Hindawi
Security and Communication Networks
Volume 2017, Article ID 7589306, 12 pages
https://doi.org/10.1155/2017/7589306

Research Article

Improved Biclique Cryptanalysis of the Lightweight Block Cipher Piccolo

Guoyong Han[1,2] and Wenying Zhang[1]

[1]*School of Information Science and Engineering, Shandong Normal University, Jinan, China*
[2]*School of Management Engineering, Shandong Jianzhu University, Jinan, China*

Correspondence should be addressed to Wenying Zhang; wenyingzh@sohu.com

Received 6 June 2016; Accepted 12 February 2017; Published 2 March 2017

Academic Editor: Nidal Nasser

Biclique cryptanalysis is a typical attack through finding a biclique which is a type of bipartite diagram to reduce the computational complexity. By investigating the subkey distribution and the encryption structure, we find out a weakness in the key schedule of Piccolo-80. A 6-round biclique is constructed for Piccolo-80 and a 7-round biclique for Piccolo-128. Then a full round biclique cryptanalysis of Piccolo is presented. The results of the attacks are with data complexity of 2^{40} and 2^{24} chosen ciphertexts and with computational complexity of $2^{79.22}$ and $2^{127.14}$, respectively. They are superior to other known results of biclique cryptanalytic on Piccolo.

1. Introduction

In ASIACRYPT 2011, Bogdanov et al. proposed a biclique on recovering the keys of the full AES-128/192/256 [1], which is a type of meet-in-the-middle attack and the recent cryptanalysis technique of block ciphers. In [1], they gave two techniques by constructing bicliques for AES. One is the independent related-key differentials biclique and the other is the long biclique. Soon after the paper was published, a great deal of cryptanalytical results on the other block ciphers were suggested.

The crucial issue of the technology is to construct a superior biclique structure at the ciphertext (or plaintext). In a biclique, one top set comprises 2^{d_1} ciphertexts (or plaintexts) while the other set is composed of 2^{d_2} intermediate states. If $d_1 = d_2 = d$, the biclique structure is called a d-dimension ($d = d_1 = d_2 = 8$ in this paper). In some constrained environments, for example, RFID tags or sensor nodes, the size of the secret key is typically 64, 80, or 128 bits. A lot of attacks on lightweight block cipher by using biclique have been published, such as Piccolo [2], IDEA [3], HIGHT [4, 5], LED [6], PRESENT [7, 8], TWINE [9, 10], and KLEIN [11].

The meet-in-the-middle (MITM) attack is a representative method which is used in the security evaluation of block cipher, and its exceptional property is only a minimal data complexity. In recent years, many varieties emerged, for example, 3-subset MITM [12]. Many methods carry out the preimage attack to the hash function [13] and they consist of spice-and-cut frame and partial matching and so forth. Using the key expansion algorithm, opponent can construct a structure and pick out wrong keys through partial matching, which is the important idea of the method.

Piccolo is a 64-bit block cipher. In accordance with the different length of the key, we signify the ciphers by Piccolo-80/128, respectively [14]. In ISPEC 2012, Wang et al. presented a biclique attack on reduced round Piccolo [2]. They attacked a 25-round Piccolo-80 with 2^{48} chosen plaintexts and $2^{78.95}$ computations. In the case of a 28-round Piccolo-128, this attack required 2^{24} chosen plaintexts and $2^{126.79}$ computations. However, the authors considered Piccolo-80 without the postwhitening key and Piccolo-128 without the prewhitening key. In [5], Song et al. proposed a full round biclique cryptanalysis on Piccolo-80 demanding 2^{48} chosen plaintexts and $2^{79.34}$ computations and on Piccolo-128 requiring 2^{24} chosen plaintexts and $2^{127.36}$ computations. In [15], we find two faults which are detailed in Section 4.1 in this paper. Compared to these results, ours are superior to theirs.

Table 1: Summary of previous results of different method on Piccolo.

Piccolo-80 rounds	Piccolo-128 rounds	Method	Reference
7	7	Differential	Reference [14]
8	8	Linear	Reference [14]
9	9	Boomerang	Reference [14]
9	9	Impossible differential	Reference [14]
14	21	MITM	Reference [17]
19	23	MITM expectation	Reference [14]
25	28	Biclique cryptanalysis	Reference [2]
25	31	Biclique cryptanalysis	This paper

Table 2: Summary of biclique cryptanalytic results on Piccolo.

Target algorithm	Round	Data	Computations	Attack type	Reference
Piccolo-80	25 (without the postwhitening key)	2^{48}	$2^{78.95}$	Biclique	Reference [2]
Piccolo-80	25 (full)	2^{48}	$2^{79.34}$	Biclique	Reference [5]
Piccolo-80	25 (full)	2^{40}	$2^{79.22}$	Biclique	Section 4.2
Piccolo-128	28 (without the prewhitening key)	2^{24}	$2^{126.79}$	Biclique	Reference [2]
Piccolo-128	31 (full)	2^{48}	$2^{127.36}$	Biclique	Reference [5]
Piccolo-128	31 (full)	2^{24}	$2^{127.14}$	Biclique	Section 4.3
Piccolo-128	31 (full)	2^{8}	$2^{127.30}$	Biclique	Section 4.4

In this paper, we detect a weakness in the key schedule on Piccolo-80; that is, the round key rk_{47} can offset the postwhitening key partially. Based on this, the data complexity can be decreased greatly. We apply some observations on Piccolo in [16] and construct an independent related-key differentials biclique for the last several rounds. Then an 8-dimensional biclique structure of 6 rounds is constructed for Piccolo-80 and an 8-dimensional biclique structure of 7 rounds for Piccolo-128. The attacks are, respectively, with data complexity of 2^{40} and 2^{24}, and with computational complexity of $2^{79.22}$ and $2^{127.14}$, which are the best results currently. The attack results on Piccolo are summarized in Tables 1 and 2.

The structure of the paper is as follows. Section 2 describes the structures of Piccolo-80 and Piccolo-128. Section 3 introduces briefly biclique cryptanalysis. Then, Section 4 presents the cryptanalysis with an 8-dimensional biclique of 6 rounds on full round Piccolo-80 and with a biclique structure of 7 rounds on full round Piccolo-128. The data complexity and computational complexity on Piccolo-80 and Piccolo-128 are given, respectively. Finally, we draw our conclusion in Section 5.

2. Piccolo Specifications

2.1. Notations

$\oplus$: bit-wise exclusive or (XOR).

r: iterative rounds.

$\|$: concatenation.

$K[i]$: the ith 16-bit group of the key K ($0 \le i \le 4$ for Piccolo-80, $0 \le i \le 7$ for Piccolo-128).

WK_i: the 16-bit whitening key ($0 \le i \le 3$).

rk_i: the 16-bit round key ($0 \le i \le 49$ for Piccolo-80, $0 \le i \le 61$ for Piccolo-128).

con_i^{80}: a 16-bit round constant.

$a_{(b)}$: b denoting the bit length of a.

P: 64-bit plaintext, P including four 16-bit words $P[i]$ ($0 \le i \le 3$).

C: 64-bit ciphertext, C including four 16-bit words $C[i]$ ($0 \le i \le 3$).

$F_{i,j}^r(64)$: the ith and jth byte of the state after F-Function in rth round.

2.2. Description of Piccolo. The structure of Piccolo is a variation of generalized Feistel, as shown in Figure 1. Piccolo-80/128 supports 80-bit and 128-bit key sizes along with 25 and 31 rounds, respectively.

The detailed descriptions of Piccolo are in [14], and each round of Piccolo consists of the following 3 steps:

(1) F-Function (FF), $\{0,1\}^{16} \rightarrow \{0,1\}^{16}$ being composed of two S-box layers and a diffusion matrix M.

(2) AddRoundKey (AK), the 64-bit intermediate state XORs a round key.

(3) RoundPermutation (RP), which splits a 64-bit input into eight bytes and then maps them.

