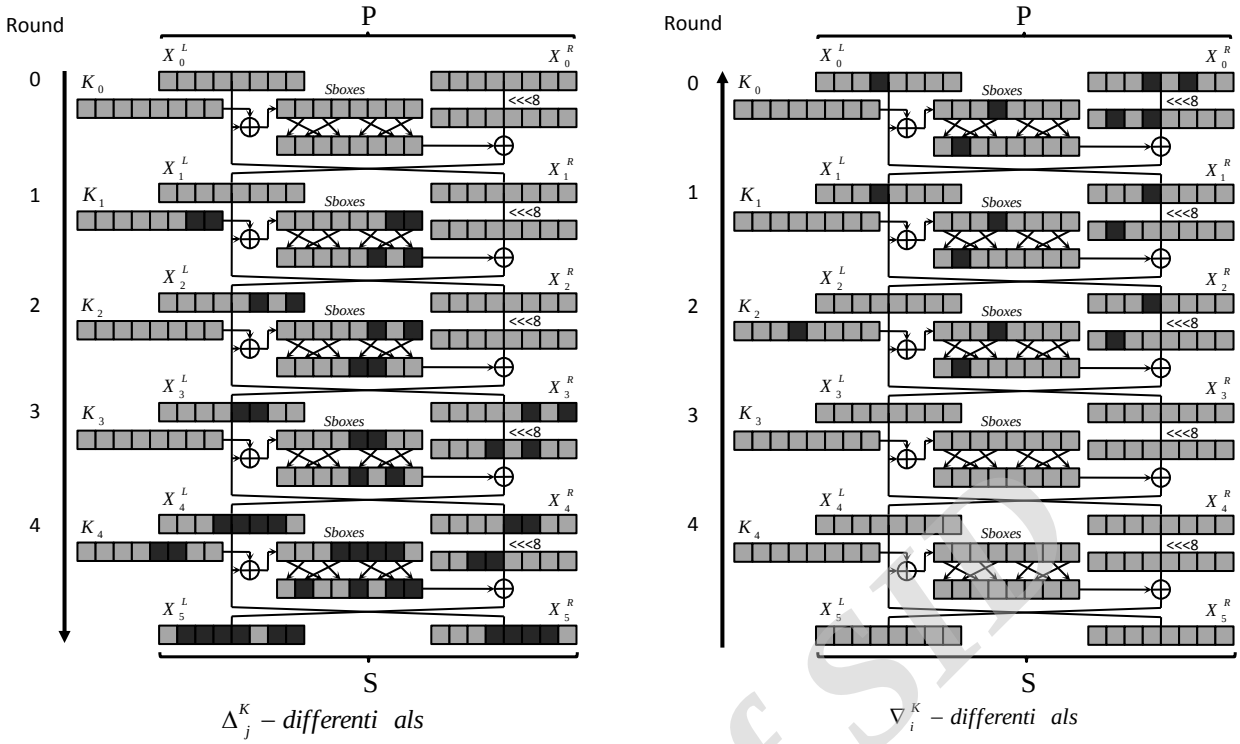



**Figure 6**. 4-Dimensional 5-round biclique for LBlock

**Table 2**. Computational complexity of attack on LBlock

| Attack step | | Number of computations | | | | Total |
|---|---|---|---|---|---|---|
| | | 1 | $2^4$ | $2^8$ | $2^4$ (Early abort) | (normalized to 318) |
| Key schedule | | 47 F | 15 F | - | - | $2^{-0.14}$ |
| Biclique | Forward | 27 F | 10 F | - | - | $2^{-0.44}$ |
| | Backward | - | 3 F | - | - | |
| Matching | Forward | - | 20 F | 47 F | 5 F | $2^{6.4}$ |
| | Backward | - | 29 F | 54 F | 9 F | |
| Recheck | | $2^8 \times 2^{-8} = 1$ Encryption | | | | |
| Total | | $2^{72} \times (2^{-0.14} + 2^{-0.44} + 2^{6.4} + 1) = 2^{78.4}$ | | | | |

### 4.2 Attack on LBlock with Modified Key Schedule

**Attack specifications.** In this case we use the weakness of diffusion of the modified key schedule in backward direction. Consider $K'$ is the key state in the last round and the left most 32 bits of the $K'$ is used for last round subkey. Let $K'^f = k'_{31}k'_{30}k'_{29}k'_{28}$ and $K'^b = k'_{35}k'_{34}k'_{33}k'_{32}$. As it can be seen in Figure A.2 of Appendix A, $\Delta_i^{K'}$ and $\nabla_j^{K'}$ differentials have shared just 10 active Sboxes in the key schedule, and the effect of the diffusion of the key differentials on the remaining parts could be computed independently.

A 5-round 4-dimensional biclique is constructed at the ciphertext side (Figure 8). The $8^{th}$ nibble of the $X_{10}^R$ is chosen as the first matching variable $V_{i,j}^{(1)}$ and the $3^{th}$ nibble of the $X_{10}^R$ is chosen as the second matching variable $V_{i,j}^{(2)}$.

**Complexities**

Figure 8 shows that there are three active nibbles in ciphertext for each biclique. So the data complexity of this attack is bounded by $2^{12}$. The computational complexity of the attack is $2^{78.74}$. The details of the

