SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2016)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1644

RESEARCH ARTICLE

Multidimensional zero-correlation linear cryptanalysis of lightweight block cipher Piccolo-128

Li-shi Fu*, Chen-hui Jin and Xin-ran Li

Zhengzhou Information Science and Technology Institute, Zhengzhou, Henan, China

ABSTRACT

Piccolo is a lightweight block cipher proposed at CHES 2011. This paper firstly gives the zero-correlation linear approximations over 7-round Piccolo and studies the security of Piccolo-128 against multidimensional zero-correlation linear cryptanalysis. Based on the statistic used in multidimensional linear cryptanalysis to detect the right key and wrong keys, this paper gives the data complexity when using this statistic in multidimensional zero-correlation linear cryptanalysis. Finally, with partial sum technique and the relation between the round keys in Piccolo-128, the first known-plaintexts attacks on round 0–12/round, 15–28/round, and 14–28 of Piccolo-128 are proposed; the data complexities of those attacks are $2^{56.8}/2^{52.43}/2^{55.6}$ known plaintexts, respectively; and the time complexities are $2^{117.2}, 2^{123.09}, 2^{126.55}$, respectively. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS
lightweight block cipher; Piccolo block cipher; multidimensional zero-correlation linear cryptanalysis; partial sum technique

***Correspondence**
Li-shi Fu, Zhengzhou Information Science and Technology Institute, Zhengzhou,450000 Henan, China.
E-mail: 15036018167@163.com

1. INTRODUCTION

Recently, with the development of the Internet, wireless sensor networks and radio frequency technology are widely used. Because the computing power of those equipments is limited, the traditional block cipher cannot run smoothly in those equipments, hence a great number of lightweight block ciphers are proposed up to adjust to those equipments. The lightweight block cipher Piccolo[1] was proposed by Shibutani *et al.* at CHES 2011, whose block size is 64-bit. Piccolo family has two versions: Piccolo-80 and Piccolo-128 according to the different key sizes.

Because Piccolo was proposed up, lots of cryptanalytic results on Piccolo have been proposed, such as Biclique attack[2–5], meet-in-the-middle attack[6,7], impossible differential attack[8], related impossible differential attack[9], and so on. [2–5] studied the ability of Piccolo against Biclique attack; the best Biclique attack was proposed in [3] by Ahmadi *et al.* in 2013. Because the time complexity of Biclique attack is close to that of the brute force attack, many researchers take Biclique attack as a brute force-like attack. Isobe *et al.* proposed meet-in-the-middle attacks on 14-round Piccolo-80 and 21-round Piccolo-128 with the whole codebook in 2012 [6]. Afterwards, Tolba *et al.* proposed the meet-in-the-middle attack on 14-round-reduced Piccolo-80 and 16, 17-round-reduced Piccolo-128 without taking advantage of the whole codebook at LightSec 2015 [7]. Wu *et al.* gave the 7-round impossible differentials of Piccolo at Indocrypt 2012 [10]; based on one of the 7-round impossible differentials in [10], Ahmadi *et al.* attacked 13-round Piccolo-80 and 15-round Piccolo-128 at ISCISC 2014 [8]. At Indocrypt 2013, Minier presented the related-key impossible differential attack on 14-round Piccolo-80 and 21-round Piccolo-128[9].

However, there is no cryptanalysis based upon zero-correlation method on Piccolo. This paper mainly studies the security of Piccolo-128 against multidimensional zero-correlation linear cryptanalysis. The former attacks are all chosen-plaintexts attacks on Piccolo, whereas the attacks presented in this paper are the first known-plaintexts attacks on Piccolo-128 so far.

In 2011, Bogdnov and Rijmen proposed a new technique called zero-correlation linear cryptanalysis [11] for the first time. Zero-correlation linear cryptanalysis can be seen as the dual technique of impossible differential attack in linear cryptanalysis area. Zero-correlation linear cryptanalysis is similar to linear cryptanalysis because they both adopt appropriate statistics to distinguish the right key from wrong keys. Zero-correlation linear cryptanalysis uses linear approximations with zero-correlation coefficient to distinguish the correct key and wrong keys whereas linear cryptanalysis uses linear approximations with high correlation coefficient. So far, linear cryptanalysis has been used to attack many ciphers, such as Simon[12,13], SMS4[14], and so on. In zero-correlation linear cryptanalysis, attackers firstly need to find a linear approximation with zero-correlation coefficient. Afterwards, attackers guess some key bits, partially encrypt and decrypt the plaintext-ciphertext pairs to the boundaries of the zero-correlation linear approximation, then compute the correlation coefficient of the given linear approximation, and detect whether the correlation coefficient is zero. Attackers only keep the key guesses, which lead the correlation coefficient of the given linear approximation to be zero.

Initial zero-correlation linear cryptanalysis only takes advantage of one zero-correlation linear approximation, and the data complexity is half of the whole codebook. In order to reduce the data complexity, [15] proposed multiple zero-correlation linear cryptanalysis, which needed the zero-correlation linear approximations to be independent from each other. However, the restriction of multiple zero-correlation linear cryptanalysis is hardly satisfied in reality. Furthermore, Bogdanov in [16] proposed multidimensional zero-correlation linear cryptanalysis, which can further reduce the data complexity. Meanwhile, multidimensional zero-correlation linear cryptanalysis does not need the zero-correlation linear approximations to be independent from each other. So far, multidimensional zero-correlation linear cryptanalysis has been used to analyses HIGHT[17], E2[18], Camellia[19], CLEFIA[19], LBlock[20], and TWINE[20].

Our multidimensional zero-correlation cryptanalysis adopts the statistic T_K used by Hermlin *et al.* in multidimensional linear cryptanalysis[21], which is different from the statistic in [16]. Under the guessed key K, T_K follows a non-central χ^2 distribution $\chi^2_{2^m-1}(NC(p))$. If $2^m - 1 > 30$; then $\chi^2_{2^m-1}(NC(p))$ can be approximated by a normal distribution, whose mean is $2^m - 1 + NC(p)$ and variance is $2 \times (2^m - 1 + 2NC(p))$, where N is the number of data and $C(p)$ is the capacity of probability distribution z^K, where $z^K = \left(z_0^K, \cdots, z_{m-1}^K\right), z_i^K = v_i \cdot x_K \oplus w_i \cdot y_K. v_i \rightarrow w_i (0 \leq i \leq m - 1)$ are m basis zero-correlation linear approximations; x_K, y_K are obtained by partially encrypting and decrypting the plaintext-ciphertext pair with guessed key K. Then attackers set the probability to wrongfully discard the right key guess (i.e., θ_0) and the probability to wrongfully accept a wrong key guess as the right key(i.e., θ_1) and compute the number of data (i.e., N) needed in multidimensional zero-correlation linear cryptanalysis.

This paper firstly presents the zero-correlation linear approximations over 7-round of Piccolo based on the fact that the branch number of the linear layer P in F-Function of Piccolo is 5. Hereafter, combining with partial sum technique, multidimensional zero-correlation linear cryptanalyses on Piccolo are given. Besides, by observation, it is easy to find that the round keys in round 26 and round 28 are the same. The total number of master key bits involved in round 16, round 17, round 25, to round 28 in Piccolo-128 is 80, so this paper chooses to attack rounds 15–28 instead of rounds 0–13 in Piccolo-128, for the time complexity of the latter exceeds 2^{128}. Similarly, this paper chooses to attack rounds 14–28 instead of rounds 0–14 in Piccolo-128 because the round keys in round 14 and round 16 are the same. Our results along with the previous cryptanalyses on Piccolo are shown in Table I.

Table I. Summary of attacks on Piccolo.

Method	Version	Round	Data	time	Ref
MIMD	P-80	14	2^{64}CP	2^{73}	[6]
MIMD	P-128	21	2^{64}CP	2^{121}	[6]
MIMD	P-80	14	2^{48}CP	$2^{75.39}$	[7]
MIMD	P-128	17	2^{48}CP	$2^{126.87}$	[7]
ID	P-80	13	$2^{43.25}$CP	$2^{69.7}$	[8]
ID	P-128	15	$2^{58.7}$CP	$2^{125.4}$	[8]
R-ID	P-80	14	$2^{68.19}$CP	$2^{68.19}$	[9]
R-ID	P-128	21	$2^{117.77}$CP	$2^{117.77}$	[9]
MLZC	P-128	13	$2^{56.8}$KP	$2^{117.2}$	Sec 4
MLZC	P-128	14	$2^{52.43}$KP	$2^{123.09}$	Sec 4
MLZC	P-128	15	$2^{55.6}$KP	$2^{126.55}$	Sec 4

Note. R-ID: Related-key impossible differential; ID: Impossible differential; MIMD: Meet in the middle; MLZC: Multidimensional zero-correlation linear cryptanalysis; P-80: Piccolo-80; P-128: Piccolo-128; CP: chosen plaintext; KP: known plaintext.

