New Analysis of Reduced-Version of Piccolo in the Single-Key Scenario

Ya Liu[1,2,3*], Liang Cheng[1], Fengyu Zhao[1], Chunhua Su[4], Zhiqiang Liu[3], Wei Li[5,6], Dawu Gu[3]
[1] Department of Computer Science and Engineering, University of Shanghai for Science and Technology, Shanghai, 200093 - P.R. China
[2] Engineering Research Center of Optical Instrument and System, Ministry of Education , Shanghai Key Lab of Modern Optical System, University of Shanghai for Science and Technology, Shanghai, 200093 - P.R. China
[3] Department of Computer Science and Engineering, Shanghai Jiao Tong University Shanghai, 200240 - P.R. China
[e-mail: liuya@usst.edu.cn]
[4] Division of Computer Science, University of Aizu, Aizuwakamatsu, Japan
[5] School of Computer Science and Technology, Donghua University, Shanghai, 201620 – P.R. China
[6] Shanghai Key Laboratory of Integrate Adminstration Technologies for Information Security, Shanghai, 200240 - P.R. China
*Corresponding author: Ya Liu

Received June 30, 2017; revised December 21, 2018; accepted February 12, 2019; published September 30, 2019

Abstract

The lightweight block cipher Piccolo adopts Generalized Feistel Network structure with 64 bits of block size. Its key supports 80 bits or 128 bits, expressed by Piccolo-80 or Piccolo-128, respectively. In this paper, we exploit the security of reduced version of Piccolo from the first round with the pre-whitening layer, which shows the vulnerability of original Piccolo. As a matter of fact, we first study some linear relations among the round subkeys and the properties of linear layer. Based on them, we evaluate the security of Piccolo-80/128 against the meet-in-the-middle attack. Finally, we attack 13 rounds of Piccolo-80 by applying a 5-round distinguisher, which requires 2^{44} chosen plaintexts, $2^{67.39}$ encryptions and $2^{64.91}$ blocks, respectively. Moreover, we also attack 17 rounds of Piccolo-128 by using a 7-round distinguisher, which requires 2^{44} chosen plaintexts, 2^{126} encryptions and $2^{125.49}$ blocks, respectively. Compared with the previous cryptanalytic results, our results are the currently best ones if considering Piccolo from the first round with the pre-whitening layer.

Keywords: Lightweight Block ciphers, Piccolo, the distinguisher, meet-in-the-middle attacks

This work was supported by National Cryptography Development Fund (Grant No. MMJJ20180202) and Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-17-008).

http://doi.org/10.3837/tiis.2019.09.022 **ISSN : 1976-7277**

1. Introduction

At CHES 2011, K. Shibutani and T. Isobe et al. worked in Sony corporation proposed a lightweight block cipher Piccolo [1]. It employs Generalized Feistel Network (GFN) structure with 64 bits of block length. Piccolo-80 and Piccolo-128 denote 80 bits of key length and 128 bits of key length, respectively. Meanwhile, the key size determines the number of rounds, i.e., 25 rounds for Piccolo-80 and 31 rounds for Piccolo-128. In addition, the pre-whitening and post-whitening layers are appended in order to improve its security. Since it was proposed, Piccolo has been evaluated by three cryptanalytic methods, i.e., impossible differential attacks, biclique cryptanalysis and meet-in-the-middle attacks. As for impossible differential cryptanalysis of Piccolo, K. Shibutani and T. Isobe attacked Piccolo-80 up to 14 rounds and Piccolo-128 up to 21 rounds not including pre-whitening and post-whitening keys in 2012 [2], M. Minier attacked Piccolo-80 up to 14 rounds and Piccolo-128 up to 21 rounds not including pre-whitening and post-whitening keys in the related-key setting in 2003 [3], S. Azimi et al. attacked 12 rounds of Piccolo-80 not including post-whitening keys, 13 rounds of Piccolo-80 not including pre- and post- whitening keys and 15 rounds of Piccolo-128 not including pre-whitening keys in 2004 [4]. As for meet-in-the-middle attack on Piccolo, M. Tolba et al. attacked 14 rounds of Piccolo-80 not including pre-whitening and post-whitening keys and 17 rounds of Piccolo-128 including post-whitening keys in 2005 [5], Y. Liu et al. attacked 14 rounds of Piccolo-80 not including pre-whitening and post-whitening layers and 18 rounds of Piccolo-128 including post-whitening layer in 2017 [6], respectively. Although T. Isobe and K. Shibutani could attack more rounds than other results, these attacks required full code book or more. Clearly, it is impractical. In addition, these results analyzed the security of reduced-round Piccolo which cannot start from the first round (round 0) except paper [4]. In addition, there are some other results on bruteforce-like cryptanalysis [7-13].

Diffie and Hellman presented the meet-in-middle attack in 1977. After that, it attracted fewer attentions of researchers because it only broke less rounds of block ciphers. However, since K. Aoki et al. applied it for attacking several hash functions such as reduced versions of SHA-0/1 and MD5 in 2008, the meet-in-the-middle attack has paid more attentions again and improved further to exploit the security of several block ciphers, for example Camellia, AES, Kasumi, TWINE etc. There are two research lines about this attack. First, researchers split a block cipher E_K into two sub-ciphers E_{K_1} and E_{K_2}, i.e., $E = E_{K_2} \circ E_{K_1}$. For a chosen plaintext-ciphertext (P,C), the adversary guesses the value of $K_1 \| K_2$. If $E_{K_1}(P) = E_{K_2}^{-1}(C)$, then the guessed key might be right. Otherwise, it must be wrong. Taking enough plaintext-ciphertexts, the right key should be recovered. However, it is difficult to attack a large number of rounds by using this research idea. Thus, some skills including initial structure [14] and splic-and-cut [15] were proposed to improve the results. Second, Demirci and Selçuk studied this method further to improve cryptanalysis of reduced round AES-256 [16]. They treated a block cipher E_K as $E_K = E_{K_2} \circ E_{K_m} \circ E_{K_1}$. In E_{K_m}, a distinguisher would be constructed in the offline phase. Then the subkeys K_1 and K_2 would be guessed and verified whether they satisfied the distinguisher or not. If so, the guessed subkeys (K_1,K_2) might be correct. According to this method, some wrong subkeys (K_1,K_2) will be removed. However, this attack requires a great deal of storage to perserve the precomputation table. To overcome this weakness, researchers proposed some skills such as multisets [17], differential

enumeration [17], efficient tabulation [18] and a key-dependent sieve [19]. Moreover, J. Guo et al. evaluated the security of generic Feistel constructions by applying meet-in-the-middle attacks [20-22].