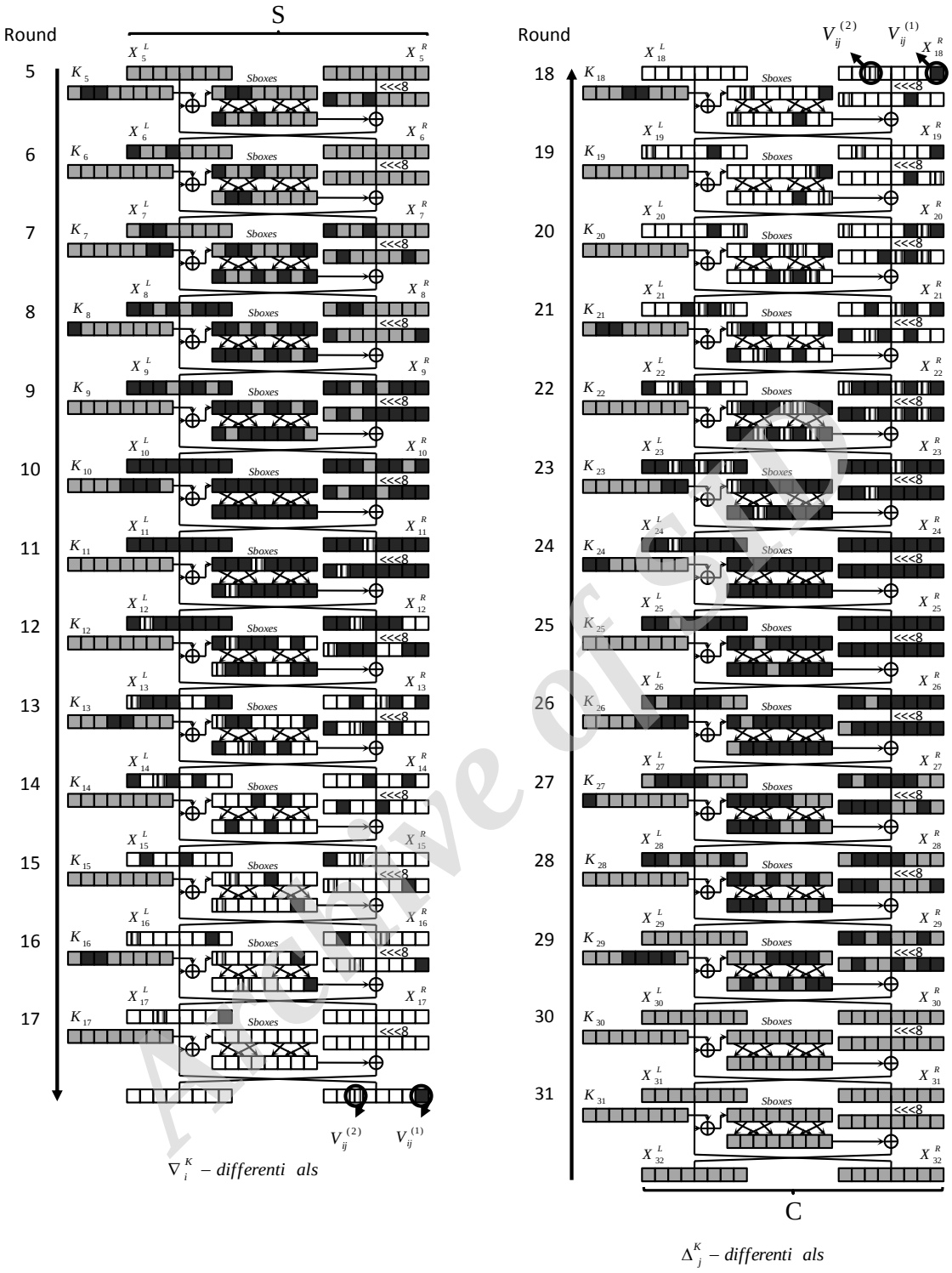



**Figure 7**. Partial matching for LBlock

computational complexity is mentioned in Table 3. Also, Figure 9 shows the matching part.

### 4.3 Our Proposed Key Schedule for LBlock

As it was shown in Section 4.2, although the diffusion of the modified key schedule in forward direction is improved very much, its diffusion in backward direction

**Table 3**. Computational complexity of attack on LBlock with Modified Key Schedule

| Attack step | | Number of computations | | | | Total |
|---|---|---|---|---|---|---|
| | | 1 | $2^4$ | $2^8$ | $2^4$ (Early abort) | (normalized to 318) |
| Key schedule | | 28 F | 24 F | 10 F | - | $2^{3.32}$ |
| Biclique | Forward | - | 3 F | - | - | $2^{-1.13}$ |
| | Backward | 33 F | 4 F | - | - | |
| Matching | Forward | - | 1 F | 42 F | 5 F | $2^{6.59}$ |
| | Backward | - | 32 F | 75 F | 9 F | |
| Recheck | | $2^8 \times 2^{-8} = 1$ Encryption | | | | |
| Total | | $2^{72} \times (2^{3.32} + 2^{-1.13} + 2^{6.59} + 1) = 2^{78.74}$ | | | | |

**Table 4**. Computational comlexity of attack on TWINE-80

| Attack step | | Number of computations | | | | Total |
|---|---|---|---|---|---|---|
| | | 1 | $2^4$ | $2^8$ | $2^4$ (Early abort) | (normalized to 358) |
| Key schedule | | 53 F | 17 F | - | - | $2^{-0.14}$ |
| Biclique | Forward | - | 3 F | - | - | $2^{-0.70}$ |
| | Backward | 28 F | 9 F | - | - | |
| Matching | Forward | - | 10 F | 49 F | 7 F | $2^{6.70}$ |
| | Backward | - | 30 F | 93 F | 8 F | |
| Recheck | | $2^8 \times 2^{-8} = 1$ Encryption | | | | |
| Total | | $2^{72} \times (2^{-0.14} + 2^{-0.70} + 2^{6.70} + 1) = 2^{78.73}$ | | | | |

is still limited, hence it is vulnerable to the biclique attack with matching part in the plaintext side. Since this weakness arises from the fact that the diffusion of the key schedule algorithm is not symmetric in the two directions, a key schedule with symmetric diffusion can strengthen LBlock against biclique attack. We propose a new key schedule that satisfies the above mentioned requirement. The proposed key schedule is as follows.