2. PRELIMINARIES

2.1. Notations

In the sequel, some explanations about the mathematical symbols appeared in this paper are listed.

F: F-Function in Piccolo;

RP: Round-permutation in Piccolo;

X_r: the input of round r, where $r = 0, \cdots, 30$;

Y_r: the input of RP in round r, where $r = 0, \cdots, 30$;

$X_{r,[i]}$: the i-th byte of X_r, where $i = 0, \cdots, 7$;

$X'_{r,[i]}$: $X_{r,[i]}$ xored with round key of round r, where $i = 2, 3, 6, 7$;

$Y'_{r,[i]}$: $Y_{r,[i]}$ xored with round key of round r, where $i = 2, 3, 6, 7$;

$X_{r,[i_1,\cdots,i_m]}$: the i_1-th byte of X_r to i_m-th byte of X_r, where $0 \leq i_1 < i_m \leq 7$;

$X_{r,[i]}[j]$: the j-th bit of $X_{r,[i]}$, where $j = 0, \cdots, 7$;

$F(x)^L$: the left 8-bit blocks of the output of F-Function;

$F(x)^R$: the right 8-bit blocks of the output of F-Function;

Γ_{in}: the input mask of n-bit block cipher E;

Γ_{out}: the output mask of n-bit block cipher E;

Γx^r : the input mask of round r;

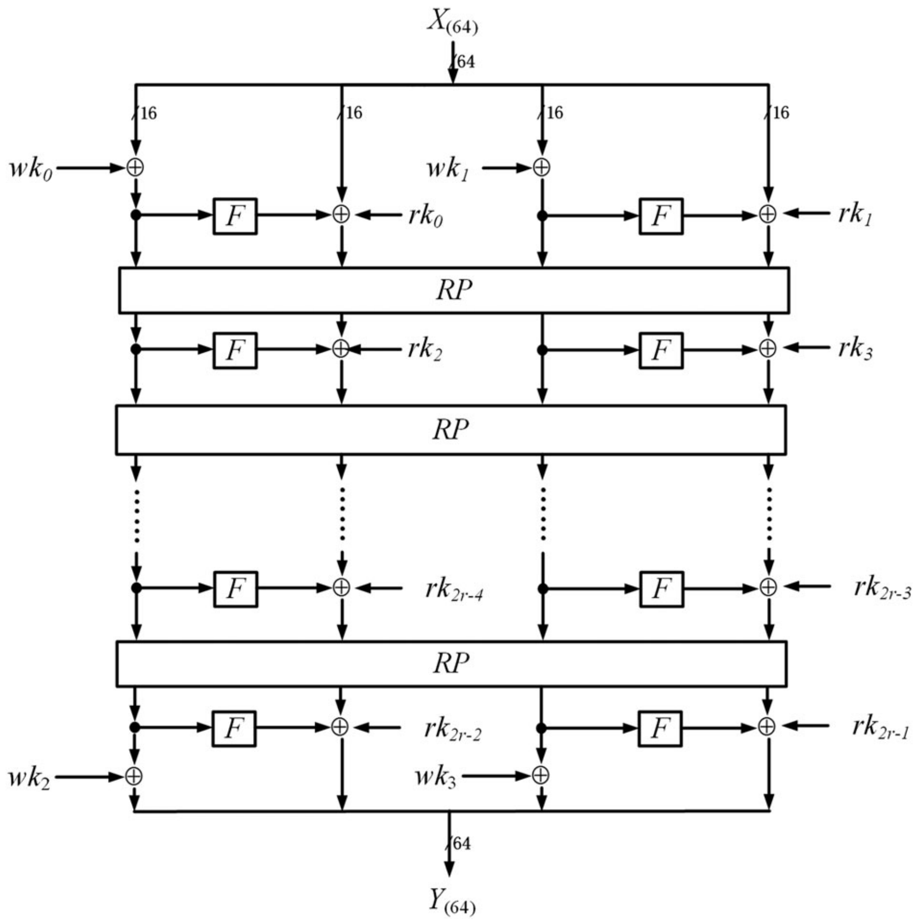

Figure 1. The structure of Piccolo.

Γy^r: the output mask of round r;

Γx_i^r: the i-th 4-bit block of Γx^r, where $i = 0, \cdots, 15$;

Γy_i^r: the i-th 4-bit block of Γy^r, where $i = 0, \cdots, 15$;

$wt(x)$: the number of nonzero components in x;

$V[z]$: the number of times that z occurs;

$C(p, q)$: the capacity between two probability distributions p and q;

N: the data complexity in our attack;

τ : the threshold used to distinguish the right key guess and wrong key guess;

m: the dimension of the zero-correlation linear approximations.

2.2. Brief description of Piccolo

Piccolo adopts generalized Feistel network. It is a 64-bit lightweight block cipher block supporting 80-bit and 128-bit keys. The 80-bit and the 128-bit key modes are denoted as Piccolo-80 and Piccolo-128, respectively. Piccolo-80 iterates 25 rounds whereas Piccolo-128 iterates 31 rounds. The structure of Piccolo is outlined in Figure 1.

The round function of Piccolo consists of F-Function and RP. The F-Function (Figure.2) of Piccolo adopts SPS network, where P is a 4×4 matrix and S is a 4 to 4 nonlinear permutation. The RP (Figure.3) of Piccolo divides four 16-bit blocks into eight 8-bit blocks, and then a linear permutation is applied to those eight 8-bit blocks. Therefore, the input to F-Function in the next round comes from two different 16-bit blocks of the former round, which leads to a higher security level.

In Piccolo-128, wk_0, wk_1 is the whiten key used in the initial round, and wk_2, wk_3 is the whiten key used in the last round. Both the whitening keys and round keys $rk_i (0 \leq i \leq 61)$ are generated from the main key according to the key schedule. The key schedule of Piccolo-128 is listed in Algorithm 1, and the key schedule of Piccolo-80 can refer to [1].

Algorithm 1. *Key schedule for 128-bit key mode. Denote the master key* $K_{(128)} = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$.

```
(i)  $wk_0 = \left(k_0^L, k_1^R\right), wk_1 = \left(k_1^L, k_0^R\right),$
     $wk_2 = \left(k_4^L, k_7^R\right), wk_3 = \left(k_7^L, k_4^R\right).$
(ii) For $i = 0, \cdots, 61$, do:
```

Security Comm. Networks (2016) © 2016 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

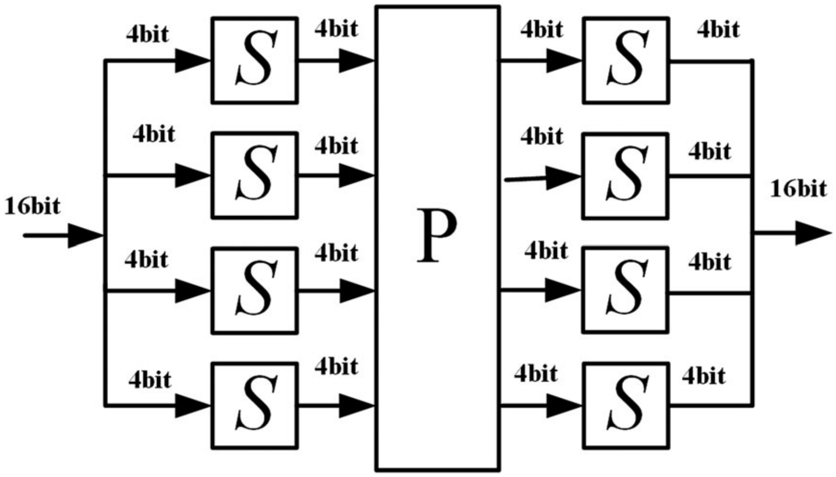

Figure 2. F-Function in Piccolo.