In this submission, we put forward meet-in-the-middle attacks on Piccolo-80 up to 13 rounds and Piccolo-128 up to 17 rounds, which starts from round 0 and contain the pre-whitening layer. For Piccolo-80, we append three rounds and five rounds before and after the 5-round distinguisher proposed in [6], respectively. Based on this attack path, we attack 13 rounds of Piccolo-80 with 2^{44} chosen plaintexts, $2^{67.39}$ encryptions and $2^{64.91}$ blocks. For Piccolo-128, we add three rounds and seven rounds before and after the 7-round distinguisher constructed in [6], respectively. On the basis of it, 17 rounds of Piccolo-128 was attacked, which requires 2^{44} chosen plaintexts, 2^{126} encryptions and $2^{125.49}$ blocks, respectively. Our results achieve the best ones if only considering Picoolo from the first round including the pre-whitening layer. In our attacks, we shift the pre-whitening keys from the round 0 to the round 1, and apply the linear relations among round subkeys and the diffusion property of linear operation, which result in the decrease of the complexity. We give all results on Piccolo in the single-key scenario except some results on biclique cryptanalysis in **Table 1**. Among them, some results without noting ‡ are about some variants of Piccolo from the middle round.

From Table 1, we can obtain some results as follows. First, the attacks in paper [2] require full codebook. It is impractical. Second, in papers [5,6] they attacked reduced-versions Piccolo-80/128 not starting from the round 0 and not considering the pre-whitening keys. Third, in paper [4] they only attacked 12-round Piccolo-80 for the same reduced-version Piccolo-80 with ours, while we can attack 13 rounds. Meanwhile, they also attacked 13 rounds of Piccolo-80 not including pre-whitening layer and 15 rounds of Piccolo-128 including post-whitening keys. If they put forward impossible differential cryptanalysis of Piccolo-80 up to 13 rounds including pre-whitening keys, they cannot apply the linear relations among the round subkeys and the early abort technique fully. Therefore, our attacks obtain the currently known best attack on Piccolo-80/128 from the round 0 with pre-whitening keys. These reduced-version Piccolo keeps the property of original Piccolo. Our results show the weakness of original Piccolo to some extend.

Table 1. Results on Piccolo-80/128 in the single key scenario not including biclique cryptanalysis

Key Length	Rounds	Attack Methods	Pre/Post-whitening layers	Time (Encryptions)	Date	Memory (blocks)	Source
Piccolo-80	14	MITMA	None	2^{73}	2^{64}*	2^{5}	[2]
	12	IDC	Pre	$2^{55.18}$	$2^{36.34}$CC	2^{63}	[4]
	13‡	IDC	None	$2^{69.7}$	$2^{43.25}$CP	2^{62}	[4]
	14	MITMA	None	$2^{75.39}$	2^{48}CP	$2^{73.49}$	[5]
	14	MITMA	None	$2^{67.44}$	2^{52}CP	$2^{64.91}$	[6]
	13‡	MITMA	Pre	$2^{67.39}$	2^{44}CP	$2^{64.91}$	Section 3
Piccolo-128	21	MITMA	None	2^{121}	2^{64}*	2^{6}	[2]
	15	IDC	Post	$2^{125.4}$	$2^{58.7}$CP	2^{61}	[4]
	16	MITMA	Post	2^{123}	2^{48}CP	$2^{113.49}$	[5]
	17	MITMA	Post	$2^{126.87}$	2^{48}CP	$2^{125.99}$	[5]

	18	MITMA	Post	$2^{126.63}$	2^{52}CP	$2^{125.29}$	[6]
	17‡	MITMA	Pre	2^{126}	2^{44}CP	$2^{125.49}$	Section 4

Rounds: the number of rounds; CC/CP: Chosen Ciphertexts/Chosen Pliantexts;
Pre/Post: Pre/Post-whitening Key; ‡: Piccolo from the first round; *: Requires full codebook;
IDC: Impossible Differential Cryptanalysis; MITMA: Meet-in-the-Middle Attacks.

This paper is organized in the following. In section 2, we introduce the notations and the Piccolo block cipher. In sections 3 and 4, we put forward meet-in-the-middle attacks on 13 rounds of Piccolo-80 and 17 rounds of Piccolo-128, respectively. In section 5, we summarize our results.

2. Preliminaries

2.1 Notations

- P and C denote the plaintext and ciphertext, respectively.
- $W||V$ denotes the concatenation of W and V.
- K_l denotes the l-th 16-bit nibble of K.
- $rk_i||rk_{i+1}$ denots 32 bits of key in round i.
- $wk_0||wk_1$ and $wk_2||wk_3$ denote the pre-whitening and post-whitening keys, respectively.
- X_j denotes the 64-bit input in the j-th round.
- Y_i denotes 64 bits of the state after the F function and the key addtion in the i-th round.
- $X_i[l]$ denotes the l-th nibble of X_i for $0 \leq l < 16$.
- $X_i[s{:}t]$ denotes from s-th to t-th nibbles of X_i for $s < t$.
- X_i[s,t] denotes the s-th and t-th nibbles of X_i.
- ΔX_i and $\Delta X_i[j]$ denote the differences of a state X_i and a nibbble $X_i[j]$, respectively.
- X_i^j denotes the j-th value of X_i in the i-th round.

2.2 Piccolo

The Piccolo block cipher adopts a GFN structure with the 64-bit block. It has two kinds of the key lengh and the number of round. Piccolo-80 has 80 bits of key size with 25 rounds, and Piccolo-128 has 128 bits of key size with 31 rounds. Their round functions consist of two Feistel Networks including a F-function and a key addition operation. In addition, the designers added the pre-whitening and post-whitening layers at the begining and at the end of the block cipher to improve its security. The encryption procedure can be shown in **Fig. 1**.

The Encryption Procedure.

- $P = X_0 = x_0||x_1||x_2||x_3$,
- $x_0 = x_0 \oplus wk_0$, $x_2 = x_2 \oplus wk_1$
- For $i = 0$ to $r - 2$, do
  - $y_0 = x_0$, $y_1 = x_1 \oplus F(x_0) \oplus rk_{2i}$,
  - $y_2 = x_2$, $y_3 = x_3 \oplus F(x_2) \oplus rk_{2i+1}$,
  - $x_0||x_1||x_2||x_3 = RP(y_0||y_1||y_2||y_3)$
- end

- $y_0 = x_0 \oplus wk_2$, $y_1 = x_1 \oplus F(x_0) \oplus rk_{2r-2}$,
- $y_2 = x_2 \oplus wk_3$, $y_3 = x_3 \oplus F(x_2) \oplus rk_{2r-1}$.