(1) $K \lll 12$
(2) $[k_{21}k_{20}k_{19}k_{18}] = s8[k_{75}k_{74}k_{73}k_{72}] \oplus [k_{21}k_{20}k_{19}k_{18}]$
(3) $[k_{53}k_{52}k_{51}k_{50}] = s9[k_{79}k_{78}k_{77}k_{76}] \oplus [k_{53}k_{52}k_{51}k_{50}]$
(4) $[k_{69}k_{68}k_{67}k_{66}] = [k_{45}k_{44}k_{43}k_{42}] \oplus [k_{69}k_{68}k_{67}k_{66}]$
(5) $[k_5k_4k_3k_2] = [k_{29}k_{28}k_{27}k_{26}] \oplus [k_5k_4k_3k_2]$
(6) $[k_{54}k_{53}k_{52}k_{51}k_{50}] = [k_{54}k_{53}k_{52}k_{51}k_{50}] \oplus [i]_2$
(7) $K \lll 12$
(8) Output the leftmost 32 bits of the register K as round subkey $K_{i+1}$

In fact, the idea behind using two cyclic shifts at the beginning and the end of the key schedule (steps 1 and 7) was to construct a symmetric key schedule in the diffusion viewpoint. The steps 2 and 4 create a good diffusion in forward direction, and the steps 1 and 3 should do the same in backward direction. The Sboxes are selected in the way that, if each of them is activated in one round, it activates two nibbles in the next round. This property was not the case with the original and key schedule of the LBlock. As simulations shows, any active bits of each round key in this algorithm, quickly diffuses in all the nibbles of the other round keys, both in forward and backward direction, after at most 16 rounds.

## 5 Improved Biclique Cryptanalysis of TWINE-80

**Attack specifications.** Using the weakness of diffusion of key schedule in backward direction is the main idea of our attack. Consider $K'$ as the key state in the last round. Let $K'^f = k'_{23}k'_{22}k'_{21}k'_{20}$ and $K'^b = k'_7k'_6k'_5k'_4$. As it can be seen in Figure A.3 of Appendix A, $\Delta_i^{K'}$ and $\nabla_j^{K'}$ differentials have not shared any active Sboxes in the key schedule, and could be computed, separately.

We could construct a 5-round 4-dimensional biclique at the ciphertext side (Figure 10). The first and second nibbles of the internal state in the input of $11^{th}$ round is chosen as the first and second matching variable $V_{i,j}^{(1)}$ and $V_{i,j}^{(2)}$, respectively.

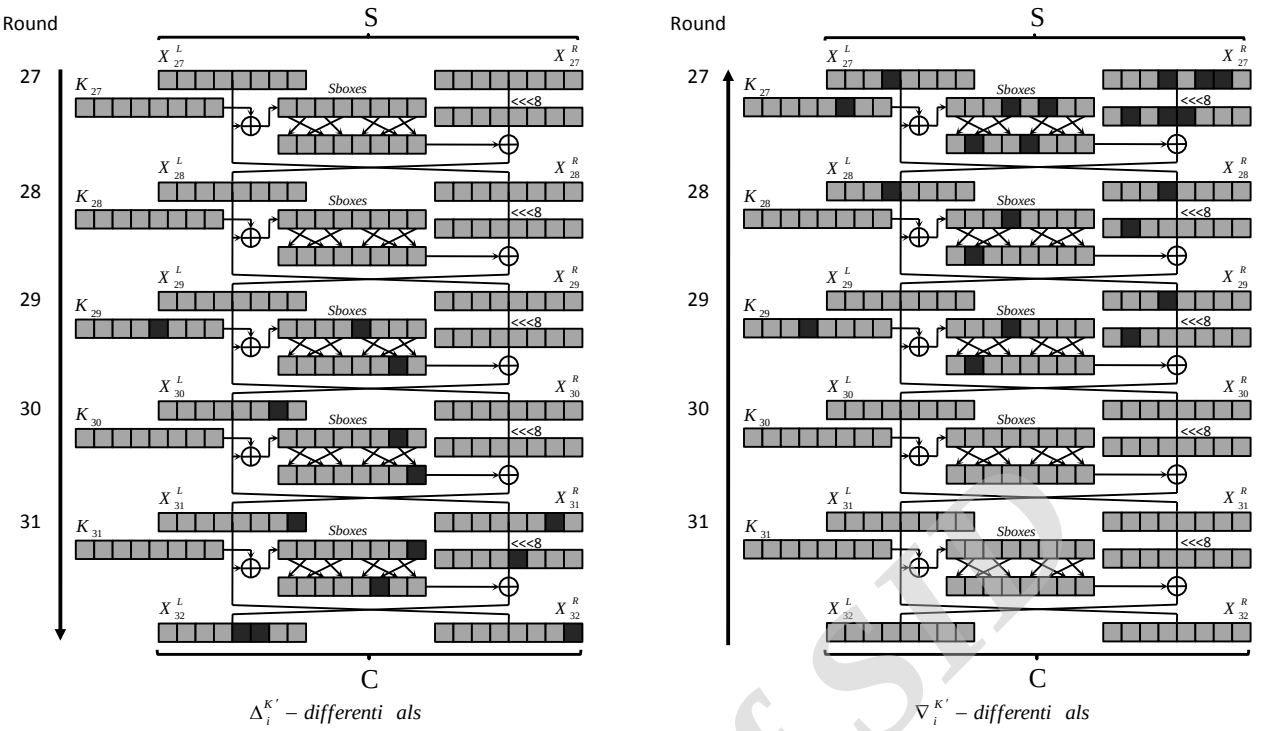



**Figure 8**. 4-Dimensional 5-round biclique for LBlock with modified key schedule

### Complexities

Figure 10 shows that there are three active nibbles in ciphertext for each biclique. So the data complexity of this attack is bounded by $2^{12}$. The computational complexity of the attack is $2^{78.73}$. The details of the computational complexity is mentioned in Table 4. Also, Figure 11 shows the matching part.

## 6 Conclusion

We found out that early abort technique, used in impossible differential attack, can slightly improve the efficiency of the matching part. Instead of this limited improvement in computations, we took this opportunity to increase the length of the matching part, and consequently shorten the biclique part. This shorter biclique potentially requires a limited amount of data complexity.

We applied this method on LBlock, and TWINE-80 lightweight block ciphers. In the case of LBlock, a modified key schedule was proposed by designers to enforce it against the biclique attack. We analyzed both the original LBlock and LBlock with modified key schedule. In all the attacks, the data complexity is $2^{12}$. The computational complexity of all the attacks are also slightly better than those in the existing attacks. According to high computational complexities, it should be mentioned that these attacks are not serious threats for the practical security of the ciphers.