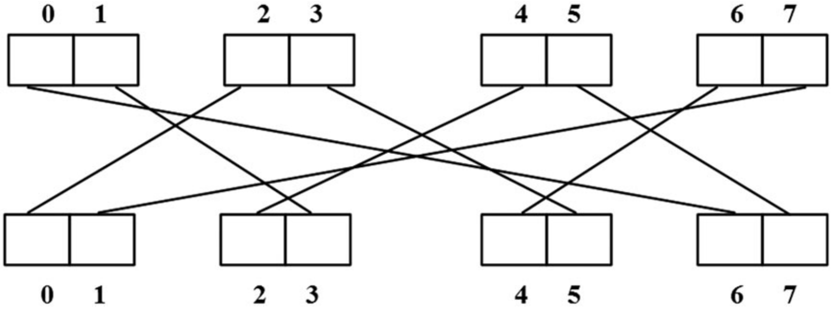

Figure 3. Round-permutation in Piccolo.

If $(i+2)mod8 = 0$*, then*

$$(k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7) \leftarrow (k_2, k_1, k_6, k_7, k_0, k_3, k_4, k_5).$$

$$rk_i \leftarrow k_{(i+2)mod8} \oplus con_i^{128}.$$

Table II lists the round keys in round 0 to round 30 of Piccolo-128.

2.3. Multidimensional Zero-correlation linear cryptanalysis

For a block cipher E with n-bit input, denote its plaintext as P and ciphertext as C, where $\mathrm{C} = E_K(\mathrm{P})$ and K is the key used for encryption.

Definition 1 ([23]). *Let the input mask and output mask of n-bit block cipher E be* Γ_{in} *and* Γ_{out}*, respectively, then the correlation coefficient of* $\Gamma_{in} \to \Gamma_{out}$ *is*

$$c(\Gamma_{in} \to \Gamma_{out}) = 2 \Pr_{\mathrm{P} \in F_2^n}(\Gamma_{in} \cdot \mathrm{P} \oplus \Gamma_{out} \cdot \mathrm{C} = 0) - 1.$$

If $c(\Gamma_{in} \to \Gamma_{out}) = 0$*, then* $\Gamma_{in} \to \Gamma_{out}$ *is called a zero-correlation linear approximation of block cipher E.*

In order to take advantage of the numerous zero-correlation linear approximations to decrease the data complexity, Bogdanov *et al.* in [16] proposed to use multidimensional zero-correlation linear approximations. In multidimensional zero-correlation linear cryptanalysis, attacker uses $2^m - 1$ non-trivial zero-correlation linear approximations generated from m independent zero-correlation linear approximations to attack the block cipher E. Those m independent zero-correlation linear approximations are called the basis zero-correlation linear approximations.

Denote those m basis zero-correlation linear approximations as $v_i \to w_i$, where $i = 0, 2, \cdots, m-1$. Attackers guess some key bits K and partially encrypt and decrypt each plaintext-ciphertext pairs to obtain the boundaries (x_K, y_K) of zero-correlation linear approximations, and then they compute $z^K = \left(z_0^K, \cdots, z_{m-1}^K\right)$, where $z_i^K = v_i \cdot x_K \oplus w_i \cdot y_K$. For $z^K \in F_2^m$, attackers build a counter $V\left[z^K\right]$ and initialize all $V\left[z^K\right]$ to be zero. For N plaintext-ciphertext pairs, compute z^K and increment the counter $V\left[z^K\right]$ of this data value by one.

Table II. Round keys of Piccolo-128

round$i$	$rk_{2i} \oplus con_{2i}^{128}$	$rk_{2i+1} \oplus con_{2i+1}^{128}$
0	k_2	k_3
1	k_4	k_5
2	k_6	k_7
3	k_2	k_1
4	k_6	k_7
5	k_0	k_3
6	k_4	k_5
7	k_6	k_1
8	k_4	k_5
9	k_2	k_7
10	k_0	k_3
11	k_4	k_1
12	k_0	k_3
13	k_6	k_5
14	k_2	k_7
15	k_0	k_1
16	k_2	k_7
17	k_4	k_3
18	k_6	k_5
19	k_2	k_1
20	k_6	k_5
21	k_0	k_7
22	k_4	k_3
23	k_6	k_1
24	k_4	k_3
25	k_2	k_5
26	k_0	k_7
27	k_4	k_1
28	k_0	k_7
29	k_6	k_3
30	k_2	k_5

This paper adopts the statistic T_K used by Hermlin *et al.* in multidimensional linear cryptanalysis [21], which is defined as follows:

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

Lemma 1 ([24]). *$f(x) = (f_1(x), f_2(x), \cdots, f_m(x))$ is a function from Z_2^n to Z_2^m, then $f(x)$ is a balanced function if and only if $f_1(x), f_2(x), \cdots, f_m(x)$ are all balanced Boolean functions and they are independent from each other.*

It is easy to know that under the right key guess *K–right*, for m basis zero-correlation linear approximations $v_i \to w_i$, $z_i^{K-right} = v_i \cdot x_{K-right} \oplus w_i \cdot y_{K-right}$ is balanced. Because those m basis zero-correlation linear approximations are independent from each other, from Lemma 1, it is easy to obtain that $\left(z_0^{K-right}, \cdots, z_{m-1}^{K-right}\right)$ is balanced. Therefore, under the right key guess $K-right$, if the chosen plaintexts fill up the whole codebook, then for any $z^{K-right} \in \{0,1\}^m$, $\frac{V[z^{K-right}]}{N} = \frac{1}{2^m}$. Under the wrong key guess $K-false$, $\frac{V[z^{K\text{-}false}]}{N}$ deviates from $\frac{1}{2^m}$. In [21], Hermelin *et al.* gave the conclusion, which is stated in Lemma 2.

Lemma 2 ([21]). *Under the key guess K, T_K follows a non-central χ^2 distribution $\chi^2_{2^m-1}(NC(p))$. Moreover, when $2^m - 1 > 30$, $\chi^2_{2^m-1}(NC(p))$ can be approximated by a normal distribution, whose mean and variance are*

$$\mu_1 = 2^m - 1 + NC(p), \sigma_1^2 = 2(2^m - 1 + 2NC(p)),$$

where $C(p)$ is the capacity of the probability distribution z^K, N is the data complexity.

Remark 1. In general, multidimensional zero-correlation linear cryptanalysis, because m is always larger than 5, $\chi^2_{2^m-1}(NC(p))$ can be approximated by a normal distribution.

Definition 2 ([22]). *The capacity between two probability distributions $p = (p_0, \cdots, p_{2^m-1}), q = (q_0, \cdots, q_{2^m-1})$ is defined by*

$$C(p,q) = \sum_{\eta=0}^{2^m-1} \frac{(p_\eta - q_\eta)^2}{q_\eta}$$

If q is an unified distribution, then $C(p,q)$ will be denoted by $C(p)$ and called $C(p)$ the capacity of p.

In [22], Hermelin *et al.* pointed the conclusion, which is stated in Lemma 3.

Lemma 3 ([22]). *In a block cipher E, $C(p)$ is the capacity of probability distribution z^K, z^K is obtained by m basis linear approximations and the plaintext-ciphertext pairs, then*

$$C(p) = \sum_{l=1}^{2^m-1} c\left(\Gamma_{in}^l \to \Gamma_{out}^l\right)^2,$$

where $\Gamma_{in}^l, \Gamma_{out}^l$ are the input mask and output mask of l-th $(1 \le l \le 2^m - 1)$ non-trivial linear approximation generated by m basis linear approximations.

This paper uses the mean of $C(p)$ (i.e., $E(C(p))$) to replace the real capacity $C(p)$. Under the right key guess, z^K follows a unified distribution; therefore, $C(p) = 0$. Hence, under the right key, $T_{K-right}$ follows a central χ^2 distribution $\chi^2_{2^m-1}$; the mean and variance are $\mu_1 = 2^m - 1, \sigma_1^2 = 2^{m+1} - 2$. Under the wrong key guess, z^K may not follow a unified distribution; therefore, $C(p)$ may not be 0. In [22], Bogdanov *et al.* gave the probability of the correlation coefficient of a non-trivial linear approximation, which is stated in Lemma 4.