2.3. Key Schedule. The key schedule of Piccolo is straightforward and simple. Firstly, the 80-bit master key of Piccolo-80 is represented by concatenation of five 2 bytes; that is, $K = K[0] \| K[1] \| K[2] \| K[3] \| K[4]$, where $K[j] =$

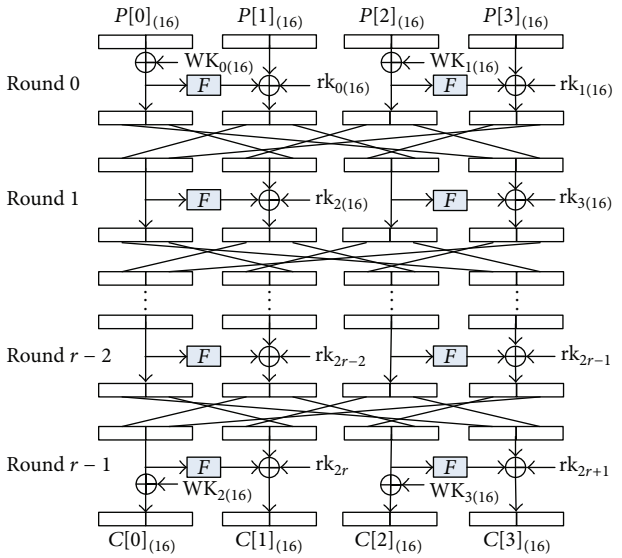

Figure 1: The structure of Piccolo.

$(K[j]^L, K[j]^R)$. The whitening keys $(\mathrm{WK}_0, \mathrm{WK}_1, \mathrm{WK}_2, \mathrm{WK}_3)$ and the subkey $(\mathrm{rk}_{2i}, \mathrm{rk}_{2i+1})$ of 25 rounds are engendered as follows:

$\mathrm{WK}_0 = K[0]^L \parallel K[1]^R$, $\mathrm{WK}_1 = K[1]^L \parallel K[0]^R$, $\mathrm{WK}_2 = K[4]^L \parallel K[3]^R$, $\mathrm{WK}_3 = K[3]^L \parallel K[4]^R$.

For $i = 0$ to $r - 1$

$$\begin{aligned}(\mathrm{rk}_{2i}, \mathrm{rk}_{2i+1}) &= \left(\mathrm{con}_{2i}^{80}, \mathrm{con}_{2i+1}^{80}\right) \\ &\oplus \begin{cases} (K[2], K[3]), & (i \bmod 5) \equiv 0 \text{ or } 2, \\ (K[0], K[1]), & (i \bmod 5) \equiv 1 \text{ or } 4, \\ (K[4], K[4]), & (i \bmod 5) \equiv 3. \end{cases}\end{aligned} \tag{1}$$

For Piccolo-128, the distribution of subkey is similar to that of Piccolo-80. The 128-bit master key is denoted by $K = K[0] \parallel K[1] \parallel K[2] \parallel K[3] \parallel K[4] \parallel K[5] \parallel K[6] \parallel K[7]$, where $K[j] = (K[j]^L, K[j]^R)$. The whitening keys and 31-round subkey are computed as follows:

$\mathrm{WK}_0 = K[0]^L \parallel K[1]^R$, $\mathrm{WK}_1 = K[1]^L \parallel K[0]^R$, $\mathrm{WK}_2 = K[4]^L \parallel K[7]^R$, $\mathrm{WK}_3 = K[7]^L \parallel K[4]^R$.

For $i = 0$ to $2r - 1$

if $((i + 2) \bmod 8 \equiv 0)$, then

$(K[0] \parallel K[1] \parallel K[2] \parallel K[3] \parallel K[4] \parallel K[5] \parallel K[6] \parallel K[7]) = (K[2] \parallel K[1] \parallel K[6] \parallel K[7] \parallel K[0] \parallel K[3] \parallel K[4] \parallel K[5])$;

$\mathrm{rk}_i = K[(i + 2) \bmod 8] \oplus \mathrm{con}_i^{128}$.

The specific subkeys of Piccolo-80/128 are illustrated in Table 3.

3. Biclique Attack on Piccolo

3.1. Definition of Biclique. Biclique cryptanalysis is an attack based on MITM. The major idea is to build bicliques on the target subcipher and promote the computational efficiency. The basic principles of the biclique attack are explained in [1]. Let f be a several-round subcipher and f^{-1} is the inverse of f. The f maps 2^d intermediate states $\{S_j\}$ to 2^d ciphertexts $\{C_i\}$ with 2^{2d} keys $\{K_{[i,j]}\}$:

$$K_{[i,j]} = \begin{bmatrix} K_{[0,0]} & K_{[0,1]} & \cdots & K_{[0,2^d-1]} \\ \vdots & \vdots & \ddots & \vdots \\ K_{[2^d-1,0]} & K_{[2^d-1,1]} & \cdots & K_{[2^d-1,2^d-1]} \end{bmatrix}. \tag{2}$$

The 3-tuple $[\{C_i\}, \{S_j\}, \{K_{[i,j]}\}]$ is named a biclique with d-dimension, if

$$C_i = f_{K_{[i,j]}}\left(s_j\right) \quad \forall i, j \in \{0,1\}^d. \tag{3}$$

To avoid duplication, we do not explicate the detailed attack basis but three stages of the attack are described in more detail.

3.2. Biclique Cryptanalysis of Piccolo-80

3.2.1. Phase 1: Key Partitioning. For greater clarity, we divide the key into 2^{64} groups which have 2^{16} keys. The $K_{[0,0]}$ enumerates 64-bit keys and fixes 16-bit keys with 0_{16}. As depicted in Section 2.3, each round has 32-bit subkey which is generated by master keys $K[i]$ and $K[j]$. By investigating the subkey distribution (Table 3), an 8-dimensional biclique structure of 6 rounds is constructed by each right half of $K[4]$ and $K[2]$, that is, $K[4]^R$ and $K[2]^R$. We find $K[4]^R$ of the round key rk_{47} can offset $K[4]^R$ of the postwhitening key, so it can decrease the data complexity greatly. By calculation, the computational complexity is optimal so far.

The keys $K_{[0,0]}, K_{[0,j]}, K_{[i,0]}$, and $K_{[i,j]}$ of each group are depicted, as shown below:

$$K_{[0,0]} = [XX, XX, XA, XX, XA],$$

where $X \in \{0,1\}^8$, $A = 0x00$,

$$K_{[0,j]} = K_{[0,0]} \oplus [00, 00, 0j, 00, 00],$$

where $j \in \{0,1\}^8$,

Table 3: Key schedule of Piccolo.

Piccolo-80			Piccolo-128		
Round i	Round key	Master key	Round i	Round key	Master key
Initial	(WK_0, WK_1)	$(K[0]^L \parallel K[1]^R, K[1]^L \parallel K[0]^R)$	Initial	(WK_0, WK_1)	$(K[0]^L \parallel K[1]^R, K[1]^L \parallel K[0]^R)$
0	(rk_0, rk_1)	$(K[2], K[3])$	0	(rk_0, rk_1)	$(K[2], K[3])$
1	(rk_2, rk_3)	$(K[0], K[1])$	1	(rk_2, rk_3)	$(K[4], K[5])$
2	(rk_4, rk_5)	$(K[2], K[3])$	2	(rk_4, rk_5)	$(K[6], K[7])$
3	(rk_6, rk_7)	$(K[4], K[4])$	3	(rk_6, rk_7)	$(K[2], K[1])$
4	(rk_8, rk_9)	$(K[0], K[1])$	4	(rk_8, rk_9)	$(K[6], K[7])$
5	(rk_{10}, rk_{11})	$(K[2], K[3])$	5	(rk_{10}, rk_{11})	$(K[0], K[3])$
6	(rk_{12}, rk_{13})	$(K[0], K[1])$	6	(rk_{12}, rk_{13})	$(K[4], K[5])$
⋮	⋮	⋮	⋮	⋮	⋮
18	(rk_{36}, rk_{37})	$(K[4], K[4])$	24	(rk_{48}, rk_{49})	$(K[4], K[3])$
19	(rk_{38}, rk_{39})	$(K[0], K[1])$	25	(rk_{50}, rk_{51})	$(K[2], K[5])$
20	(rk_{40}, rk_{41})	$(K[2], K[3])$	26	(rk_{52}, rk_{53})	$(K[0], K[7])$
21	(rk_{42}, rk_{43})	$(K[0], K[1])$	27	(rk_{54}, rk_{55})	$(K[4], K[1])$
22	(rk_{44}, rk_{45})	$(K[2], K[3])$	28	(rk_{56}, rk_{57})	$(K[0], K[7])$
23	(rk_{46}, rk_{47})	$(K[4], K[4])$	29	(rk_{58}, rk_{59})	$(K[6], K[3])$
24	(rk_{48}, rk_{49})	$(K[0], K[1])$	30	(rk_{60}, rk_{61})	$(K[2], K[5])$
Final	(WK_2, WK_3)	$(K[4]^L \parallel K[3]^R, K[3]^L \parallel K[4]^R)$	Final	(WK_2, WK_3)	$(K[4]^L \parallel K[7]^R, K[7]^L \parallel K[4]^R)$