## 7 Acknowledgement

This work was partially supported by Iranian National Science Foundation (INSF) under contract no. 96/53979 and INSF cryptography chair and by the Office of Vice-President for the Science and Technology, I. R. Iran.

## References

[1] Ahmadi, Siavash, *et al.* "Biclique cryptanalysis of LBlock with modified key schedule." Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on. IEEE, (2015)

[2] Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita T., and Shirai, T.: Piccolo: An Ultra-Lightweight Blockcipher, CHES 2011, LNCS 6917, pp. 342-357, Springer, Heidelberg, (2011)

[3] Bogdanov, A., Knudsen, L., 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. 450466. Springer, Heidelberg (2007)

[4] Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326341.

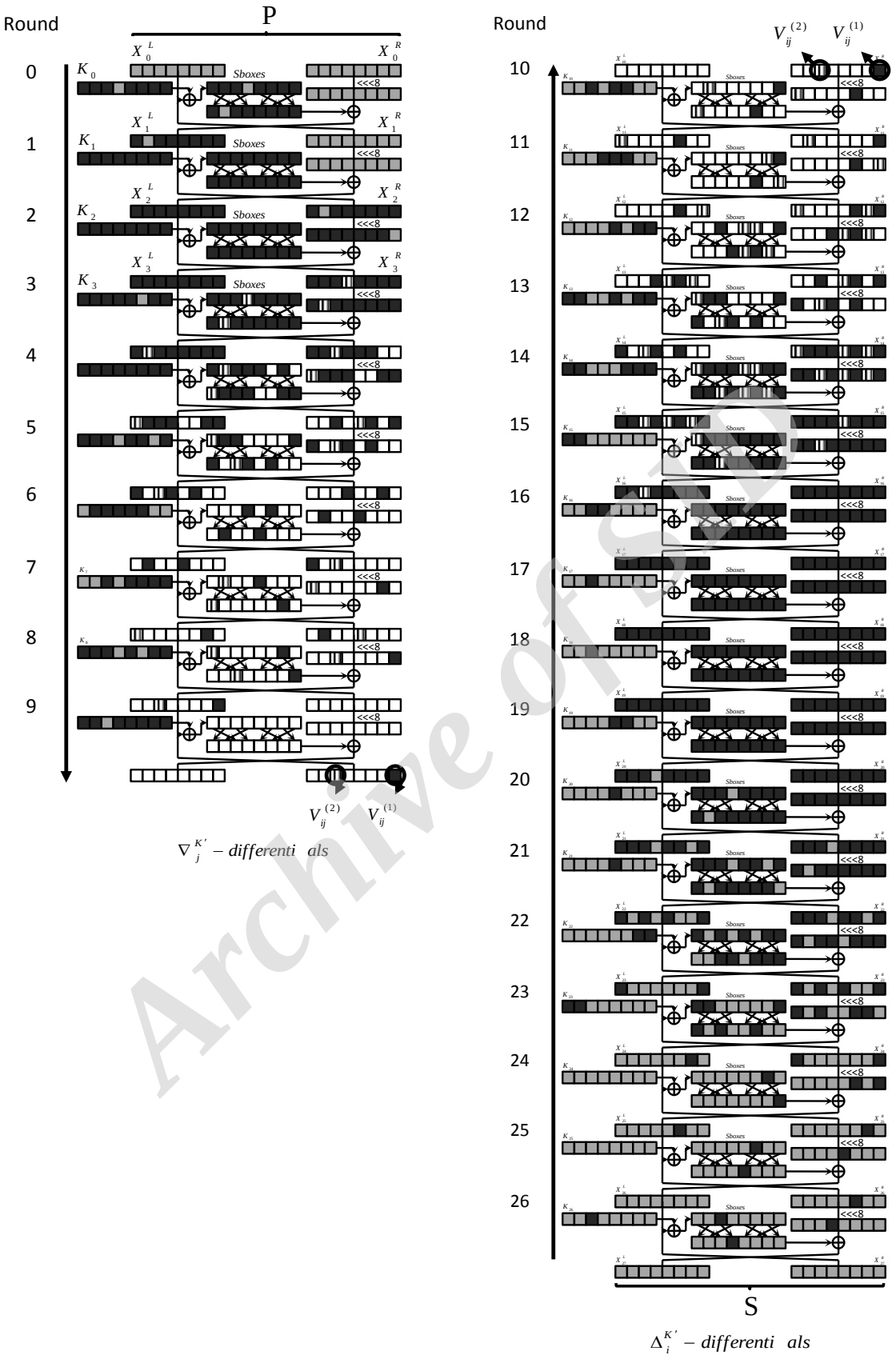



**Figure 9**. Partial matching for LBlock with modified key schedule

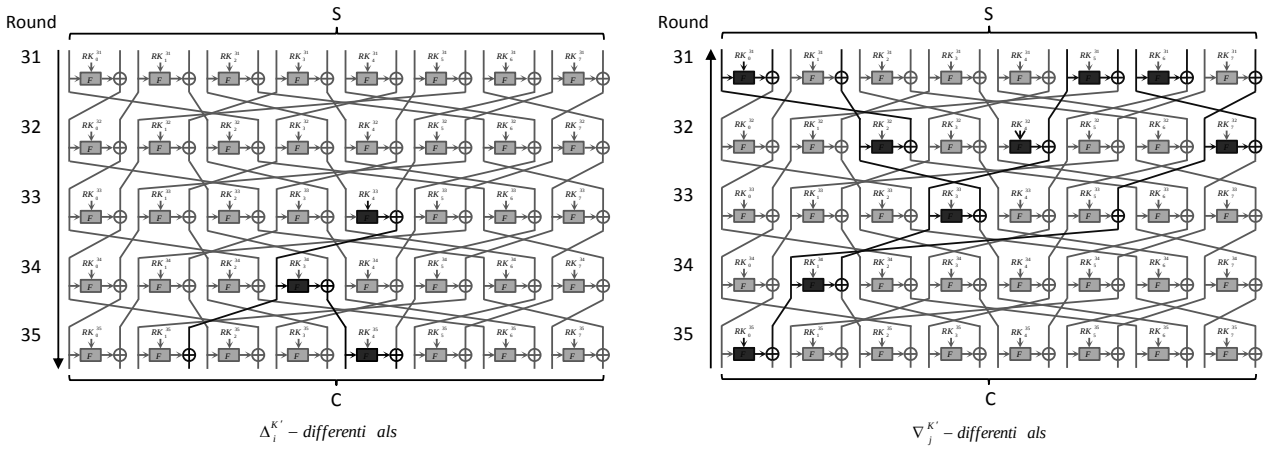



**Figure 10**. 4-Dimensional 5-round biclique for TWINE-80

Springer, Heidelberg (2011)
[5] Gong, Z., Nikova, S., Law, Y.W.: KLEIN: A New Family of Lightweight Block Ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 118. Springer, Heidelberg (2012)
[6] Aumasson, J.P., Henzen, L., Meier, W., Naya-Plasencia, M.: Quark: A lightweight hash. In: Mangard and Standaert F.X. (eds.): CHES 2010, LNCS, vol. 6225, pp. 115 Springer, Heidelberg (2010)
[7] Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In Phillip Rogaway (ed.): CRYPTO 2011, LNCS, vol.6841, pp. 222-239. Springer, Heidelberg (2011)
[8] Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., Verbauwhede, I.: SPONGENT: A lightweight hash function. In Bart Preneel and Tsuyoshi Takagi (eds.): CHES 2011, LNCS, vol.6917, pp. 312-325. Springer, Heidelberg (2011)
[9] Wu, W., Zhang, L.: LBlock: A lighweight block cipher in: Lopez, J., Tsudik, G. (Eds.), ACNS, in: Lecture Notes in Computer Science, vol. 6715, pp. 327-344, (2011)
[10] Li, Y.: Integral Cryptanalysis on Block Ciphers (in Chinese): [D]. Beijing: Institue of Software, Chinese Academy of Sciences, (2012)