Lemma 4 ([23]). *For a non-trivial linear approximation of an n-bit idealized block cipher(i.e. a randomly permutation) under a fixed key, the distribution of the correlation value will be as follows:*

$$\Pr\left\{c(\Gamma_{in} \to \Gamma_{out}) = u \cdot 2^{2-n}\right\} \approx \frac{1}{\sqrt{2\pi}2^{\frac{n-4}{2}}} e^{-\frac{z^2}{2^{n-3}}},$$

for integer u between -2^{n-2} and 2^{n-2}.

Theorem 1. *For an n-bit block cipher, the mean of the capacity (i.e. $E(C(p))$) of probability distribution z^K is $(2^m - 1) \times \frac{2^{-n-1}}{\sqrt{2\pi}}$, where $z_i^K = v_i \cdot x_K \oplus w_i \cdot y_K, v_i \to w_i (i = 0, 1, \cdots, m-1)$ are m basis zero-correlation linear approximations. Besides, x_K, y_K are obtained by the plaintext-ciphertext pair with the guessed key K(K is a wrong guess).*

Proof. Because $C(p) = \sum_{l=1}^{2^m-1} c\left(\Gamma_{in}^l \to \Gamma_{out}^l\right)^2$, then

$$\begin{aligned} E(C(p)) &= E\left(\sum_{l=1}^{2^m-1} c\left(\Gamma_{in}^l \to \Gamma_{out}^l\right)^2\right) \\ &= \sum_{l=1}^{2^m-1} E\left(c\left(\Gamma_{in}^l \to \Gamma_{out}^l\right)^2\right). \end{aligned}$$

Then calculate the mean of the square of the correlation of one linear approximation (i.e., $E\left(c\left(\Gamma_{in}^l \to \Gamma_{out}^l\right)^2\right)$). From Lemma 4, it is obviously to obtain

$$\begin{aligned} & E\left(c\left(\Gamma_{in}^l \to \Gamma_{out}^l\right)^2\right) \\ &= \sum_{u=-2^{n-2}}^{2^{n-2}} \frac{1}{\sqrt{2\pi}2^{\frac{n-4}{2}}} e^{-\frac{u^2}{2^{n-3}}} \times (u \cdot 2^{2-n})^2 \\ &= \sum_{u=-2^{n-2}}^{2^{n-2}} \frac{1}{\sqrt{2\pi}2^{\frac{n-4}{2}}} e^{-\frac{u^2}{2^{n-3}}} \times u^2 \times 2^{4-2n} \\ &= \frac{2^{4-2n}}{\sqrt{2\pi}2^{\frac{n-4}{2}}} \times \sum_{u=-2^{n-2}}^{2^{n-2}} e^{-\frac{u^2}{2^{n-3}}} \times u^2 \\ &= \frac{2^{4-2n}}{\sqrt{2\pi}2^{\frac{n-4}{2}}} \times 2^{n-3} \times \sum_{u=-2^{n-2}}^{2^{n-2}} e^{-\frac{u^2}{2^{n-3}}} \times \frac{u^2}{2^{n-3}} \\ &= \frac{2^{3-1.5n}}{\sqrt{2\pi}} \times \sum_{u=-2^{n-2}}^{2^{n-2}} e^{-\frac{u^2}{2^{n-3}}} \times \frac{u^2}{2^{n-3}} \\ &= \frac{2^{3-1.5n}}{\sqrt{2\pi}} \times 2 \sum_{u=1}^{2^{n-2}} e^{-\frac{u^2}{2^{n-3}} \times \frac{u^2}{2^{n-3}}}. \\ &= \frac{2^{4-1.5n}}{\sqrt{2\pi}} \sum_{u=1}^{2^{n-2}} \frac{u^2}{2^{n-3}} e^{-\frac{u^2}{2^{n-3}}} \\ &= \frac{2^{4-1.5n}}{\sqrt{2\pi}} \sum_{u=1}^{2^{\frac{n}{2}-2}} \frac{u^2}{2^{n-3}} e^{-\frac{u^2}{2^{n-3}}} + \sum_{i=1,3,5,\cdots,n-1} 2^i \mathrm{e}^i \\ &\approx \frac{2^{4-1.5n}}{\sqrt{2\pi}} \left(0.274 + \sum_{u=1}^{2^{\frac{n}{2}-2}} \frac{u^2}{2^{n-3}} e^{-\frac{u^2}{2^{n-3}}}\right) \\ &> \frac{2^{4-1.5n}}{\sqrt{2\pi}} \sum_{u=1}^{2^{\frac{n}{2}-2}} \frac{u^2}{2^{n-3}} e^{-\frac{u^2}{2^{n-3}}}. \end{aligned}$$

Because $e^{-\frac{u^2}{2^{n-3}}} \geq 1 - \frac{u^2}{2^{n-3}} + \frac{\left(\frac{u^2}{2^{n-3}}\right)^2}{2} - \frac{\left(\frac{u^2}{2^{n-3}}\right)^3}{3!}$, then

$$\begin{aligned} & \frac{2^{4-1.5n}}{\sqrt{2\pi}} \sum_{u=1}^{2^{\frac{n}{2}-2}} \frac{u^2}{2^{n-3}} e^{-\frac{u^2}{2^{n-3}}} \\ &\geq \frac{2^{4-1.5n}}{\sqrt{2\pi}} \sum_{u=1}^{2^{\frac{n}{2}-2}} \frac{u^2}{2^{n-3}} \\ &\quad \times \left(1 - \frac{u^2}{2^{n-3}} + \frac{\left(\frac{u^2}{2^{n-3}}\right)^2}{2} - \frac{\left(\frac{u^2}{2^{n-3}}\right)^3}{3!}\right) \\ &= \frac{2^{4-1.5n}}{\sqrt{2\pi}} \left\{\frac{1}{2^{n-3}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^2\right) - \frac{1}{2^{2n-6}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^4\right)\right. \\ &\quad \left. + \frac{1}{2} \times \frac{1}{2^{3n-9}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^6\right) - \frac{1}{6} \times \frac{1}{2^{4n-12}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^8\right)\right\}. \end{aligned}$$

Therefore,

$$\begin{aligned} & \frac{2^{4-1.5n}}{\sqrt{2\pi}} \left\{\frac{1}{2^{n-3}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^2\right) - \frac{1}{2^{2n-6}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^4\right)\right. \\ &\quad \left. + \frac{1}{2} \times \frac{1}{2^{3n-9}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^6\right) - \frac{1}{6} \times \frac{1}{2^{4n-12}}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^8\right)\right\} \\ &= \frac{2^{4-1.5n}}{\sqrt{2\pi}} \left\{2^{-(n-3)}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^2\right) - 2^{6-2n}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^4\right)\right. \\ &\quad \left. + \frac{1}{2} \times 2^{9-3n}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^6\right) - \frac{1}{6} \times 2^{12-4n}\left(\sum_{u=1}^{2^{\frac{n}{2}-2}} u^8\right)\right\} \end{aligned}$$

$$\begin{aligned}
&= \frac{2^{4-1.5n}}{\sqrt{2\pi}} \Big\{ 2^{-(n-3)} \left(0.33 \times \left(2^{\frac{n}{2}-2}\right)^3 - 1.5 \times \left(2^{\frac{n}{2}-2}\right)^2\right) \\
&\quad - 2^{6-2n} \left(0.2 \times \left(2^{\frac{n}{2}-2}\right)^5 - 1.6 \times \left(2^{\frac{n}{2}-2}\right)^4\right) \\
&\quad + \frac{1}{2} \times 2^{9-3n} \left(0.143 \times \left(2^{\frac{n}{2}-2}\right)^7 - 2.65 \times \left(2^{\frac{n}{2}-2}\right)^6\right) \\
&\approx \frac{2^{-n-1}}{\sqrt{2\pi}}. \\
&\quad - \frac{1}{6} \times 2^{12-4n} \left(0.11 \times \left(2^{\frac{n}{2}-2}\right)^9 - 0.44 \times \left(2^{\frac{n}{2}-2}\right)^8\right) \Big\} \\
&\approx \frac{2^{4-1.5n}}{\sqrt{2\pi}} \times 0.03 \times 2^{\frac{n}{2}} \\
&\approx \frac{2^{-n-1}}{\sqrt{2\pi}}.
\end{aligned}$$