$$K_{[i,0]} = K_{[0,0]} \oplus [00, 00, 00, 00, 0i], \quad \text{where } i \in \{0,1\}^8. \tag{4}$$

Finally,

$$\begin{aligned} K_{[i,j]} &= K_{[0,0]} \oplus K_{[0,j]} \oplus K_{[i,0]} \\ &= K_{[0,0]} \oplus [00, 00, 0j, 00, 0i]. \end{aligned} \tag{5}$$

Thus, the space of K is divided into 2^{64} groups of 2^{16} keys each.

3.2.2. Phase 2: 8-Dimensional Biclique Structure of 6 Rounds. We construct an 8-dimensional biclique structure of 6 rounds for Piccolo-80 with whitening keys for each group (Figure 2). The biclique structure connects 2^8 ciphertexts to 2^8 intermediate states in each group of keys. The process of calculating the ciphertexts and intermediate states consists of the following 3 steps.

Step 1. Let $C_0 = 0_{(64)}$ and decrypt C_0 for 6 rounds to obtain S_0 (Figure 2(a)); that is, $S_0 = f^{-1}K_{[0,0]}(C_0)$. The procedure is named basic calculation.

Step 2. In order to get the corresponding ciphertext C_i, encrypt S_0 using different keys $K_{[i,0]}$ for $i \in \{0,1\}^8$ (Figure 2(c)). The differences between $K_{[i,0]}$ and $K_{[0,0]}$ can lead to the gray intermediate states' differences and cause the computational complexity. The gray intermediate states need to be computed $2^8 - 1$ times, whereas the remaining states are calculated just once because they have been already computed in Step 1. This step derives $f(S_0) \xrightarrow{K_{[i,0]}} C_i$.

Step 3. To get the corresponding states S_j, decrypt C_0 using different keys $K_{[0,j]}$ for $j \in \{0,1\}^8$ (Figure 2(b)). The differences between $K_{[0,j]}$ and $K_{[0,0]}$ can bring about the gray intermediate states' differences. The gray intermediate states need to be computed $2^8 - 1$ times, whereas the remaining states have been already computed. As a result, $f^{-1}(C_0) \xrightarrow{K_{[0,j]}} (S_j)$ has been constructed.

Thanks to the simplicity of the distribution of the subkey of Piccolo, the two differential paths do not share any active state. Fortunately, it is so easy to verify that $f(S_j) \xrightarrow{K_{[i,j]}} C_i$ is always true for all $i, j \in \{0,1\}^8$. Up to now, for each key group, we get a corresponding 8-dimensional biclique structure as discussed above.

From Figure 2, we find a weakness in the key schedule of Piccolo-80; that is, $K[4]^R$ of the round key rk_{47} can offset $K[4]^R$ of the postwhitening key. So it can reduce the data complexity greatly. The calculations of complexities are presented in Section 4.2.

3.2.3. Phase 3: Meeting in the Middle over 19 Rounds. Choose a 16-bit internal state ($V = F^9_{1,4}$) after F-Function in round 9, as the intermediate matching variable (see Figure 3). The choice is made according to the total number of F-Function and an effective filtering of the wrong keys. Next, we calculate these matching variates in both directions in order to obtain the accurate key.

Backward Direction. Each value of the state S_j is decrypted under the key $K_{[0,j]}$ to derive $\overleftarrow{V}_{0,j} \xleftarrow{K_{[0,j]}} S_j$. After that,

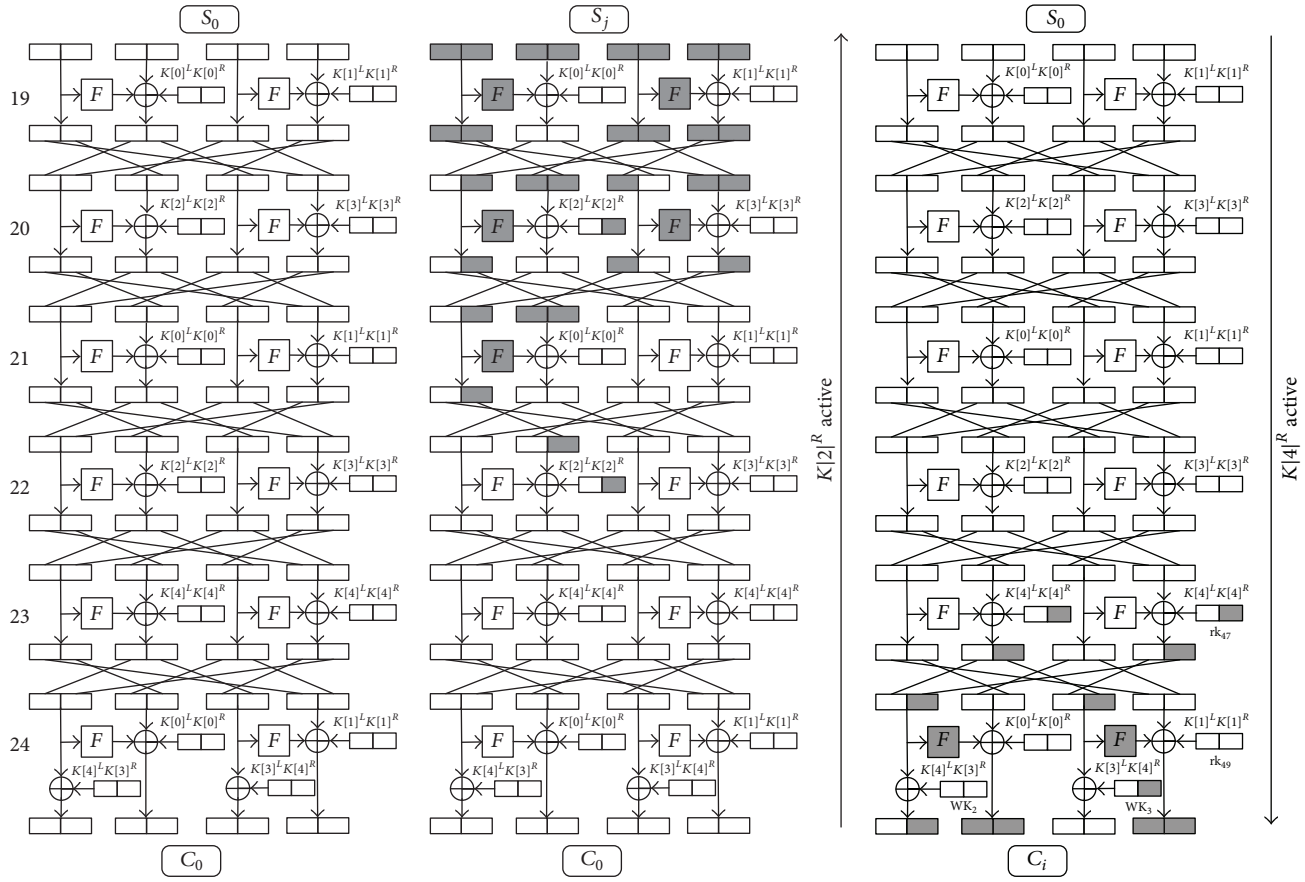

Figure 2: 6-round biclique construction of dimension 8 in Piccolo-80.