[11] Liu, Y., Gu, D., Liu, Z., Li, W.: Impossible differential attacks on reduced-round lblock. In Ryan, M., Smytg, B, and Wang, G., editors, Information Security Practice and Experience, volume 7232 of Lecture Notes in Computer Science, Pages 97-108. Springer Berlin / Heidelberg, (2012)
[12] Soleimany H., Nyberg K.: Zero-Correlation Linear Cryptanalysis of Reduced-Round LBlock, In proceeding of Workshop on Coding and Cryptography, WCC'13, (2013)
[13] Emami, S., McDonald, C., Pieprzyk, J., Steinfeld, R.: Truncated Differential Analysis of Reduced-Round LBlock. In Cryptology and Network Security (pp. 291-308). Springer International Publishing (2013)
[14] Bogdanov, A., Boura, C., Rijmen, V., Wang, M., Wen, L., Zhao, J.: Key Difference Invariant Bias in Block Ciphers. In Advances in Cryptology-ASIACRYPT 2013 (pp. 357-376). Springer Berlin Heidelberg (2013)
[15] Wang, Y., Wu, W., Yu, X., Zhang, L.: Security on LBlock against Biclique Cryptanalysis, WISA 2012, LNCS 7690, pp 1-14, Springer, Heidelberg, (2012)
[16] Karakoc, F., Demirci, H., Harmanci, A.E.: Biclique cryptanalysis of LBlock and TWINE, Information Processing Letters, Volume 113, Issue 12, pp. 423429, (2013)
[17] Suzaki, T., Minematsu, K., Morioka, S. and Kobayashi, E.: TWINE : A Lightweight Block Cipher for Multiple Platforms. SAC 2012, LNCS, vol. 7707, pp. 339-354, Springer-Verlag (2012)
[18] Najarkolaei, S. R. H., Ahangarkolaei, M. Z., Ahmadi, S., and Aref, M. R.: Biclique cryptanalysis of Twine-128. In Information Security and Cryptology (ISCISC), 2016 13th International Iranian Society of Cryptology Conference on (pp. 46-51). IEEE (2016)
[19] Bogdanov, A., Khovratovich, D., Rechberger, C.: Biclique Cryptanalysis of the Full AES, ASIACRYPT 2011, LNCS, vol. 7073, pp. 344-371. Springer, Heidelberg (2011)
[20] Abed, F., Forler, C., List, E., Lucks, S., Wenzel, J., A Framework for Automated Biclique Cryptanalysis of Block Ciphers, FSE 2013, (2013)
[21] Ahmadian, Z., Salmasizadeh, M., Aref, M.R.: Biclique Cryptanalysis of the Full-round KLEIN Block Cipher, Cryptology ePrint Archive, Report 2013/097 (2013)