Here, two 4 × 4-bit S-box layers and a diffusion matrix M constitute F-function, shown in **Fig. 1**. These two S-Boxes are the same and the matrix M operates over a finite field $GF(2^4)$ as follows:

$$(z_0, z_1, z_2, z_3)^t = M \bullet (z_0, z_1, z_2, z_3)^t,$$

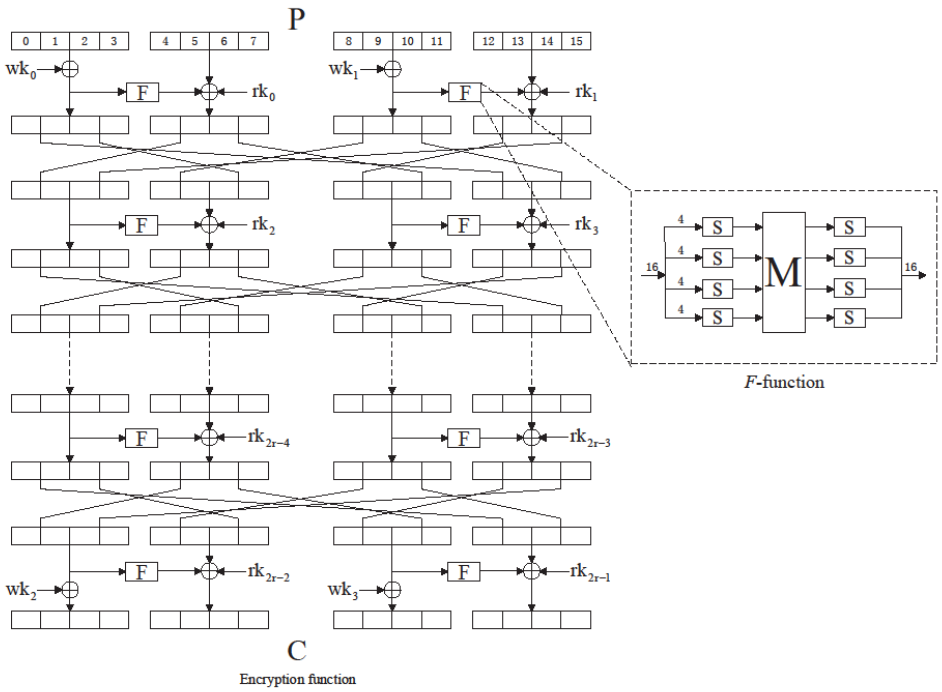

Fig. 1. Structure of Piccolo

The RP round permutation is defined as follows:

$$RP(x_0, x_1, ..., x_7) = (x_2, x_7, x_4, x_1, x_6, x_3, x_0, x_5).$$

Key Schedule. For Piccolo-80, 80 bits of master key are divided into five 16-bit subkeys (k_0, k_1, k_2, k_3, k_4). For Piccolo-128, 128 bits of master key are divided into eight 16-bit subkeys (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7). The generating algorithms of whitening keys and round subkeys can be found in [1].

3. Cryptanalysis of 13 Rounds of Piccolo-80 from the First Round

We apply 5 rounds of the meet-in-the-middle distinguisher proposed in [6] to perform an attack on 13 rounds of Piccolo-80 from the round 0 including the pre-whitening keys. Meanwhile, we analyze the complexity.

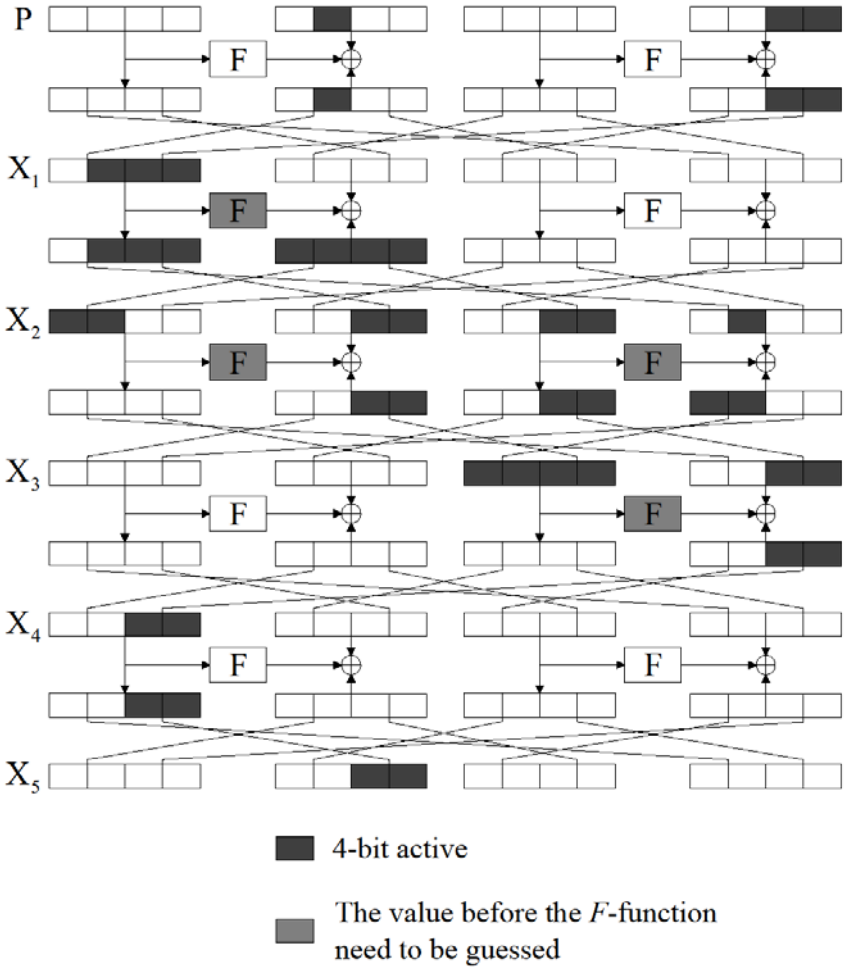

Fig. 2. The 5 Rounds of Meet-in-the-middle Distinguisher for Piccolo-80

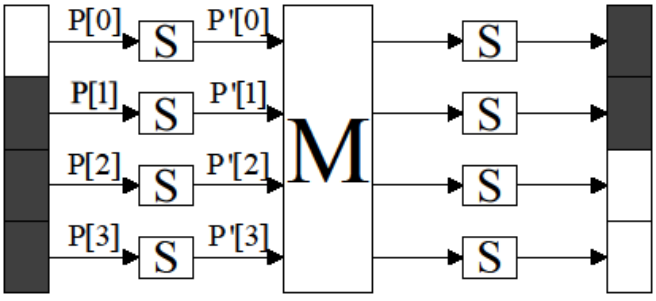

Fig. 3. The diffusion property of M

Proposition 1: [6] Encrypt a δ-set $\{P^0, P^1, ..., P^j\}$ through 5-round Piccolo, where $P^i = X_0^i[5,14,15] \| X_0[0,...,4] \| X_0[6,...,13], (0 \le i \le j)$. Take all possible values of three nibbles $X_0^i[5,14,15]$ and the remaining nibbles take the constants. Then the ordered sequence

$X_5^0[6:7] \oplus X_5^1[6:7]$, $X_5^0[6:7] \oplus X_5^2[6:7]$,…, $X_5^0[6:7] \oplus X_5^j[6:7]$ can be calculated from these variables, i.e., $X_1^0[0:3]$, $X_2^0[0:3]$, $X_2^0[8:11]$ and $X_3^0[8:11]$. In **Fig. 2**, we show the detailed structure.