S_j is decrypted using all the possible $2^d - 1$ keys $K_{[i,j]}$ to get $\overleftarrow{V_{i,j}} \xleftarrow{K_{[i,j]}} S_j$. Because of the same beginning, the key differences between $K_{[0,j]}$ and $K_{[i,j]}$ can cause the computational complexity. On Figure 3(b), the gray bytes are active and the white bytes need not be computed.

Forward Direction. The procedure of forward direction is a bit more complex than the backward direction in calculation. Firstly, we decrypt the ciphertexts C_i for $i \in \{0,1\}^8$ to obtain 2^8 plaintexts P_i. Secondly, each P_i is encrypted under the key $K_{[i,0]}$ to derive $P_i \xrightarrow{K_{[i,0]}} \overrightarrow{V_{i,0}}$. After that, P_i is encrypted using all the possible $2^d - 1$ keys $K_{[i,j]}$ to obtain $P_i \xrightarrow{K_{[i,j]}} \overrightarrow{V_{i,j}}$. The differences between $K_{[i,0]}$ and $K_{[i,j]}$ can influence the computational complexity. On Figure 3(a), the gray bytes are active and the white bytes need not be computed.

Search Candidates. In the last session of the attack, the adversary verifies the rest candidate key by the equality of $\overrightarrow{V_{i,j}}$ and $\overleftarrow{V_{i,j}}$ for all $i, j \in \{0,1\}^8$ in each group exhaustively, until the right key is discovered.

3.3. Biclique Cryptanalysis of Piccolo-128

3.3.1. Phase 1: Key Partitioning. We divide the 128-bit key into 2^{112} groups. $K_{[0,0]}$ enumerates 112-bit keys and fixes 16-bit keys with 0_{16}. By investigating the subkey distribution (Table 3), an 8-dimensional biclique structure of 7 rounds is constructed by each left half of $K[6]$ and $K[7]$, that is, $K[6]^L$ and $K[7]^L$. The computational complexity of this structure is less than others'.

Similar to Piccolo-80, the keys $K_{[0,0]}, K_{[0,j]}, K_{[i,0]}$, and $K_{[i,j]}$ of each group are depicted, as shown below:

$$\begin{aligned} K_{[0,0]} &= [XX, XX, XX, XX, XX, XX, AX, AX], \\ &\qquad \text{where } X \in \{0,1\}^8,\ A = 0x00, \\ K_{[0,j]} &= K_{[0,0]} \oplus [00, 00, 00, 00, 00, 00, 00, j0], \\ &\qquad \text{where } j \in \{0,1\}^8, \\ K_{[i,0]} &= K_{[0,0]} \oplus [00, 00, 00, 00, 00, 00, i0, 00], \\ &\qquad \text{where } i \in \{0,1\}^8. \end{aligned} \tag{6}$$

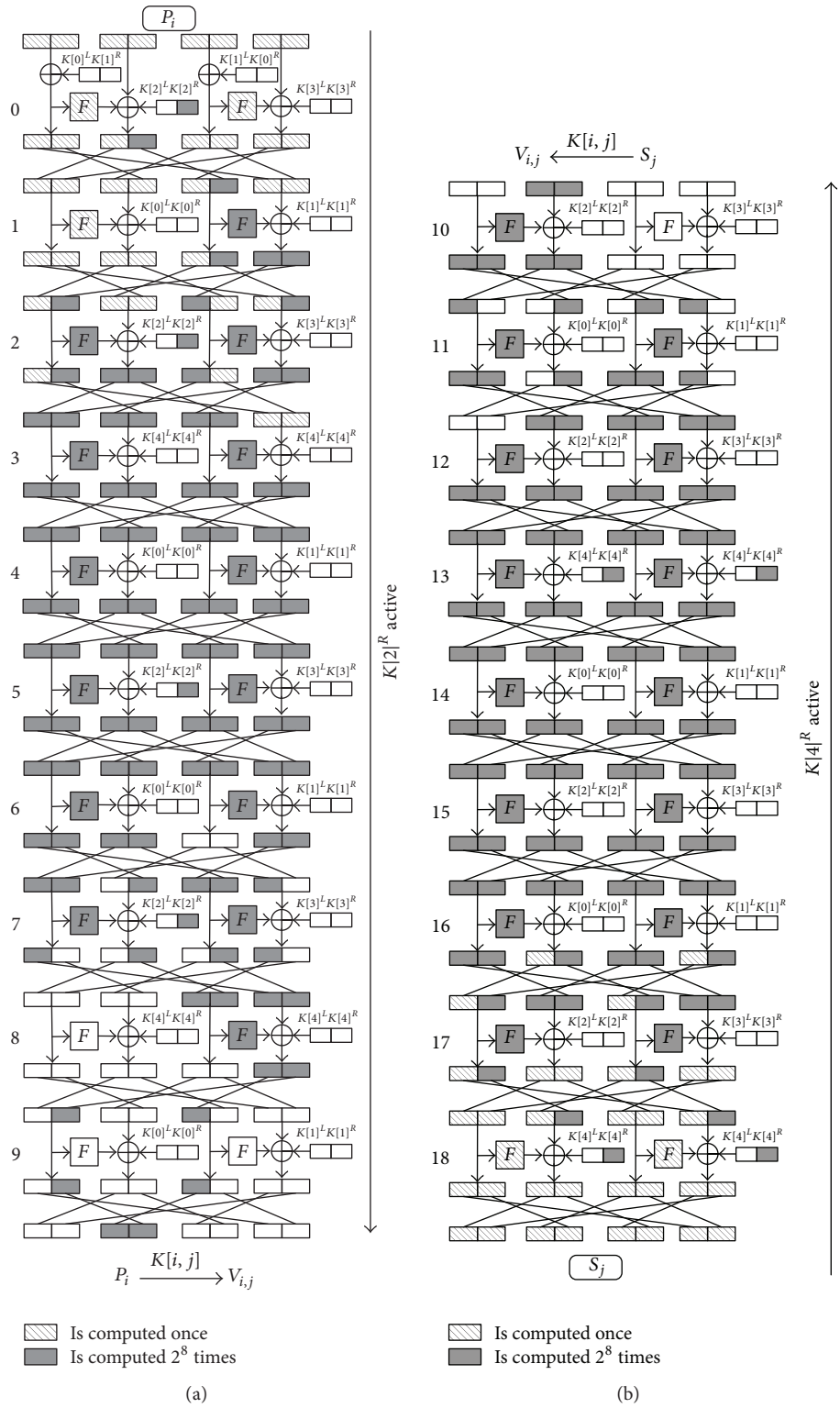

Figure 3: Recomputations in MITM for Piccolo-80.