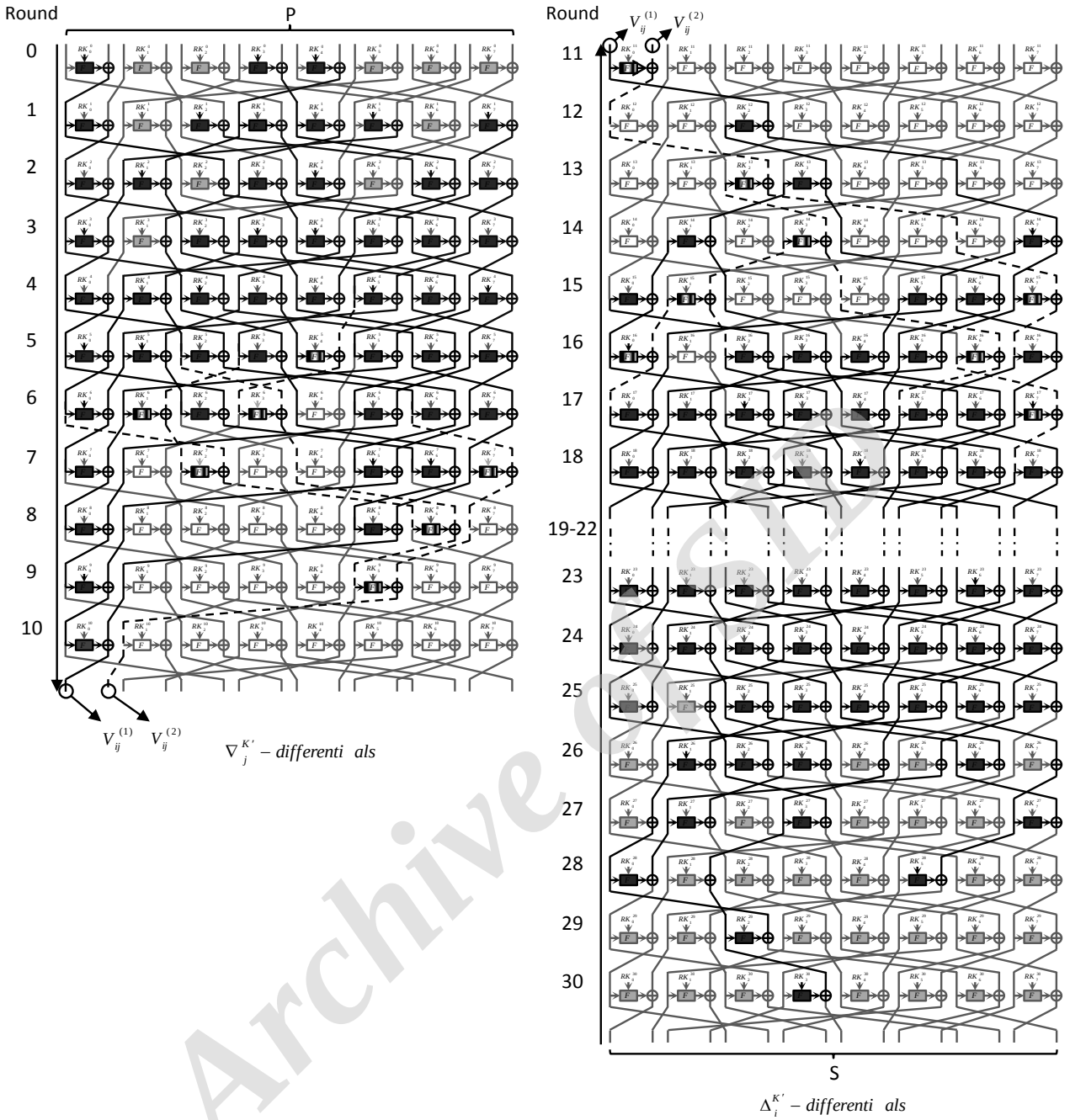



**Figure 11**. Partial matching for TWINE-80

[22] Ahmadi, S., Ahmadian, Z., Mohajeri, J., and Aref, M.R.:Low Data Complexity Biclique Cryptanalysis of Block Ciphers with Application to Piccolo and HIGHT." IEEE Trans. Information Forensics and Security 9.10 (2014): 1641-1652.

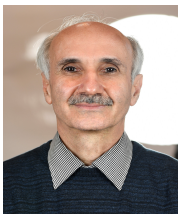
[23] Song, J., Lee, K., and Lee, H.: Biclique cryptanalysis on lightweight block cipher: HIGHT and Piccolo. International Journal of Computer Mathematics, (2013)

[24] Wang, Y., Wu, W., and Yu, X.: Biclique Cryptanalysis of Reduced-Round Piccolo Block Cipher, ISPEC 2012, LNCS 7232, pp. 337-352, Springer, Heidelberg (2012)

[25] Lu, J., Kim, J., Keller, N., Dunkelman, O.: Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1, CT-RSA 2008, LNCS Volume 4964, pp 370-386, (2008)

**Siavash Ahmadi** received the B.S. and M.S. degrees in electrical engineering in 2012 and 2014, respectively, from Sharif University of Technology, Tehran, Iran. He is currently a Ph.D. candidate in electrical engineering (communication systems and security) at Sharif University of Technology. His special fields of interest include cryptology and wireless security, with emphasis on cryptanalysis.

**Zahra Ahmadian** received the B.S. degree in electrical engineering (communications and electronics fields) from the Amirkabir University of Technology, Tehran, Iran, in 2006, and the M.S. degree in electrical engineering (secure communications) and the Ph.D. degree in electrical engineering (communication systems) from the Sharif University of Technology, Tehran, in 2008 and 2014, respectively. Since 2014, she has been with the electrical engineering department, Shahid Beheshti University, Tehran, as an assistant professor. Her special fields of interest include wireless security and cryptology with emphasis on cryptanalysis.



**Javad Mohajeri** is currently an assistant professor with the electronics research institute, Sharif University of Technology, Tehran, Iran, where he is an adjunct assistant professor with the electrical engineering department. He has authored or coauthored of 3 books and 100 research articles in refereed journals/conferences. His current research interests include data security, and design and analysis of cryptographic protocols and algorithms. Mr. Mohajeri is a founding member of the Iranian Society of Cryptology.

**Mohammad Reza Aref** received the B.S. degree in 1975 from the University of Tehran, Iran, and the M.Sc. and Ph.D. degrees in 1976 and 1980, respectively, from Stanford University, Stanford, CA, USA, all in electrical engineering. He returned to Iran in 1980 and was actively engaged in academic affairs. He was a faculty member of Isfahan University of Technology from 1982 to 1995. He has been a professor of electrical engineering at Sharif University of Technology, Tehran, since 1995, and has published more than 290 technical papers in communication and information theory and cryptography in international journals and conferences proceedings. His current research interests include areas of communication theory, information theory, and cryptography.