Lemma 1: [5,6] If the input of linear operation M contains three active nibbles and its output has two active nibbles as shown in **Fig. 3**, then we found the number of such differences is 15 by enumerating all the possible values.

As like paper [6], $j = 15$. Thus there are $2^{4\times16} = 2^{64}$ ordered sequences. In theory, there are $2^{15\times8} = 2^{120}$ possible ones. By using this 5-round distinguisher above, 13 rounds of Piccolo-80 from the rounds 0 to 12 including the pre-whitening keys can be attacked successfully. In our attack, we shift rk_0 and rk_1 from the round 0 to the round 1 to decrease the data complexity, seen in **Fig. 4**. Our attack relies on Lemma 1 and the linear relations among the round subkeys. The attack procedure will be given as follows.

- **The pre-processing phase.** According to Proposition 1, we build a precomputation table H to preserve 2^{64} ordered sequences.
- **The online phase.**
  1. Choose a plaintext P^0. By guessing the pre-whitening keys wk_0 and wk_1, we can compute the value of X_1^0. Next, guess the value of $\left(rk_0^L \| rk_1^R, rk_1^L \| rk_0^R, rk_2^R, rk_3^L\right)$ and calculate $Y_1^0[0:3] \| Y_1^0[6:7] \| Y_1^0[12,13]$. Therefore, we can know the value of $X_2^0[8:13]$. Because $X_3^0[4,5,14,15] = Y_2^0[8:11] = X_2^0[8:11]$, we can get the value of $X_3^0[4,5,14,15]$.
  2. According to 15 differences in Lemma 1, we have obtained $\Delta X_3^i \triangleq X_3^0 \oplus X_3^i$ $(1 \le i \le 15)$, where three nibbles $\Delta X_3^i[5,14,15]$ are non-zero and other nibbles equal zero. So the value of $X_3^i[4,5,14,15] = X_2^i[8:11]$ $(1 \le i \le 15)$ can be computed. Next, the value of $\Delta X_2^i \triangleq X_2^0 \oplus X_2^i$ and $\Delta Y_1^i \triangleq Y_1^i \oplus Y_1^0$ $(1 \le i \le 15)$ can be calculated, too .
  3. Since $Y_1^0[0:3]$ and $\Delta Y_1^i (1 \le i \le 15)$ have been known, the value of $X_1^i \oplus X_1^0$ $\triangleq \Delta X_1^i (1 \le i \le 15)$ can be computed. So the value of $Y_0^i \oplus Y_0^0 \triangleq \Delta Y_0^i (1 \le i \le 15)$ and $\Delta X_0^i (1 \le i \le 15)$ can also be known.
  4. The other 15 plaintexts P^1, P^2,…, P^{15} can be known from the value of $\Delta X_0^i (1 \le i \le 15)$ and P^0.
  5. Ask for the corresponding ciphertexts C^0, C^1,…, C^{15}.
  6. Guess these subkeys rk_{24}, rk_{25}, rk_{22}, rk_{23}, rk_{20}, rk_{21}. Then we can decrypt the ciphertexts C^0, C^1,…, C^{15} to get the value of X_{10}^i (i.e., Y_9^i) $(1 \le i \le 15)$.
  7. Next, guess the value of rk_{18}^R, rk_{19}^L. Then we can compute the value of $X_9^i[6,7,10,11,12,13]$ $(1 \le i \le 15)$. Thus the value of $Y_8^i[0:3]$ $\|$ $Y_8^i[6,7]$ $(1 \le i \le 15)$ can be known. Finally, the ordered sequence $X_8^0[6:7] \oplus X_8^1[6:7]$, $X_8^0[6:7] \oplus X_8^2[6:7]$,…, $X_8^0[6:7] \oplus X_8^j[6:7]$ can be calculated.
  8. We verify whether the ordered sequence is in the precomputation table H or not.