Finally, it is easy to obtain

$$\begin{aligned}
E(C(p)) &= \sum_{l=1}^{2^m-1} E\left(c\left(\Gamma_{in}^l \to \Gamma_{out}^l\right)^2\right) \\
&= (2^m - 1) \times \frac{2^{-n-1}}{\sqrt{2\pi}}.
\end{aligned}$$

By Theorem 1, the data complexity needed in the multidimensional zero-correlation linear cryptanalysis is given, which is stated in Theorem 2. □

Theorem 2. *In the multidimensional zero-correlation linear cryptanalysis of an n-bit block cipher E, attackers use 2^m zero-correlation linear approximations made up by $m \geq 5$ basis zero-correlation linear approximations. If the probability to wrongfully discard the right key is θ_0 and the probability to wrongfully accept a wrong key as the right key is θ_1, then the number of data used to retrieve the right key is*

$$N \approx \frac{2^{n+2.33}}{2^m} \times \left(2{z_1}^2 + \tau - 2^m - 2z_1\sqrt{{z_1}^2 + \tau - \frac{1}{2}l}\right), \tag{1}$$

where $\Phi(z_1) = p_1, \Pr\left(\chi^2_{2^m-1} \leq \tau\right) = 1 - \theta_0$. Φ is the standard normal distribution, χ_l^2 is a χ^2 distribution whose degree of freedom is l. Attackers assume if $T_k \leq \tau$, then the guessed key is kept, otherwise the guessed key is discarded.

Proof. As the probability to wrongfully discard the right key is θ_0, then $\Pr\left(\chi^2_{2^m-1} \leq \tau\right) = 1-\theta_0$. On the other hand, if $T_{k\text{–}false} \leq \tau$, then $k - false$ is kept as a candidate key. Because $m \geq 5$, then the χ^2 distribution, which followed by $T_{k\text{–}false}$, can be approximated by a normal distribution. Therefore, $\theta_1 = \Phi\left(\frac{\tau-\mu_1}{\sqrt{\sigma_{12}}}\right)$, where Φ is a standard normal distribution.

Denote $\Phi^{-1}(\theta_1) = z_1$, then $\frac{\tau-\mu_1}{\sqrt{\sigma_{12}}} = z_1$, hence $\tau = \mu_1 + z_1\sqrt{\sigma_{12}}$. Because

$$\mu_1 = 2^m - 1 + NC(p), \sigma_1 = 2(2^m - 1 + 2NC(p)),$$

$$C(p) = (2^m - 1) \times \frac{2^{-n-1}}{\sqrt{2\pi}}.$$

Denote $M = \frac{2^{-n-1}}{\sqrt{2\pi}}$, then $C(p) = (2^m - 1)M$; therefore,

$$\begin{aligned}
\tau &= \mu_1 + z_1\sqrt{\sigma_{12}} = 2^m - 1 + (2^m - 1)NM \\
&\quad + z_1\sqrt{2(2^m - 1 + (2^{m+1} - 2)NM)} \\
&= 2^m - 1 + (2^m - 1)NM \\
&\quad + z_1\sqrt{2^{m+1} - 2 + (2^{m+2} - 4)NM} \\
&\approx 2^m + 2^m NM + z_1\sqrt{2^{m+1} - 2 + 2^{m+2}NM} \\
&\approx 2^m + 2^m NM + z_1\sqrt{2^{m+1} + 2^{m+2}NM}.
\end{aligned}$$

Finally,

$$\begin{aligned}
N &\approx \frac{2{z_1}^2 + \tau - 2^m - 2z_1\sqrt{z_{12} + \tau - \frac{1}{2}l}}{2^m M} \\
&\approx \frac{2{z_1}^2 + \tau - 2^m - 2z_1\sqrt{z_{12} + \tau - \frac{1}{2}l}}{2^m \times \frac{2^{-n-1}}{\sqrt{2\pi}}} \\
&\approx \frac{\sqrt{2\pi} \times 2^{n+1}\,{}^m}{2}\left(2z_{12} + \tau - 2^m - 2z_1\sqrt{z_{12} + \tau - \frac{1}{2}l}\right) \\
&\approx \frac{2^{n+2.33}}{2^m} \times \left(2z_{12} + \tau - 2^m - 2z_1\sqrt{z_{12} + \tau - \frac{1}{2}l}\right).
\end{aligned}$$

In Piccolo, the round key *rk* is xored with the output of F-Function; *rk* is not involved in F-Function in the current round, namely that the round key *rk* is involved in F-Function in the next round for the first time. Based on this fact, Theorem 3 shows the number of key bits needed to be guessed in multidimensional zero-correlation cryptanalysis can be decreased under which situation. □

Theorem 3. *With the given m basis zero-correlation linear approximations $v_i \to w_i$, where $i = 0, 1, \cdots, m-1$. For $(x_0, y_0), (x_1, y_1), \cdots, (x_{N-1}, y_{N-1})$ and (k_1, k_2) which is independent from $(x_0, y_0), (x_1, y_1), \cdots, (x_{N-1}, y_{N-1})$. Compute*

$$z' = \left(z'_0, \cdots, z'_{m-1}\right), z = (z_0, \cdots, z_{m-1}).$$

where $z'_i = v_i \cdot (x \oplus k_1) \oplus w_i \cdot (y \oplus k_2), z_i = v_i \cdot x \oplus w_i \cdot y$, $(x, y) \in \{(x_0, y_0), \cdots, (x_{N-1}, y_{N-1})\}$. For any $z', z \in F_2^m$, construct $V[z']$ and $V[z]$, $V[z']$ and $V[z]$ are used to count the frequency of z' and z respectively. Then for any integer *n, it is directly to obtain* $\#\{z' : V[z'] = n\} = \#\{z : V[z] = n\}$*, and*

$$\sum_{z=0}^{2^m-1} \frac{(V[z]-N2^{-m})^2}{N2^{-m}} = \sum_{z=0}^{2^m-1} \frac{(V[z']-N2^{-m})^2}{N2^{-m}}.$$

Proof. Because $z_i' = v_i \cdot (x \oplus k_1) \oplus w_i \cdot (y \oplus k_2), z_i = v_i \cdot x \oplus w_i \cdot y$, then $z_i' \oplus z_i = v_i \cdot k_1 \oplus w_i \cdot k_2$; therefore, $z = z' \oplus (v_0 \cdot k_1 \oplus w_0 \cdot k_2, \cdots, v_{m-1} \cdot k_1 \oplus w_{m-1} \cdot k_2)$. Then for any $z' \in F_2^m$,

$$\begin{aligned}
&\#\{z' : V[z'] = n\} \\
&= \#\{z : V[z \oplus (v_0 \cdot k_1 \oplus w_0 \cdot k_2, \cdots, \\
&\qquad v_{m-1} \cdot k_1 \oplus w_{m-1} \cdot k_2)] = n\} \\
&= \#\{z : V[z] = n\}.
\end{aligned}$$

Furthermore, it is directly to obtain

$$\sum_{z=0}^{2^m-1} \frac{(V[z]-N2^{-m})^2}{N2^{-m}} = \sum_{z=0}^{2^m-1} \frac{(V[z']-N2^{-m})^2}{N2^{-m}}.$$

□

3. 7-ROUND ZERO-CORRELATION LINEAR APPROXIMATIONS IN PICCOLO

This section mainly studies the zero-correlation linear approximations in Piccolo. The 7-round zero-correlation linear approximations in Piccolo are given based upon the fact that the branch number of the linear layer of F-Function in Piccolo is 5. Because the S-box used in F-Function is a 4-bit to 4-bit bijection, the 64-bit input mask Γx and output mask Γy are split into 16 4-bit blocks, namely $\Gamma x = (\Gamma x_0, \cdots, \Gamma x_{15}), \Gamma y = (\Gamma y_0, \cdots, \Gamma y_{15})$.

When the input mask of Piccolo is $(??00, 0000, 00??, 0000)$, from the encryption view, the 4 rounds propagation path of the input mask is listed in Table III. When the output mask of Piccolo is $(0000, ????, 0000, 0000)$, from the decryption view, the 3 rounds propagation path of the output mask is listed in Table IV. $'?'$ represents a fixed value in F_2^4, and $'*'$ represents an arbitrary value in F_2^4. Because in the process of constructing 7-round zero-correlation linear approximation, the specific values of each $'*'$ and $'?'$ are not necessary; there is no need to distinguish each $'*'$ and $'?'$ in this paper.