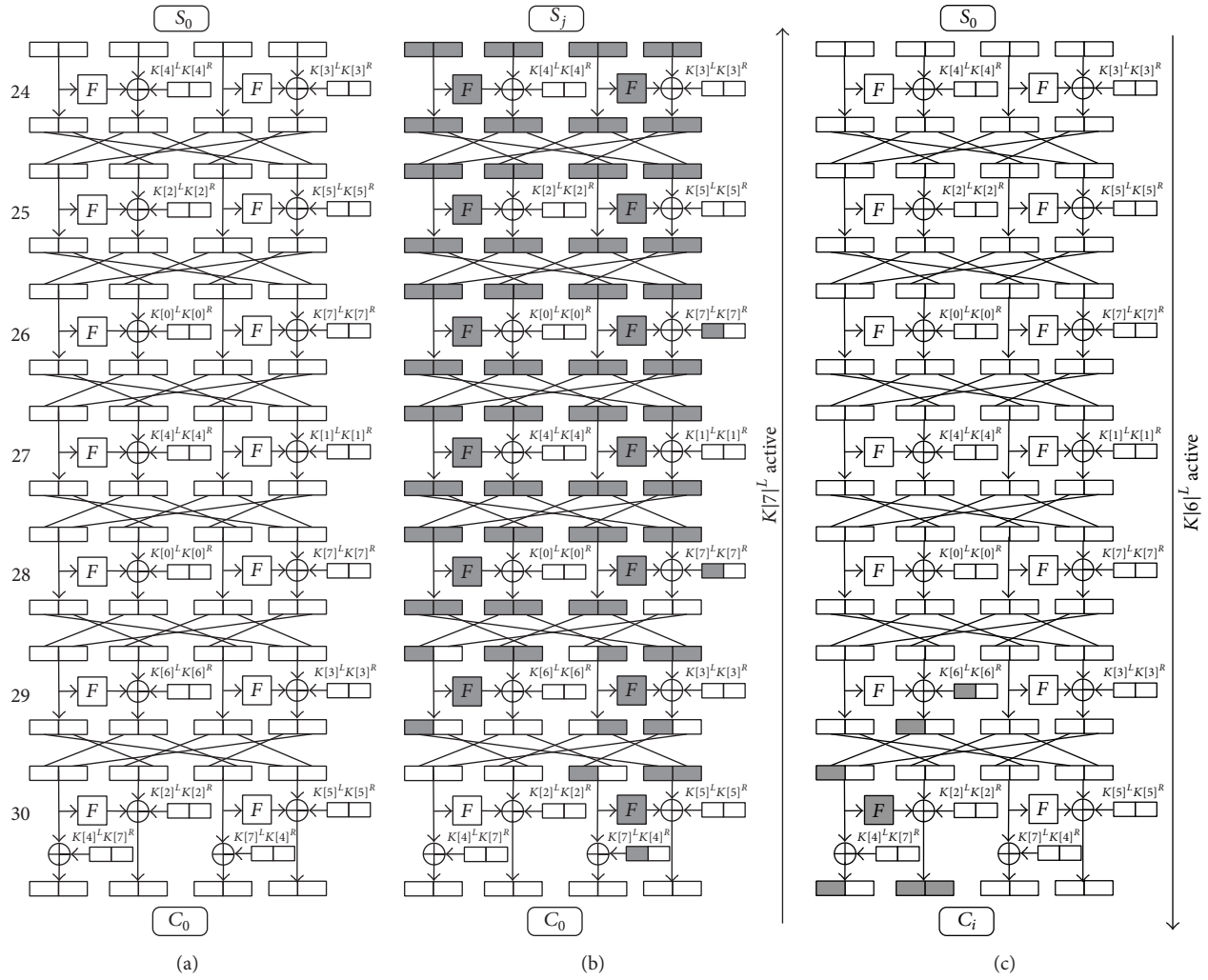

Figure 4: 7-round biclique construction of dimension 8 in Piccolo-128.

Finally,

$$\begin{aligned} K_{[i,j]} &= K_{[0,0]} \oplus K_{[0,j]} \oplus K_{[i,0]} \\ &= K_{[0,0]} \oplus [00, 00, 00, 00, 00, 00, i0, j0]. \end{aligned} \tag{7}$$

Thus, the key space of K is divided into 2^{112} groups of 2^{16} keys each.

3.3.2. Phase 2: 8-Dimensional Biclique Structure of 7 Rounds. We construct an 8-dimensional biclique structure of 7 rounds for Piccolo-128 for each group (Figure 4). Here, g is subciphers for round 24~30 and g^{-1} is the inverse of g. The process of calculating the ciphertexts and intermediate states consists of the following 3 steps.

Step 1. Let $C_0 = 0_{(64)}$ and decrypt C_0 for 7 rounds to obtain S_0 (Figure 4(a)); that is, $S_0 = g^{-1}K_{[0,0]}(C_0)$.

Step 2. Encrypt S_0 using different keys $K_{[i,0]}$ for $i \in \{0,1\}^8$ (Figure 4(c)). The differences between $K_{[i,0]}$ and $K_{[0,0]}$ can influence the gray intermediate states' differences. This step derives $g(S_0) \xrightarrow{K_{[i,0]}} C_i$.

Step 3. Decrypt C_0 using different keys $K_{[0,j]}$ for $j \in \{0,1\}^8$ (Figure 4(b)). The differences between $K_{[0,j]}$ and $K_{[0,0]}$ can bring about the gray intermediate states' differences. As a result, $g^{-1}(C_0) \xrightarrow{K_{[0,j]}} (S_j)$ has been constructed.

Thanks to the simplicity of the distribution of the subkey of Piccolo-128, it is also very easy to verify that $g(S_j) \xrightarrow{K_{[i,j]}} C_i$ is always true for all $i, j \in \{0,1\}^8$. Up to now, for each key group, we get a corresponding 8-dimensional biclique structure.

3.3.3. Phase 3: Meeting in the Middle over 24 Rounds. Select a 16-bit internal state ($U = F^{12}_{1,4}$) after F-Function in round 12, as the intermediate matching variable (see Figure 5). Next, we calculate these matching variates in both directions in order to obtain the right key.