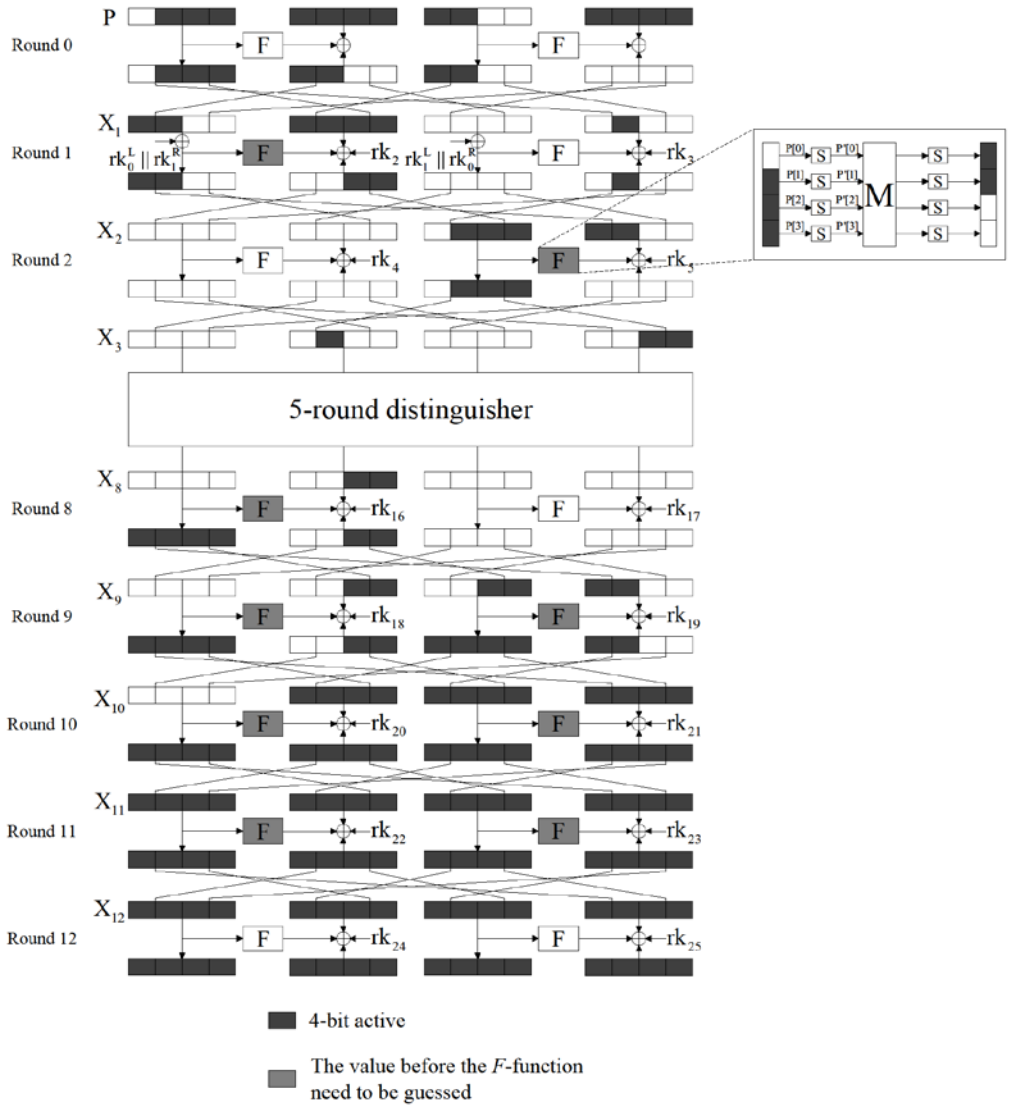

Fig. 4. The attacking path of 13 rounds of Piccolo-80 from the first round with pre-whitening key

During this attack, the subkeys wk_0, wk_1, rk_0, rk_1, rk_2^R, rk_3^L, rk_{18}^R, rk_{19}^L, rk_{20}, rk_{21}, rk_{22}, rk_{23}, rk_{24}, rk_{25}, are guessed. By the key schedule, we find these subkeys are related to k_0, k_1, k_2, k_3, i.e., 2^{64} keys. Thus we expect that only $2^{64-(120-64)} = 2^8$ round subkeys are left after 8 steps. Finally, we retrieve the master key by applying two plaintext-ciphertext pairs.

The memory complexity is determined by the size of H which consists of 2^{64} ordered sequences. Hence, the memory complexity is $2^{64} \times 120/64 \approx 2^{64.91}$ 64-bit blocks. As depicted in **Fig. 4**, we have 2^{28} states in X_1 and decrypt these states to obtain corresponding plaintexts. It is worth noting that $P_0[12:15]$ can be computed by decrypting $Y_0[8:11]$ while no keys will be involved. Hence, the number of $P_0[12:15]$ is equal to the number of $Y_0[8:11]$. In other word,

$P_0[12:15]$ only have 2^8 states. Finally, the data complexity is $2^{12}\times 2^{16}\times 2^8\times 2^8 = 2^{44}$ chosen plaintexts. The time complexity in th pre-processing phase is about $2^{64}\times 16\times 4/(2\times 13)\approx 2^{65.3}$, and the time complexity in the online phase is about $2^{64}\times 16\times(4+9)/(2\times 13)+2\times 2^{(64-(120-64))}\times 2^{16} = 2^{67}+2^{25}$. Totally, the time complexity is $2^{65.3}+2^{67.1}+2^{25}\approx 2^{67.39}$ 13-round Piccolo-80 encryptions.

4. Cryptanalysis of 17 Rounds of Piccolo-128 from the First Round

Similarly, we use 7 rounds of distinguisher proposed in [6] to attack 17 rounds of Piccolo-128 from the rounds 0 to 16 including the pre-whitening keys. In [6], the authors constructed a 7-round distinguisher as follows. In **Fig. 5**, we depict it in detail.

Proposition 2: [6] Encrypt the δ-set $\{P^0, P^1, ..., P^j\}$ through 7-round Piccolo, where $P^i = X_0^i[5,14,15] \,||\, X_0^i[0,...,4] \,||\, X_0^i[6,...,13]$ $(0\le i\le j)$. Take all possible vaues of three nibbles $X_0^i[5,14,15]$ $(0\le i\le j)$ and the other nibbles are taken constants. Then the ordered sequence $X_7^0[5:7]\oplus X_7^1[5:7]$, $X_7^0[5:7]\oplus X_7^2[5:7]$,..., $X_7^0[5:7]\oplus X_7^j[5:7]$ is calculated from the following parameters $X_1^0[0:3]$, $X_2^0[0:3]$, $X_2^0[8:11]$, $X_3^0[0:3]$, $X_3^0[8:11]$, $X_4^0[0:3]$, $X_4^0[8:11]$ and $X_5^0[8:11]$ fully.

Similarly, j = 15. Meanwhile, we obtain $2^{8\times 16} = 2^{128}$ 180-bit ordered sequences. In theory, there are the $2^{15\times 8} = 2^{180}$ possible ones.

On the basis of 7-round distinguisher above, we attack on Piccolo-128 from round 0 to round 16 including the pre-whitening key. As like Section 3, rk_0 and rk_1 are shifted from the round 0 to the round 1 equivalently. In **Fig. 6**, we list the attacking path. The attack procedure contains the proprocessing phase and the online phase. In the pre-processing phase, we construct a pre-computation table to preserve the ordered sequence $X_{10}^0[5:7]\oplus X_{10}^1[5:7]$, $X_{10}^0[5:7]\oplus X_{10}^2[5:7]$,..., $X_{10}^0[5:7]\oplus X_{10}^{15}[5:7]$. In the online phase, select some plaintext-ciphertexts, encrypt or decrypt them and verify whether they satisfy H' or not. We simply give this attacking procedure as follows.

- **The preprocessing phase.** According to Proposition 2, we build a hash table H' to store all 2^{128} 180-bit ordered sequences.
- **The online phase.**
  1. Take one plaintext P^0.
  2. Guess these round subkeys wk_0, wk_1, rk_0, rk_1, rk_2^R and rk_3^L to obtain a δ-set P^0, P^1,..., P^{15}.
  3. Encrypt these plaintexts to get the corresponding ciphertexts C^0, C^1,..., C^{15}.
  4. Guess these round keys rk_{22}^R, rk_{22}^L, rk_{24}, rk_{25},..., rk_{30}, rk_{31}, rk_{32} and rk_{33}. Decrypt these ciphertexts to calculate the ordered sequences $X_{10}^0[5:7]\oplus X_{10}^1[5:7]$, $X_{10}^0[5:7]\oplus X_{10}^2[5:7]$,..., $X_{10}^0[5:7]\oplus X_{10}^{15}[5:7]$.
  5. Finally, check whether the ordered sequences belong to the table H' or not.

By the key schedule, we found that wk_0, wk_1, rk_0, rk_1, rk_2^R, rk_3^L, rk_{22}^R, rk_{23}^L, rk_{24}, rk_{25},…, rk_{30}, rk_{31}, rk_{32} and rk_{33} are determined by seven and half keys k_0, k_1, k_2, k_3, k_4^R, k_5, k_6, and k_7. The detailed relations can be found in **Table 2**.