From Tables III and IV, one class of 7-round zero-correlation linear approximation in Piccolo is stated in Theorem 4.

Theorem 4. *In Piccolo,* $(??00, 0000, 00??, 0000) \rightarrow (0000, ????, 0000, 0000)$ *is a 7-round zero-correlation linear approximation, where at least one* $'?'$ *is nonzero.*

Proof. By Table IV, if the output mask of 7-round Piccolo is $(0000, ????, 0000, 0000)$, then after 3 rounds decryption, $\Gamma y_4^4 \Gamma y_5^4 = \Gamma y_{14}^4 \Gamma y_{15}^4 = 00$, hence $\Gamma x_4^4 \Gamma x_5^4 = \Gamma x_{14}^4 \Gamma x_{15}^4 = 00$. By the structure of Piccolo, it is easy to obtain

$$\begin{aligned}
&\Gamma x_4^4 \Gamma x_5^4 \Gamma x_{14}^4 \Gamma x_{15}^4 = \Gamma x_8^3 \Gamma x_9^3 \Gamma x_{10}^3 \Gamma x_{11}^3 \\
&\oplus F\left(\Gamma x_{12}^3 \Gamma x_{13}^3 \Gamma x_{14}^3 \Gamma x_{15}^3\right) = 0000.
\end{aligned} \tag{2}$$

By Table III, $\Gamma x_8^3 \Gamma x_9^3 \Gamma x_{10}^3 \Gamma x_{11}^3 = 0000$. As F is bijective, it is easy to obtain $\Gamma x_{12}^3 \Gamma x_{13}^3 \Gamma x_{14}^3 \Gamma x_{15}^3 = 0000$ combined with Formula (2). Besides, by the structure of Piccolo

$$\begin{aligned}
&\Gamma x_0^2 \Gamma x_1^2 \Gamma x_2^2 \Gamma x_3^2 \oplus F\left(\Gamma x_4^2 \Gamma x_5^2 \Gamma x_6^2 \Gamma x_7^2\right) \\
&= 00?? \oplus F\left(\Gamma x_4^2 \Gamma x_5^2 \Gamma x_6^2 \Gamma x_7^2\right) \\
&= \Gamma x_{12}^3 \Gamma x_{13}^3 \Gamma x_6^3 \Gamma x_7^3 = 00**,
\end{aligned} \tag{3}$$

Table III. The input mask of each round in 4-round encryption in Piccolo.

Round	$\Gamma x_0 \sim \Gamma x_{15}$															
0	?	?	0	0	0	0	0	0	0	0	?	?	0	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	?	?	?	?
2	0	0	?	?	∗	∗	0	0	?	?	0	0	0	0	∗	∗
3	∗	∗	∗	∗	∗	∗	∗	∗	0	0	0	0	∗	∗	∗	∗
4	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗

Table IV. The output mask of each round in 3-round decryption in Piccolo.

Round	$\Gamma y_0 \sim \Gamma y_{15}$															
r	0	0	0	0	?	?	?	?	0	0	0	0	0	0	0	0
$r-1$	0	0	?	?	0	0	0	0	?	?	0	0	0	0	0	0
$r-2$	0	0	0	0	0	0	0	0	∗	∗	∗	∗	?	?	?	?
$r-3$	∗	∗	∗	∗	0	0	∗	∗	∗	∗	∗	∗	∗	∗	0	0

$$\begin{aligned}&\Gamma x_8^2\Gamma x_9^2\Gamma x_{10}^2\Gamma x_{11}^2 \oplus F\left(\Gamma x_{12}^2\Gamma x_{13}^2\Gamma x_{14}^2\Gamma x_{15}^2\right)\\ &=??00 \oplus F\left(\Gamma x_{12}^2\Gamma x_{13}^2\Gamma x_{14}^2\Gamma x_{15}^2\right)\\ &= \Gamma x_4^3\Gamma x_5^3\Gamma x_{14}^3\Gamma x_{15}^3 = **00.\end{aligned} \tag{4}$$

Therefore, by Formulas (3) and (4)

$$\begin{aligned}&wt\left(F\left(\Gamma x_{12}^2\Gamma x_{13}^2\Gamma x_{14}^2\Gamma x_{15}^2\right)\right) \le 2,\\ &wt\left(F\left(\Gamma x_4^2\Gamma x_5^2\Gamma x_6^2\Gamma x_7^2\right)\right) \le 2.\end{aligned} \tag{5}$$

On the other hand, by Table III $\Gamma x_{12}^2\Gamma x_{13}^2\Gamma x_{14}^2\Gamma x_{15}^2 = 00**, \Gamma x_4^2\Gamma x_5^2\Gamma x_6^2\Gamma x_7^2 = **00$. Because the branch number of the linear layer in F-function in Piccolo is 5, then

$$\begin{aligned}&wt\left(F\left(\Gamma x_{12}^2\Gamma x_{13}^2\Gamma x_{14}^2\Gamma x_{15}^2\right)\right) \ge 3,\\ &wt\left(F\left(\Gamma x_4^2\Gamma x_5^2\Gamma x_6^2\Gamma x_7^2\right)\right) \ge 3.\end{aligned} \tag{6}$$

As Formula (5) contradicts to Formula (6), therefore,

$$(??00, 0000, 00??, 0000) \rightarrow (0000, ????, 0000, 0000)$$

is a class of 7-round zero-correlation linear approximations in Piccolo. □

In the following, another class of 7-round zero-correlation linear approximation in Piccolo is stated. Firstly, the 4 rounds propagation path of the input mask when the input mask of Piccolo is (00??, 0000, ??00, 0000) from the encryption view is listed in Table V. Additionally, when the output mask of Piccolo is (0000, 0000, 0000, ????), the 3 rounds propagation path of the output mask is listed in Table VI from the decryption view.

From Tables V and VI, Theorem 5 gives another class of 7-round zero-correlation in Piccolo.

Theorem 5. *In Piccolo,* (00??, 0000, ??00, 0000) → (0000, 0000, 0000, ????) *is a 7-round zero-correlation linear approximation, where at least one* ′?′ *is nonzero.*

The proof of Theorem 5 is the same as that of Theorem 4; therefore, the details of the proof is not given.

Remark 2. For the sake of convenience, this paper denotes the 7-round zero-correlation linear approximations in Theorems 4 and 5 as $A_1 0, 00, 0A_2, 00 \rightarrow 00, B_1B_2, 00, 00$ and $0A_1, 00, A_2 0, 00 \rightarrow 00, 00, 00, B_1B_2$, respectively, where $(A_1, A_2, B_1, B_2) \in F_2^{32}\backslash\{0\}$.

4. KEY-RECOVERY ATTACK ON 13 /14 /15-ROUND PICCOLO-128

4.1. Key-recovery attack on 13-round Piccolo-128

Based on the 7-round zero-correlation linear approximation $A_1 0, 00, 0A_2, 00 \rightarrow 00, B_1B_2, 00, 00$, this section presents the attack on rounds 0–12 in Piccolo-128 which can be seen in Figure 4. The 7-round zero-correlation linear approximations are inserted in rounds 3–9. According to the principle of multidimensional zero-correlation cryptanalysis, the distribution of the value of $A_1 \cdot X_{3,0} \oplus A_2 \cdot X_{3,5} \oplus B_1 \cdot Y_{9,1} \oplus B_2 \cdot Y_{9,4}$ needed to be calculated. Therefore, the values of $(X_{3,0}, X_{3,5}, Y_{9,1}, Y_{9,4})$ after partially encryption and decryption of N plaintext-ciphertext pairs are collected.

Combining with partial sum technique, the attack on 13-round Piccolo-128 is presented in this section. The key-recovery attack on 13-round Piccolo-128 is proceeded from Step 1 to Step 8 as follows. The 13-round attack on Piccolo-128 assumes $A_1 = 0$ and $(A_2, B_1, B_2) \in F_2^{24}\backslash\{0\}$.