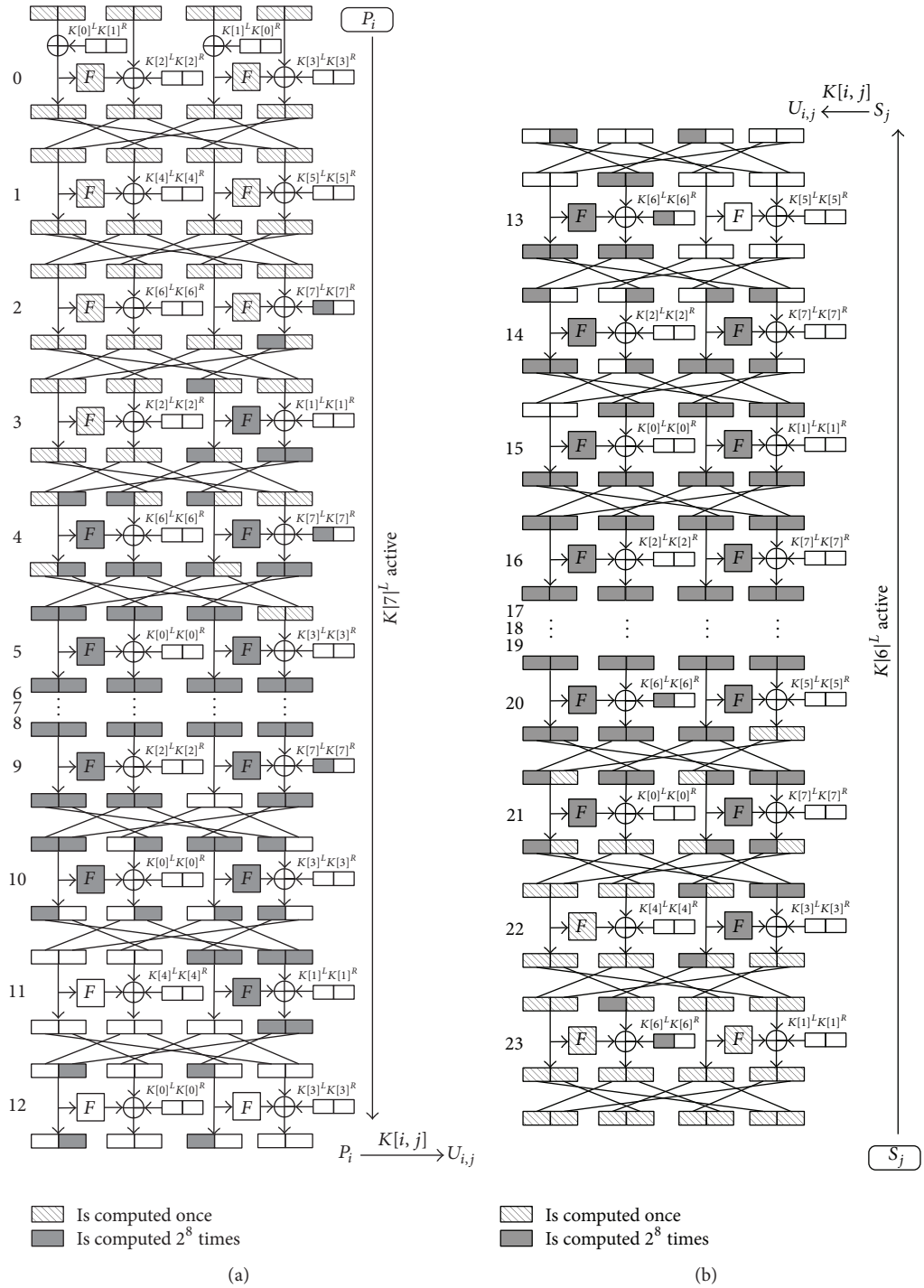

Figure 5: Recomputations in MITM for Piccolo-128.

Backward Direction. Each value of the state S_j is decrypted under the key $K_{[0,j]}$ to obtain $\overleftarrow{U_{0,j}} \xleftarrow{K_{[0,j]}} S_j$. After that, S_j is decrypted using all the possible $2^d - 1$ keys $K_{[i,j]}$ to get $\overleftarrow{U_{i,j}} \xleftarrow{K_{[i,j]}} S_j$. On Figure 5(b), the gray bytes are active and the white bytes do not need to be computed.

Forward Direction. Firstly, we decrypt the ciphertexts C_i for $i \in \{0,1\}^8$ to obtain 2^8 plaintexts P_i. Secondly, each P_i is encrypted under the key $K_{[i,0]}$ to obtain $P_i \xrightarrow{K_{[i,0]}} \overrightarrow{U_{i,0}}$. Then, P_i is encrypted using all the possible $2^d - 1$ keys $K_{[i,j]}$ to get $P_i \xrightarrow{K_{[i,j]}} \overrightarrow{U_{i,j}}$. On Figure 5(a), the gray bytes are active and the white bytes do not need to be computed.

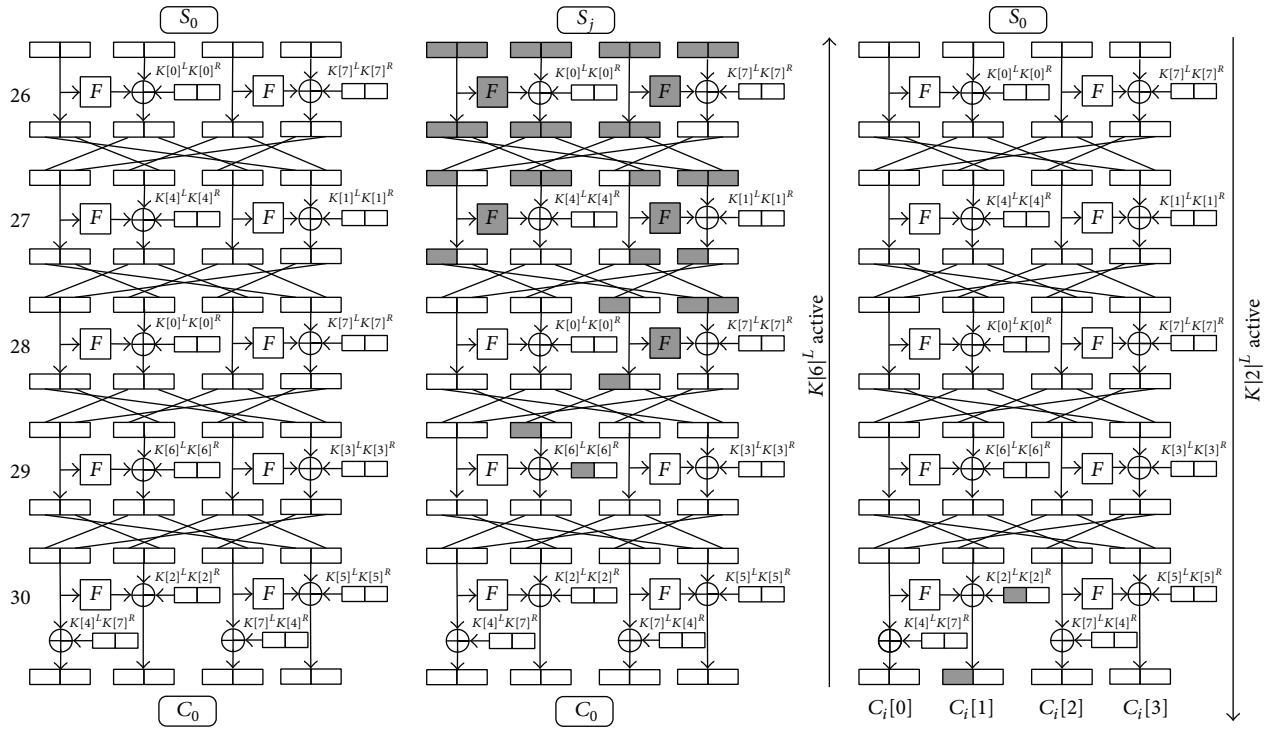

Figure 6: 5-round biclique construction of dimension 8 in Piccolo-128.

Search Candidates. In the last session of the attack, the adversary verifies the equality of $\overrightarrow{U_{i,j}}$ and $\overleftarrow{U_{i,j}}$ for all $i, j \in \{0,1\}^8$ to discover the correct key.

3.4. Another Biclique Cryptanalysis of Piccolo-128. Similar to Section 3.3, we construct an 8-dimensional biclique structure of 5 rounds (26~30) for Piccolo-128 by each left half of $K[6]$ and $K[2]$, that is, $K[6]^L$ and $K[2]^L$ (Figure 6).

In the phase of meeting in the middle over 26 rounds, we select a 16-bit internal state ($U = F^{13}_{1,4}$) after F-Function in round 13, as the intermediate matching variable.

4. Complexities

4.1. Comments on the Result of [15]. Jeong et al. applied biclique cryptanalysis to the lightweight block ciphers LED, Piccolo, and PRESENT in [15]. They used the concept of independent-biclique which included constructing biclique structure by independent related-key differentials and matching with precomputations. They found a limited and slow diffusion of the subkey distribution and encryption process. As a result, their attacks can discover the master key with computational complexities superior to an exhaustive search. However, we find two faults of their biclique cryptanalysis of Piccolo as follows:

(1) Jeong et al. found that $K[4]^L$ and $K[2]^L$ gave the construction of an 8-dimensional biclique which was shown in Figure 10 of [15]. The Δ_i-differential affected only 6 bytes ($C[0]^L$, $C[1]^L$, $C[1]^R$, $C[2]^L$, $C[3]^L$, and $C[3]^R$) which is drawn on Figure 7(a) (including the grid line byte) in this paper. As a result, the data complexity does not go beyond 2^{48}.

In the attack shown in Figure 7, it is clear that the left half of the round key rk_{46} can offset the left half of WK_2 (the postwhitening key); that is, there is no difference in the grid line byte ($C[0]^L$). Based on this, the biclique cryptanalysis of Jeong et al. goes wrong.

So, the Δ_i-differential affects only 5 bytes ($C[1]^L$, $C[1]^R$, $C[2]^L$, $C[3]^L$, and $C[3]^R$) of the ciphertext and the data complexity does not go beyond 2^{40}. The correct difference path does not include the grid line byte ($C[0]^L$).

(2) Jeong et al. thought that only 2 bytes were active in the decryption of 17th round in backward direction for Piccolo-80 of recomputation, shown in Figure 11 of [15]. 13 F-Functions (without the grid line) were computed 2^8 times and 4 F-Functions were computed once. They are drawn on Figure 7(b) in this paper. Then the total complexity of this step is $2^8 \times (2^8 \times 13 + 4)$ F-Functions.