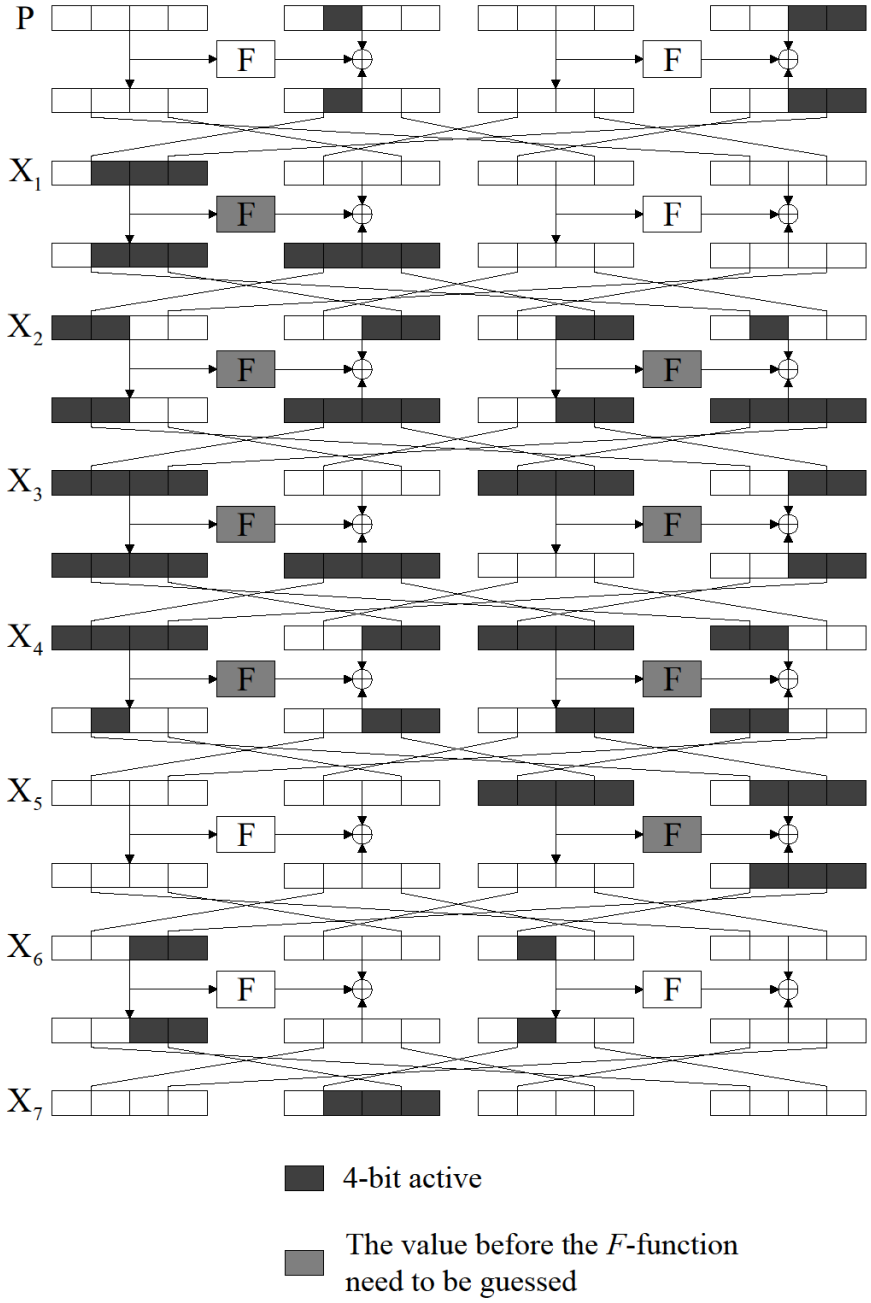

Fig. 5. The 7 Rounds of Distinguisher of Piccolo-128

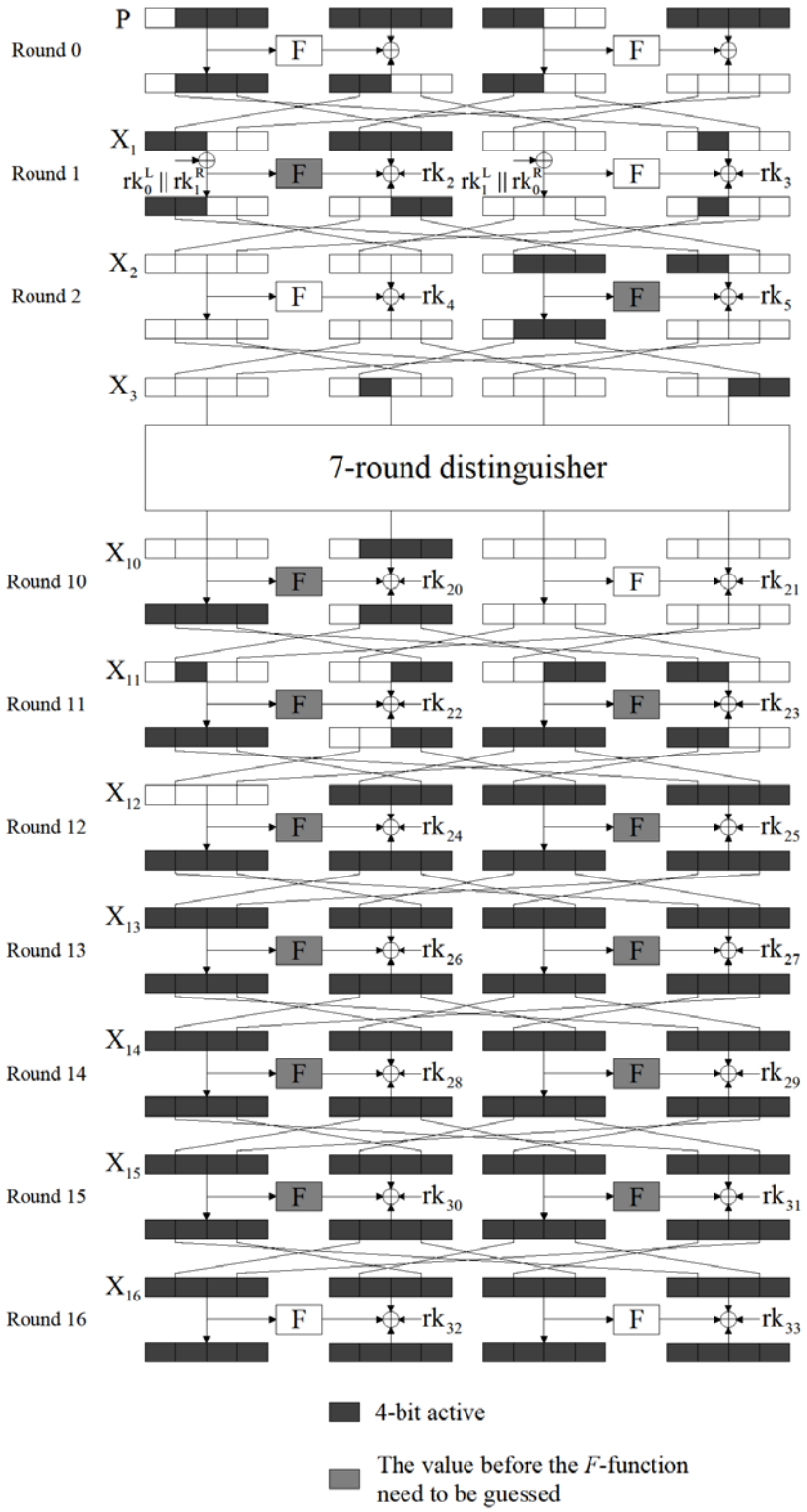

Fig. 6. The attacking path of 17 rounds of Piccolo-128 from the first round with the pre-whitening keys

rk_{25},…, rk_{30}, rk_{31}, rk_{32} and rk_{33} are determined by seven and half keys k_0, k_1, k_2, k_3, k_4^R, k_5, k_6, and k_7. The detailed relations can be found in **Table 2**.

We estimate that the memory complexity is $2^{8\times16}\times(15\times12)/64\approx2^{129.49}$ blocks. In order to decrease it, we can employ the time-memory trade-off skill. We choose a factor $\alpha = 2^4$. So the memory complexity can be decrease to $2^{125.49}$ blocks. The time complexity in the preprocessing phase is about $2^{128-4}\times16\times8/(2\times17)\approx2^{123.5}$. In order to reduce the time complexity in the online phase, we compute the intermediate states step by step. By guessing the values of k_2, k_3, k_4^R and k_5^L, we identify the value of δ-set, which requires about $2^{48}\times16\times4/(2\times17)\approx2^{48.91}$ encryptions. Then, we decrypt round 16 by guessing k_7, which requires about $2^{48+16}\times16\times2/(2\times17)\approx2^{63.91}$. Next, by guessing k_0, k_1, we can decrypt round 14 and round 15, which requires about $2^{64+32}\times16\times4/(2\times17)\approx2^{96.91}$. Fourth, by guessing k_6 and k_5^R, we can calculate the ordered sequence, which needs $2^{96+24}\times16\times7/(2\times17)\approx2^{121.72}$ encryptions. In all, the time complexity in the online phase is about $2^{48.91}+2^{63.91}+2^{96.91}+2^{121.72}\approx2^{121.72}$. Since we use the time and memory trade-off and take the factor $\alpha = 2^4$, the time complexity of our attack is about $2^{125.72}$. In order to retrieve the master key, we use two plaintext-ciphertexts to verify whether it is correct, which requires $2\times2^{120}\times2^{128-180}\times2^8=2^{77}$ encryptions. Finally, the time complexity is $2^{123.5}+2^{125.72}+2^{77}\approx2^{126}$ encryptions in total. In addition, this attack requires 2^{44} chosen plaintexts.

Table 2. Relations between Subkeys and Master Key for Piccolo-128

subkey	MK	subkey	MK
rk_0	k_2	rk_1	k_3
rk_2^R	k_4^R	rk_3^L	k_5^L
rk_{22}^R	k_4^R	rk_{23}^L	k_1^L
rk_{24}	k_0	rk_{25}	k_3
rk_{26}	k_6	rk_{27}	k_5
rk_{28}	k_2	rk_{29}	k_7
rk_{30}	k_0	rk_{31}	k_1
rk_{32}	k_2	rk_{33}	k_7
wk_0	$k_0^L \parallel k_1^R$	wk_1	$k_1^L \parallel k_0^R$

MK: Master Key

5. Conclusion