# Appendix

## A Key Schedules of Algorithms

| Active bits for $\nabla_i^K$: 9-8-7-6 Active bits for $\Delta_j^K$: 25-24-23-22 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| round | Nibble 0 (S) | | | | Nibble 1 (S) | | | | Nibble 2 | | | | Nibble 3 | | | | Nibble 4 | | | | Nibble 5 | | | | Nibble 6 | | | | Nibble 7 | | | |
| 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 |
| 1 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 |
| 2 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 |
| 3 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 |
| 4 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 |
| 5 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 |
| 6 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 |
| 7 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 |
| 9 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 |
| 10 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 |
| 11 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 |
| 12 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 |
| 13 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 |
| 14 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 |
| 15 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 |
| 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 |
| 17 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 |
| 18 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 |
| 19 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 |
| 20 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 |
| 21 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 |
| 22 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 |
| 23 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 |
| 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 |
| 25 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 |
| 26 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 |
| 27 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 |
| 28 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 |
| 29 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 | 28 | 27 | 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 |
| 30 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 79 | 78 | 77 | 76 | 75 | 74 | 73 | 72 | 71 | 70 | 69 | 68 | 67 | 66 | 65 | 64 | 63 | 62 | 61 | 60 | 59 | 58 |
| 31 | 60 | 59 | 58 | 57 | 56 | 55 | 54 | 53 | 52 | 51 | 50 | 49 | 48 | 47 | 46 | 45 | 44 | 43 | 42 | 41 | 40 | 39 | 38 | 37 | 36 | 35 | 34 | 33 | 32 | 31 | 30 | 29 |

**Figure A.1**. Key schedule of LBlock. The bits in dark gray are affected by $\Delta_j^K$ and the bits in light gray are affected by $\nabla_i^K$.

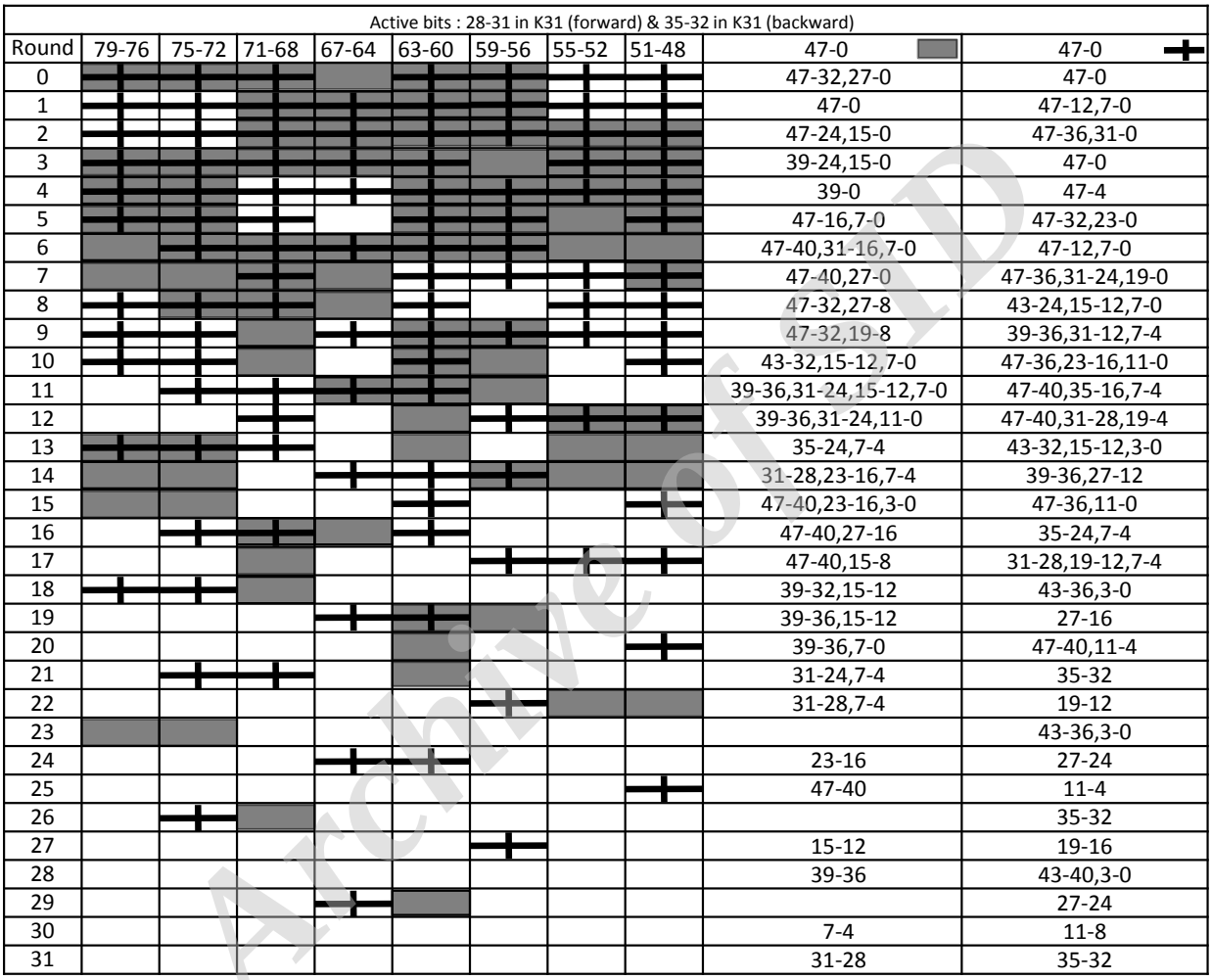



**Figure A.2**. Modified key schedule of LBlock. The bits in gray are affected by $\Delta_i^K$ and the bits marked by "+" are affected by $\nabla_j^K$.