It is clear that 6 bytes of intermediate are active in the decryption of 17th round in backward direction for Piccolo-80 of recomputation and all bytes are active of 16th round. Based on these, their computational complexity of this step goes wrong.

So, 15 F-Functions (including the grid line) are computed 2^8 times and 2 F-Functions are computed once. Then the total complexity of this step is $2^8 \times (2^8 \times 15 + 2)$ F-Functions. The correct difference path includes the grid line bytes.

Similarly, 3 bytes but not one byte are active in the decryption of 22nd round in backward direction for Piccolo-128 of recomputation and they are shown in Figure 13 of [15].

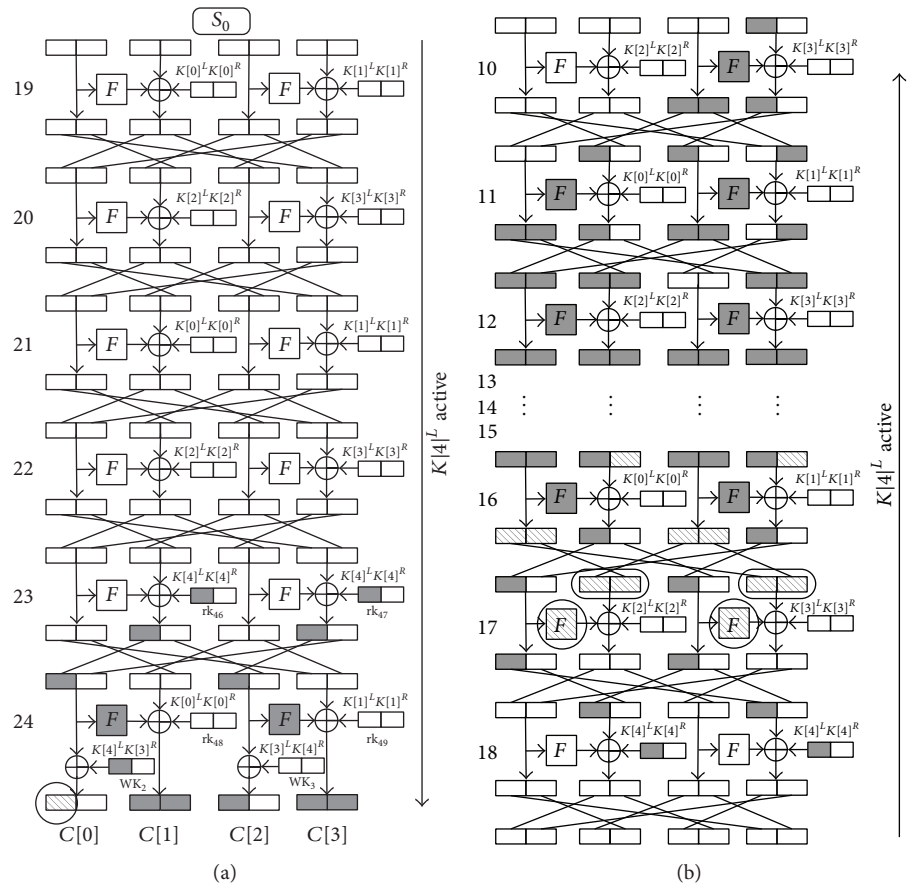

Figure 7: Revision of the other solutions.

20 rather than 18 F-Functions are computed 2^8 times and 3 instead of 5 F-Functions are computed once.

4.2. Complexities of Biclique Cryptanalysis on Piccolo-80

4.2.1. Data Complexity. By analyzing the key schedule, we find a weakness in the key schedule on Piccolo-80; that is, the round key rk_{47} can offset the postwhitening key partially (see Figure 2). Based on this, the data complexity can be reduced greatly.

The amount of ciphertexts to be decrypted dominates the data complexity (Figure 2). For each biclique structure, let $C_0 = 0_{(64)}$. All the ciphertexts share the equal values in 3 bytes ($C_i[0]$, $C_i[4]$, and $C_i[5]$, i.e., white bytes), so the data complexity does not go beyond 2^{40}.

4.2.2. Computational Complexity. The amount of the F-Functions to be computed determines the attack complexity. Each round of Piccolo-80 takes 2 F-Functions computations. So, the single encryption equals computed $25 \times 2 = 50$ F-Functions. For each of 2^{64} groups of keys, the following calculation should be completed.

Biclique Complexity. 5 F-Functions (Figure 2(b), noted with gray) need to be computed 2^8 times and 2 F-Functions (Figure 2(c), noted with gray) need to be computed 2^8 times. The remaining 5 F-Functions are computed only once. Thus, this stage requires $2^8 \times 7 + 5$ F-Functions computations in total. Then, the computational complexity of a biclique structure is about $2^{5.17}$ full round Piccolo-80 encryptions.

Matching Complexity. In forward direction, the differences between $K_{[i,0]}$ and $K_{[i,j]}$ dominate the computational complexity. On Figure 3(a), for a single P_i, 14 F-Functions (noted with gray) are computed 2^8 times, 3 F-Functions (noted with grid line) are computed only once, and 3 F-Functions (noted with white) do not need to be computed. So, the complexity of this process is $2^8 \times (2^8 \times 14 + 3)$ F-Functions, which is about $2^{14.16}$ full round Piccolo-80 encryptions.

In backward direction, on Figure 3(b), for a single S_j, 15 F-Functions (noted with gray) are computed 2^8 times, 2 F-Functions (noted with grid line) are computed only once, and 1 F-Function (noted with white) need not be computed. So, the complexity of this process is $2^8 \times (2^8 \times 15 + 2)$ F-Functions, which is about $2^{14.26}$ full round Piccolo-80 encryptions.

Finally, 2^{16} key candidates are verified by a matching variable (16 bits) in each group, and the average of $2^{16-16} = 1$ candidate key needs to be rechecked.

Thus, the total computational complexity of this attack on Piccolo-80 is

$$C = 2^{64} \times \left(2^{5.17} + 2^{14.16} + 2^{14.26} + 1\right) \approx 2^{79.22}. \quad (8)$$

4.3. Complexities of Biclique Cryptanalysis on Piccolo-128

4.3.1. Data Complexity. For each biclique structure, let $C_0 = 0_{(64)}$. All the ciphertexts share the equal values in 5 bytes ($C_i[1]$, $C_i[4]$, $C_i[5]$, $C_i[6]$, and $C_i[7]$, i.e., white bytes), so the data complexity does not go beyond 2^{24} (See Figure 4).

4.3.2. Computational Complexity. Each round of Piccolo-128 takes 2 F-Functions computations. So, the single encryption equals computed $31 \times 2 = 62$ F-Functions. For each of 2^{112} groups of keys, the following calculation should be completed.

Biclique Complexity. 13 F-Functions (Figure 4(b), noted with gray) need to be computed 2^8 times and 1 F-Function (Figure 4(c), noted with gray) needs to be computed 2^8 times. Thus, this stage requires $2^8 \times 14$ F-Functions computations in total. Then, the computational complexity of a biclique structure is about $2^{5.85}$ full round Piccolo-128 encryptions.

Matching Complexity. In forward direction, for a single P_i, 16 F-Functions (noted with gray) are computed 2^8 times, 7 F-Functions (noted with grid line) are computed only once, and 3 F-Functions (noted with white) do not need to be computed on Figure 5(a). So, the complexity of this process is $2^8 \times (2^8 \times 16 + 7)$ F-Functions, which is about $2^{14.05}$ full round Piccolo-128 encryptions.

In backward direction, for a single S_j, 18 F-functions (noted with gray) are computed 2^8 times, 3 F-functions (noted with grid line) are computed only once, and 1 F-Function (noted with white) need not be computed on Figure 5(b). So, the complexity of this process is $2^8 \times (2^8 \times 18 + 3)$ F-Functions, which is about $2^{14.22}$ full round Piccolo-128 encryptions.