This paper first studies the diffusion properties of the linear operations *M* and *RP* and the linear relations among the round subkeys. Then, we apply a 5-round distinguisher and a 7-round distinguisher proposed in [6] to attack Piccolo-80 up to 13 rounds and Piccolo-128 up to 17 rounds, respectively. Their data complexities are the same, i.e., 2^{44} chosen plaintexts. However, their time and memory complexities are different. The adversary requires $2^{67.39}$ encryptions and $2^{64.91}$ blocks in order to attack 13 rounds of Piccolo-80, and 2^{126} encryptions and $2^{125.49}$ blocks in order to attack 17 rounds of Piccolo-128. These results show the

vulnerability of original Piccolo-80/128.

References

[1] Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita and Taizo Shirai, "Piccolo: An Ultra-Lightweight Blockcipher," in *Proc. of 13th Cryptographic Hardware and Embedded Systems*, pp. 342-357, September 28 - October 1, 2011. Article (CrossRef Link).

[2] Takanori Isobe and Kyoji Shibutani, "Security Analysis of the Lightweight Block Ciphers XTEA, LED and Piccolo," in *Proc. of 17th Australasian Conference on Information Security and Privacy*, pp. 71-86, July 9-11, 2012. Article (CrossRef Link).

[3] Marine Minier, "On the Security of Piccolo Lightweight Block Cipher against Related Key Impossible Differentials," in *Proc. of 14th International Conference on Cryptology in India*, pp. 308-318, December 7-10, 2013. Article (CrossRef Link).

[4] Seyyed Arash Azimi, Zahra Ahmadian, Javad Mohajeri and Mohammad Reza Aref, "Impossible Differential Cryptanalysis of Piccolo Lightweight Block Cipher," in *Proc. of 11th International ISC Conference on Information Security and Cryptology*, pp. 3-20, September 15-18, 2014. Article (CrossRef Link).

[5] Mohamed Tolba, Ahmed Abdelkhalek and Amr M Youssef, "Meet-in-the-Middle Attacks on Reduced Round Piccolo," in *Proc. of 4th International Workshop on Lightweight Cryptography for Security & Privacy*, pp. 3-20, September 10-11, 2015. Article (CrossRef Link).

[6] Ya Liu, Liang Cheng, Zhiqiang Liu, Wei Li, Qingju Wang and Dawu Gu, "Improved Meet-in-the-Middle Attacks on Reduced-Round Piccolo," *SCIENCE CHINA Information Science*, vol. 61, no. 3, pp. 321-329, 2017. Article (CrossRef Link).

[7] JiaLin Huang and XueJia Lai, "What is the effective key length for a block cipher: an attack on every practical block cipher," *SCIENCE CHINA Information Science*, vol. 57, no. 7, pp. 1-11, 2014. Article (CrossRef Link).