Step 1. Guess all possible values of 40-bit key $\left(k_0^L, k_2^R, k_3, k_5^R\right)$, allocate a counter vector $V_1[x_1]$ for all possible values of 72-bit $x_1 = \left(X'_{11,6}, X'_{12,3}, X'_{12,[5,6]},\right.$

Table V. The input mask of each round in 4-round encryption in Piccolo.

Round	$\Gamma x_0 \sim \Gamma x_{15}$															
0	0	0	?	?	0	0	0	0	?	?	0	0	0	0	0	0
1	0	0	0	0	0	?	?	?	?	0	0	0	0	0	0	0
2	?	?	0	0	0	0	*	*	0	0	?	?	*	*	0	0
3	*	0	0	0	0	*	*	*	*	*	*	*	*	*	*	*
4	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*

Table VI. The output mask of each round in 3-round decryption in Piccolo.

Round	$\Gamma y_0 \sim \Gamma y_{15}$															
r	0	0	0	0	0	0	0	0	0	0	0	0	?	?	?	?
$r-1$	?	?	0	0	0	0	0	0	0	0	?	?	0	0	0	0
$r-2$	*	*	*	*	?	?	?	?	0	0	0	0	0	0	0	0
$r-3$	*	*	*	*	*	*	0	0	*	*	*	*	0	0	*	*

$X_{11,5}, Y'_{0,2}, X_{1,[1,2]}, Y_{1,7}\big)$ and initialize each counter to be zero. Traverse N plaintext-ciphertext pairs, get $X_{12,[3,\cdots,7]}, X'_{12,2}$ by k_0, k_3 and $Y_{12,[0,\cdots,7]}$, get $Y_{0,[4,5,6,7]}$ by $X_{0,[4,5,6,7]}$ and k_3. Then compute

$$\begin{aligned}
X'_{12,3} &= F(Y_{12,0}, Y_{12,1})^R \oplus Y_{12,3},\\
Y_{0,3} &= F(X_{0,0}, X_{0,1})^R \oplus X_{0,3} \oplus k_2^R,\\
Y'_{0,2} &= F(X_{0,0}, X_{0,1})^L \oplus X_{0,2},\\
Y_{1,7} &= F(X_{1,4}, X_{1,5})^R \oplus X_{1,7} \oplus k_5^R.
\end{aligned}$$

Add one to the corresponding $V_1[x_1]$. The time complexity of this step is $N \times 2^{40} \times (16+8+6+8+6) \approx N \times 2^{45.6}$ table look-ups.

Step 2. For each value of $\left(k_0^L, k_2^R, k_3, k_5^R\right)$, guess 8-bit k_0^R and allocate a counter vector $V_2[x_2]$ for all possible values $x_2 = \left(X'_{11,6}, X'_{11,3}, X_{11,0}, X_{11,5}, Y'_{0,2}, X_{1,[1,2]}, Y_{1,7}\right)$, initialize each counter to zero. Traverse x_1, compute

$$\begin{aligned}
Y_{11,1} &= X_{12,3} = X'_{12,3} \oplus k_0^R,\\
X'_{11,3} &= F(Y_{11,0}, Y_{11,1})^R \oplus Y_{11,3}.
\end{aligned}$$

Add the corresponding $V_1[x_1]$ to $V_2[x_2]$, namely $V_2[x_2]+ = V_1[x_1]$. The time complexity of this step is $2^{40} \times 2^8 \times 2^{72} \times 6 \approx 2^{122.6}$ table look-ups.

Step 3. For each value of $\left(k_0, k_2^R, k_3, k_5^R\right)$, guess 8-bit k_2^L and allocate a counter vector $V_3[x_3]$ for all possible values $x_3 = \left(X'_{11,6}, X'_{11,3}, X_{11,0}, X_{11,5}, Y'_{1,2}, Y_{1,1}, Y_{1,7}\right)$, initialize each counter to zero. Traverse x_2, compute

$$\begin{aligned}
X_{0,0} &= Y_{0,2} = Y'_{0,2} \oplus k_2^L,\\
Y'_{1,2} &= X_{1,2} \oplus F(X_{1,0}, X_{1,0})^L.
\end{aligned}$$

Add the corresponding $V_2[x_2]$ to $V_3[x_3]$, namely $V_3[x_3]+ = V_2[x_2]$. The time complexity of this step is $2^{40} \times 2^8 \times 2^8 \times 2^{64} \times 6 \approx 2^{122.6}$ table look-ups.

Step 4. For each value of $\left(k_0, k_2, k_3, k_5^R\right)$, guess 8-bit k_4^L and allocate a counter vector $V_4[x_4]$ for all possible values $x_4 = \left(X'_{11,6}, X'_{11,3}, X_{11,0}, X_{11,5}, Y'_{2,3}\right)$, initialize each counter to zero. Traverse x_3, compute

$$Y_{1,2} = Y'_{1,2} \oplus k_4^L,$$

$$\begin{aligned}
(Y'_{2,2}, Y'_{2,3}) &= (X_{2,2}, X_{2,3}) \oplus\\
&\left(F(X_{2,0}, X_{2,1})^L, F(X_{2,0}, X_{2,1})^R\right).
\end{aligned}$$

Add the corresponding $V_3[x_3]$ to $V_4[x_4]$, namely $V_4[x_4]+ = V_3[x_3]$. The time complexity of this step is $2^{40} \times 2^8 \times 2^8 \times 2^8 \times 2^{56} \times 8 = 2^{123}$ table look-ups.

Step 5. For each value of $\left(k_0, k_2, k_3, k_4^L, k_5^R\right)$, guess 16-bit $\left(k_1^L, k_4^R\right)$ and allocate a counter vector $V_5[x_5]$ for all possible values $x_5 = (X_{10,[2,3]}, Y'_{2,3})$, initialize each counter to zero. Traverse x_4, compute

$$X_{11,6} = X'_{11,6} \oplus k_1^L, X_{11,3} = X'_{11,3} \oplus k_4^R,$$

$$\begin{aligned}
(X'_{10,2}, X'_{10,3}) &= (Y_{10,2}, Y_{10,3}) \oplus\\
&(F(Y_{10,0}, Y_{10,1})^L, F(Y_{10,0}, Y_{10,1})^R).
\end{aligned}$$

Add the corresponding $V_4[x_4]$to $V_5[x_5]$, namely $V_5[x_5]+ = V_4[x_4]$. The time complexity of this step is $2^{40} \times 2^8 \times 2^8 \times 2^8 \times 2^{16} \times 2^{40} \times 8 = 2^{123}$ table look-ups.

Step 6. For each value of $\left(k_0, k_1^L, k_2, k_3, k_4, k_5^R\right)$, allocate a counter vector $V[z]$ of size 2^{24}, where $z = (z_0, \cdots, z_{23})$ and $z_i = A_{2,i} \cdot X'_{2,5} \oplus B_{1,i} \cdot Y_{9,1} \oplus B_{2,i} \cdot Y_{9,4}$ for $0 \leq i \leq 23$, initial each vector to be zero. Then compute the evaluations of all 24 basis zero-correlations linear approximations with valuex_5. Add the corresponding $V_5[x_5]$ to $V[z]$, namely $V[z]+ = V_5[x_5]$.

Step 7. Compute $T_{(k_0,k_1^L,k_2,k_3,k_4,k_5^R)} = N2^{24} \sum_{z=0}^{2^{24}-1} \left(\frac{V[z]}{N} - \frac{1}{2^{24}}\right)^2$. If $T_{(k_0,k_3,k_2,k_5^R,k_4,k_1^L)} \leq \tau$, then the guessed key $\left(k_0, k_1^L, k_2, k_3, k_4, k_5^R\right)$ is kept as a right key candidate.

Step 8. Do exhaustive search for all candidate keys to retrieve the right key.

Our 13-round attack on Piccolo-128 set $\theta_0 = 2^{-2.7}, \theta_1 = 2^{-14.3}$, as $m = 24$, then $z_1 \approx -3.9, \tau \approx 2^{24}$. Because $n = 64, l = 2^{24} - 1$, then according to Formula (1), it can obtain $N \approx 2^{56.8}$. Because 80 master key bits are guessed in total in the given steps, then after step 7, there are $2^{80} \times 2^{-14.3} = 2^{65.7}$ key candidates kept. Besides, there are $128 - 80 = 48$ master key bits needed to be guessed because the scale of the master key in Piccolo-128 is 128. As $N \approx 2^{56.8}$, Step 1 to Step 7 cost $2^{124.8}$ table look-ups. Because there are $13 \times 16 \approx 2^{7.7}$ table look-ups in 13-round Piccolo-128 as each round has 16 table look-ups, therefore, the total time complexity of the attack on 13-round Piccolo-128 is $2^{124.8}/2^{7.7}+2^{65.7+48} \approx 2^{117.2}$ 13-round encryptions.