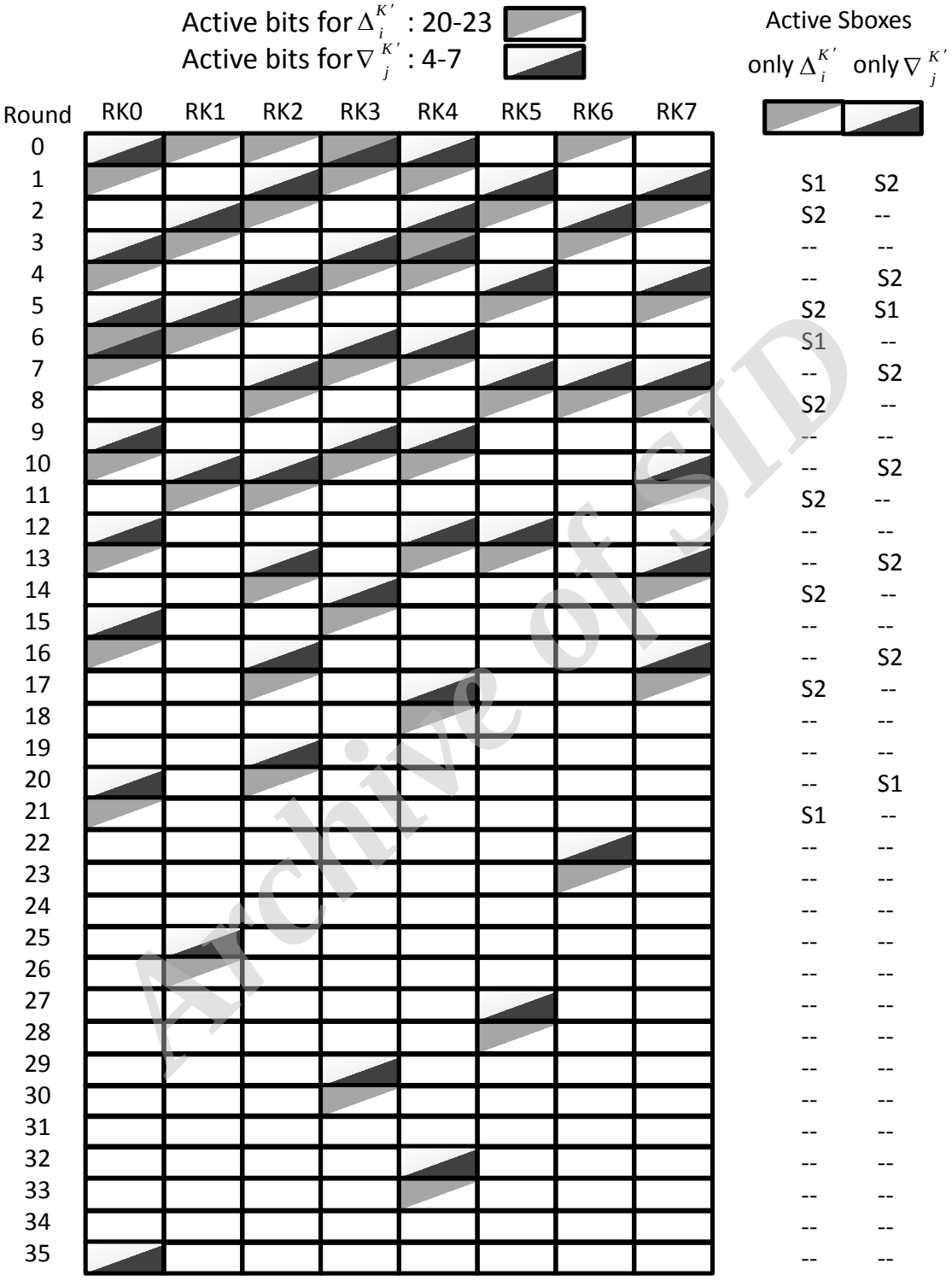



**Figure A.3**. Key schedule of TWINE-80

The ISC Int'l Journal of Information Security
ISeCure

January 2019, Volume 11, Number 1 (p. 91)
http://www.isecure-journal.org

## Persian Abstract

# حمله دو بخشی به رمزهای قالبی LBlock و Twine-80 با پیچیدگی داده عملی

سیاوش احمدی[۱]، زهرا احمدیان[۲]، جواد مهاجری[۱] و محمدرضا عارف[۱]

[۱]دانشگاه صنعتی شریف، تهران، ایران
[۲]دانشگاه شهید بهشتی، تهران، ایران

در حمله دوبخشی، استفاده از دوبخشی کوتاه‌تر معمولا منجر به کاهش پیچیدگی داده می‌شود، اما در عین حال پیچیدگی محاسباتی را افزایش می‌دهد. با استفاده از روش حذف اولیه در قسمت تطبیق جزئی حمله دوبخشی می‌توان این محاسبات را مقداری جزئی کاهش داد. در مقاله حاضر، با استفاده از این روش، اما به جای کاهش جزئی پیچیدگی محاسباتی، مقدار این پیچیدگی را ثابت نگه داشته‌ایم و پیچیدگی داده را به بهره‌گیری از دوبخشی کوچکتر، به میزان قابل توجه کم کرده‌ایم. با این رویکرد، رمز LBlock را در دو حالت معمولی و با فرانمای کلید اصلاح‌شده (که برای مقاومت در برابر حمله دوبخشی طراحی شده است)، هر دو با پیچیدگی داده $2^{12}$ تحلیل کرده‌ایم. در مورد LBlock معمولی، بهترین حمله قبلی دارای پیچیدگی داده $2^{52}$ بوده و در مورد LBlock با فرانمای کلید اصلاح‌شده، تا کنون حمله دور کاملی ارائه نشده بود. اگرچه پراکنش کم الگوریتم رمز LBlock موجب آسیب‌پذیری آن در برابر حمله دوبخشی صرف نظر فرانمای کلید آن می‌شود، اما به منظور تقویت بیشتر LBlock در برابر حمله دوبخشی، فرانمای کلید جدیدی نیز برای آن پیشنهاد کرده‌ایم. ضمنا، با استفاده از این روش، Twine-80 را نیز با پیچیدگی داده $2^{12}$ تحلیل کرده‌ایم. برای Twine-80، کمترین پیچیدگی داده قبلی برابر $2^{60}$ بوده است. در تمامی حملات ارائه شده در این مقاله، پیچیدگی‌های محاسباتی نیز مقداری نسبت به سایر حملات موجود بهبود پیدا کرده‌اند.

**واژه‌های کلیدی:** رمزنگاری سبک، تحلیل دوبخشی، تطبیق جزئی، روش حذف اولیه.