[8] Kitae Jeong, Hyungchul Kang, Changhoon Lee, Jaechul Sung and Seokhie Hong, "Biclique Cryptanalysis of Lightweight Block Ciphers PRESENT, Piccolo and LED," *IACR Cryptology ePrint Archive*, vol. 2012, pp. 621-648, 2012. Article (CrossRef Link).

[9] Yanfeng Wang, Wenling Wu and Xiaoli Yu, "Biclique Cryptanalysis of Reduced-Round Piccolo Block Cipher," in *Proc. of 10th Information Security Practice and Experience Conference*, pp. 337-352, 2012. Article (CrossRef Link).

[10] Siavash Ahmadi, Zahra Ahmadian, Javad Mohajeri, and Mohammad Reza Aref, "Low-Data Complexity Biclique Cryptanalysis of Block Ciphers With Application to Piccolo and HIGHT," *IEEE Trans. Information Forensics and Security*, vol. 9, no. 10, pp. 1641-1652, 2014.

[11] Kitae Jeong, "Cryptanalysis of block cipher Piccolo suitable for cloud computing," *The Journal of Supercomputing*, vol. 66, no.2, pp. 829-840, 2013. Article (CrossRef Link).

[12] Junghwan Song, Kwanhyung Lee and Hwanjin Lee, "Biclique Cryptanalysis on Lightweight Block Cipher: HIGHT and Piccolo," *International Journal of Computer Mathematics*, vol. 90, no. 12, pp. 2564-2580, 2013. Article (CrossRef Link).

[13] Zheng Gong, Shusheng Liu, Yamin Wen, Yiyuan Luo and Weidong Qiu, "Biclique cryptanalysis using balanced complete bipartite subgraphs," *SCIENCE CHINA Information Sciences*, vol. 59, no. 4, pp. 1-3, 2016. Article (CrossRef Link).

[14] Yu Sasaki and Kazumaro Aoki, "Finding preimages in full MD5 faster than exhaustive search," in *Proc. of EUROCRYPT 2009*, pp. 134-152, April 26-30, 2009. Article (CrossRef Link).

[15] Kazumaro Aoki and Yu Sasaki, "Preimage attacks on one-block MD4, 63-step MD5 and more," in *Proc. of 15th International Workshop SAC*, pp. 103-119, August 14-15, 2008. Article (CrossRef Link).

[16] Hüseyin Demirci and Ali Aydın Selçuk, "A Meet-in-the-Middle Attack on 8-Round AES," in *Proc. of 15th International Conference on Fast Software Encryption*, pp. 116-126, February 10-13, 2008. Article (CrossRef Link).

[17] Orr Dunkelman, Nathan Keller and Adi Shamir, "Improved Single-Key Attacks on 8-Round AES-192 and AES-256," in *Proc. of ASIACRYPT 2010*, pp. 158-176, December 5-9, 2010. Article (CrossRef Link).
[18] Patrick Derbez, Pierre-Alain Fouque and Jérémy Jean, "Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting," in *Proc. of EUROCRYPT 2013*, pp. 371-387, May 26-30, 2013. Article (CrossRef Link).
[19] Leibo Li, Keting Jia and Xiaoyun Wang, "Improved Single-Key Attacks on 9-Round AES-192/256," in *Proc. of 21st International Conference on Fast Software Encryption*, pp. 127-146, March 3-5, 2014. Article (CrossRef Link).
[20] Jian Guo, Jérémy Jean, Ivica Nikolic and Yu Sasaki, "Meet-in-the-Middle Attacks on Generic Feistel Constructions," in *Proc. of Asiacrypt 2014*, pp. 458-477, December 7-11, 2014. Article (CrossRef Link).
[21] Jian Guo, Jérémy Jean, Ivica Nikolić and Yu Sasaki a, "Extended meet-in-the-middle attacks on some Feistel constructions," *Designs Codes & Cryptography*, vol. 80, no. 3, pp. 587-618, 2016. Article (CrossRef Link).
[22] Jian Guo, Jérémy Jean, Ivica Nikolić and Yu Sasaki, "Meet-in-the-Middle Attacks on Classes of Contracting and Expanding Feistel Constructions," *IACR Transactions on Symmetric Cryptology*, vol. 2016, no. 2, pp. 307-377, 2017. Article (CrossRef Link).

Ya Liu received M.S. degree from Anhui Normal University in 2004 and Ph.D. degree from Shanghai Jiao Tong University in 2013. She is currently a lecturer in Department of Computer Science and Engineering, University of Shanghai for Science and Technology. Her research interests include applied cryptography, network security, cloud computing, the design and analysis of symmetric ciphers and computational number theory.

Liang Cheng received his B.S. degree from Jilin Business and Technology College in 2015. He is currently a graduate student in Department of Computer Science and Engineering, University of Shanghai for Science and Technology. His research interests mainly include the analysis of block ciphers.

Fengyu Zhao received his M.S. degree from Nanjing University of Aeronautics and Astronautics in 1989 and Ph.D. degree from Fudan University in 2010. He is currently a professor in Department of Computer Science and Engineering, University of Shanghai for Science and Technology. His research interests mainly include software engineer and web security.

Chunhua Su received the B.S. degree for Beijing Electronic and Science Institute in 2003 and received his M.S. and PhD of computer science from Faculty of Engineering, Kyushu University in 2006 and 2009, respectively. He is currently working as an Associate Professor in Division of Computer Science, University of Aizu. He has worked as a research scientist in Cryptography and Security Department of the Institute for Infocomm Research, Singapore from 2011-2013. From 2013-2016, he has worked as an Assistant professor in School of Information Science, Japan Advanced Institute of Science and Technology. From 2016-2017, he worked as an Assistant Professor in Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in data mining and IoT security and privacy.

Zhiqiang Liu received his M.S. and Ph.D degrees from Shanghai Jiao Tong University in 1998 and 2012, respectively. He is currently an associate professor in Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests mainly include block chain and symmetric ciphers.

Wei Li received his M.S. and Ph.D degrees from Shanghai Jiao Tong University in 2005 and 2009, respectively. She is currently an associate professor in Department of Computer Science and Engineering, Donghua University. Her research interests mainly include the design and analysis of symmetric ciphers.

Dawu Gu received his M.S and Ph.D degrees from Xidian university of China in 1995 and 1998. He is a professor at Computer Science and Engineering Department, Shanghai Jiao Tong University. He serves as a technical committee members for China Association of Cryptologic Research (CACR) and China Computer Federation (CCF), also as the members of ACM, IACR, and IEICE. He was the winner of New Century Excellent Talent Program made by Ministry of Education of China in 2005. He has been invited as chairs and TPC members for many international conferences like E-Forensics, ISPEC, ICIS, ACSA, CNCC, etc. His research interests cover cryptology and computer security. He has received more than 100 scientific papers in academic journals and conferences.