Finally, 2^{16} key candidates are verified by a matching variate (16 bits) in each group, and the average of $2^{16-16} = 1$ candidate key needs to be rechecked.

Thus, the total computational complexity of this attack on Piccolo-128 is

$$C = 2^{112} \times \left(2^{5.85} + 2^{14.08} + 2^{14.22} + 1\right) \approx 2^{127.14}. \quad (9)$$

4.4. Complexities of Another Biclique Cryptanalysis on Piccolo-128

4.4.1. Data Complexity. For each biclique structure, let $C_0 = 0_{(64)}$. All the ciphertexts share the equal values in 7 bytes ($C_i[0]$, $C_i[1]$, $C_i[3]$, $C_i[4]$, $C_i[5]$, $C_i[6]$, and $C_i[7]$, i.e., white bytes), so the data complexity does not go beyond 2^8 (See Figure 6).

4.4.2. Computational Complexity

Biclique Complexity. This stage requires $2^8 \times 5 + 5$ F-Functions computations in total. Then, the computational complexity of a biclique structure is about $2^{4.38}$ full round Piccolo-128 encryptions.

Matching Complexity. In forward direction, the complexity is $2^8 \times (2^8 \times 18 + 7)$ F-Functions, which is about $2^{14.22}$ full round Piccolo-128 encryptions. In backward direction, the complexity is $2^8 \times (2^8 \times 20 + 3)$ F-Functions, which is about $2^{14.37}$ full round Piccolo-128 encryptions.

Thus, the total computational complexity of this attack on Piccolo-128 is

$$C = 2^{112} \times \left(2^{4.38} + 2^{14.22} + 2^{14.37} + 1\right) \approx 2^{127.30}. \quad (10)$$

5. Conclusion

Designers have given several attacks including linear cryptanalysis, impossible differential cryptanalysis, and MITM attack on security analysis for Piccolo. The best result was 3-subset MITM attacks on 14/21-round Piccolo-80/128 without the whitening key. The previous results and our results are summarized on Piccolo in Tables 1 and 2. Some results did not include whitening key; some attacks were reduced-round. However, our results are full round Piccolo-80/128.

By analyzing the distribution of the subkey and the structure of encryption, we find two faults of the results in [15] and a weakness in the key schedule on Piccolo-80. The two faults are depicted in Section 4.1. The weakness on Piccolo-80 is that the right half of the round key rk_{47} can offset the right half of the postwhitening key WK_3 (Figure 2(c)). Based on this, the data complexity can be decreased greatly.

We use biclique cryptanalysis to recover the master key for the full round Piccolo-80 with a 6-round biclique and the full round Piccolo-128 with a 7-round biclique, respectively. The attacks require data complexity of 2^{40} and 2^{24} chosen ciphertexts and computational complexity of $2^{79.22}$ and $2^{127.14}$, respectively. These results are superior to other biclique cryptanalytic results on Piccolo.

This result is that the biclique technology can attack some ciphers with simple key schedule and slow diffusion. So, the designers of lightweight ciphers need to consider not only the implementation efficiency, but also key schedule complexity and diffusion speed.

Conflicts of Interest

None of the authors declare any conflicts of interest.

Acknowledgments

This work is partially supported by National Natural Science Foundation of China (nos. 61272434, 61672330, and 61602287) and Nature Science Foundation of Shandong Province (no. ZR2013FQ021).

References

[1] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique cryptanalysis of the full AES," in *Advances in Cryptology—ASIACRYPT 2011*, vol. 7073 of *Lecture Notes in Comput. Sci.*, pp. 344–371, Springer, Heidelberg, Germany, 2011.

[2] Y. Wang, W. Wu, and X. Yu, "Biclique cryptanalysis of reduced-round piccolo block cipher," in *Proceedings of the 8th International Conference on Information Security Practice and Experience (ISPEC '12)*, M. R. Dermot, S. Ben, and G. Wang, Eds., vol. 7232 of *Lecture Notes in Computer Science*, pp. 337–352, Springer, Heidelberg, Germany, 2012.

[3] D. Khovratovich, G. Leurent, and C. Rechberger, "Narrow-bicliques: cryptanalysis of full IDEA," in *Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '12)*, Lecture Notes in Computer Science, pp. 392–410, Springer, Heidelberg, Germany, 2012.

[4] D. Hong, B. Koo, and D. Kwon, "Biclique attack on the full HIGHT," in *Information Security and Cryptology—ICISC 2011*, vol. 7259 of *Lecture Notes in Computer Science*, pp. 365–374, Springer, Berlin, Germany, 2012.

[5] J. Song, K. Lee, and H. Lee, "Biclique cryptanalysis on lightweight block cipher: HIGHT and Piccolo," *International Journal of Computer Mathematics*, vol. 90, no. 12, pp. 2564–2580, 2013.

[6] F. Abed, C. Forler, E. List, S. Lucks, and J. Wenzel, "Biclique cryptanalysis of the PRESENT and LED lightweight ciphers," Tech. Rep. 2012/591, Cryptology ePrint Archive, 2012.

[7] M. Sereshgi and M. Shakiba, "Biclique cryptanalysis of MIBS-80 and PRESENT-80 block ciphers," *Security and Communication Networks*, vol. 9, no. 1, pp. 27–33, 2016.

[8] O. Özen, K. Varıcı, C. Tezcan, and Ç. Kocair, "Lightweight block ciphers revisited: cryptanalysis of reduced round PRESENT and HIGHT," in *Information Security and Privacy*, vol. 5594 of *Lecture Notes in Computer Science*, pp. 90–107, Springer, Berlin, Germany, 2009.

[9] Y. F. Wang and W. L. Wu, "Meet-in-the-middle attack on TWINE block cipher," *Journal of Software*, vol. 26, no. 10, pp. 2684–2695, 2015 (Chinese).

[10] M. Çoban, F. Karakoc, and Ö. Biztaş, "Biclique cryptanalysis of TWINE," Tech. Rep. 2012/422, Cryptology ePrint Archive, 2012.

[11] Z. Ahmadian, M. Salmasizadeh, and M. R. Aref, "Biclique cryptanalysis of the full-round KLEIN block cipher," *IET Information Security*, vol. 9, no. 5, pp. 294–301, 2015.

[12] W. Diffie and M. E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer*, vol. 10, no. 6, pp. 74–84, 1977.

[13] Y. Sasaki, "Meet-in-the-middle preimage attacks on AES hashing modes and an application to whirlpool," in *Proceedings of the International Workshop on Fast Software Encryption (FSE '11)*, A. Joux, Ed., vol. 6733 of *Lecture Notes in Computer Science*, pp. 378–396, Springer, Heidelberg, Germany, 2011.

[14] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "Piccolo: an ultra-lightweight blockcipher," in *Proceedings of the 13th International Workshop on Cryptographic Hardware and Embedded Systems (CHES '11)*, B. Preneel and T. Takagi, Eds., vol. 6917 of *Lecture Notes in Computer Science*, pp. 342–357, Springer, Heidelberg, Germany, 2011.

[15] K. Jeong, H. Kang, C. Lee, J. Sung, and S. Hong, "Biclique cryptanalysis of lightweight block ciphers PRESENT, piccolo and LED," Tech. Rep. 2012/621, Cryptology ePrint Archive, 2012.

[16] W. Zhang, J. Zhang, and X. Zheng, "Some observations on the lightweight block cipher piccolo-80," in *Proceedings of the 6th International Conference on Trusted Systems (INTRUST '14)*, vol. 9473 of *Lecture Notes in Computer Science*, pp. 364–373, Springer, Cham, Switzerland, 2015.

[17] T. Isobe and K. Shibutani, "Security analysis of the lightweight block ciphers XTEA, LED and piccolo," in *Information Security and Privacy*, vol. 7372, pp. 71–86, Springer, Berlin, Germany, 2012.