4.2. Key-recovery attack on 14-round Piccolo-128

This section presents the attack on rounds 15–28 of Piccolo-128 which can be seen in Figure 5. The 7-round zero-correlation linear approximations $A_1 0, 00, 0A_2, 00 \rightarrow 00, B_1B_2, 00, 00$ are inserted in rounds 18–24. Because a lot of master key bits needed to be guessed to obtain the boundaries of the zero-correlation linear approximations, the time complexity will be larger than 2^{128} if attacking rounds 0–13 in Piccolo-128. By Table II, the round key of round 26 is the same as the round key of round 28. The

15-round attack on Piccolo-128 assumes $(A_1, A_2, B_1, B_2) \in F_2^{32} \backslash \{0\}$.

Combining with partial sum technique, the key-recovery attack on 14-round Piccolo-128 is proceeded from Step 1 to Step 4 as follows.

Step 1. Guess all possible values of 72-bit key $\left(k_0, k_1, k_2^L, k_4, k_7\right)$, allocate a counter vector $V_1[x_1]$ for all possible values of 32-bit $x_1 = \left(X_{18,0}, X_{18,5}, Y'_{24,1}, Y_{24,4}\right)$ and initialize each counter to zero. Traverse N plaintext-ciphertext pairs, get $Y'_{24,1}, Y_{24,4}$ by $\left(k_0, k_1, k_2^L, k_4, k_7\right)$ and Y_{28}, get $X_{18,0}, X_{18,5}$ by $\left(k_0, k_1, k_2^L, k_4, k_7^R\right)$ and X_{15}. Add one to the corresponding $V_1[x_1]$. The time complexity of this step is $N \times 2^{72} \times (16+6+6+8+16+16+6+6+8) \approx N \times 2^{78.46}$ table look-ups.

Step 2. For each value of $\left(k_0, k_1, k_2^L, k_4, k_7\right)$, allocate a counter vector $V[z]$ of size 2^{32}, where $z = (z_0, \cdots, z_{31})$ and $z_i = A_{1,i} \cdot X_{18,0} \oplus A_{2,i} \cdot X_{18,5} \oplus B_{1,i} \cdot Y'_{24,1} \oplus B_{2,i} \cdot Y_{24,4}$ for $0 \le i \le 31$, initial each vector to be zero. Then compute the evaluations of all 32 basis zero-correlations linear approximations with valuex_5. Add the corresponding $V_1[x_1]$ to $V[z]$, namely $V[z]+ = V_1[x_1]$.

Step 3. Compute $T_{\left(k_0,k_1,k_2^L,k_4,k_7\right)} = N 2^{32} \sum_{z=0}^{2^{32}-1} \left(\frac{V[z]}{N} - \frac{1}{2^{32}}\right)^2$. If $T_{\left(k_0,k_1,k_2^L,k_4,k_7\right)} \le \tau$, then the guessed key $\left(k_0, k_1, k_2^L, k_4, k_7\right)$ is a right key candidate.

Step 4. Do exhaustive search for all candidate keys to retrieve the right key.

Our 14-round attack on Piccolo-128 sets $\theta_0 = 2^{-2.7}, \theta_1 = 2^{-9.5}$, as $m = 32$, then $z_1 \approx -3, \tau \approx 2^{32}$. Because $n = 64, l = 2^{32} - 1$, then according to Formula (1), the data complexity $N \approx 2^{52.43}$. Seventy-two main key bits are guessed in total; then after step 3, there are $2^{72} \times 2^{-9.5} = 2^{62.5}$ key candidates survive. Besides, there are $128 - 72 = 56$ master key bits also needed to be guessed because the scale of the master key in Piccolo-128 is 128. As $N \approx 2^{52.43}$, Step 1 to Step 3 cost $2^{130.89}$ table look-ups. Because there are $16 \times 14 \approx 2^{7.8}$ table look-ups in 14-round Piccolo-128 as each round has 16 table look-ups, therefore, the total time complexity of the attack on 14-round Piccolo-128 is $2^{130.89}/2^{7.8} + 2^{62.5+56} \approx 2^{123.09}$ 14-round encryptions.

4.3. Key-recovery attack on 15-round Piccolo-128

This section presents the multidimensional zero-correlation linear cryptanalysis on rounds 14–28 of Piccolo-128 which can be seen in Figure 6. The 7-round zero-correlation linear approximations $A_1 0, 00, 0 A_2, 00 \rightarrow 00, B_1 B_2, 00, 00$ are inserted in rounds 18–24. By Table II, it is easy to obtain that the round key of round 14 is the same as the round key of round 16 in Piccolo-128. This attack assumes $(A_1, A_2, B_2) \in F_2^{24} \backslash \{0\}$ and $B_1 = 0$.

Combining with partial sum technique, the key-recovery attack on 15-round Piccolo-128 is proceeded from Step 1 to Step 5 as follows.

Step 1. Guess all possible values of 72-bit key $\left(k_0, k_1, k_2, k_4^L, k_7\right)$, allocate a counter vector $V_1[x_1]$ for all possible values of 48-bit $x_1 = \left(Y_{17,2}, Y'_{17,3}, Y_{26,[0,3]}, X'_{27,3}, X_{26,6}\right)$ and initialize each counter to zero. Traverse N plaintext-ciphertext pairs, get $Y_{26,[0,3]}, X'_{27,3}, X_{26,6}$ by $\left(k_0, k_1, k_2, k_7, k_4^L\right)$ and Y_{28}, get $X_{18,0}, Y'_{17,3}$ by $\left(k_0, k_1, k_2, k_7, k_4^L\right)$ and X_{14}. Add one to the corresponding $V_1[x_1]$. The time complexity of this step is $N \times 2^{72} \times (16+16+6+6+8+16+16+6) \approx N \times 2^{78.5}$ table look-ups.

Step 2. For each value of $(k_0, k_1, k_2, k_4^L, k_7)$, guess 8-bit k_4^R and allocate a counter vector $V_2[x_2]$ for all possible values $x_2 = (X_{18,0}, X_{18,5}, X_{25,2})$, initialize each counter to zero. Traverse x_1, compute

$$
\begin{aligned}
X_{18,5} &= Y_{17,3} = Y'_{17,3} \oplus k_4^R, \\
Y_{26,1} &= X_{27,3} = X'_{27,3} \oplus k_4^R, \\
Y_{25,1} &= X_{26,3} = Y_{26,3} \oplus F(Y_{26,0}, Y_{26,1})^R \oplus k_0^R, \\
X_{25,2} &= Y_{25,2} \oplus F(Y_{25,0}, Y_{25,1})^L \oplus k_2^L.
\end{aligned}
$$

Add the corresponding $V_1[x_1]$ to $V_2[x_2]$, namely $V_2[x_2]+ = V_1[x_1]$. The time complexity of this step is $2^{72} \times 2^8 \times 2^{48} \times (6+6) \approx 2^{131.6}$ table look-ups.

Step 3. For each value of $(k_0, k_1, k_2, k_4, k_7)$, allocate a counter vector $V[z]$ of size 2^{24}, where $z = (z_0, \cdots, z_{23})$ and $z_i = A_{1,i} \cdot X_{18,0} \oplus A_{2,i} \cdot X_{18,5} \oplus B_{2,i} \cdot X_{25,2}$ for $0 \le i \le 23$, initial each vector to be zero. Then compute the evaluations of all 24 basis zero-correlations linear approximations with valuex_5. Add the corresponding $V_2[x_2]$ to $V[z]$, namely $V[z]+ = V_2[x_2]$.

Step 4. Compute $T_{(k_0,k_1,k_2,k_4,k_7)} = N 2^{24} \sum_{z=0}^{2^{24}-1} \left(\frac{V[z]}{N} - \frac{1}{2^{24}}\right)^2$. If $T_{(k_0,k_1,k_2,k_4,k_7)} \le \tau$, then the guessed key $(k_0, k_1, k_2, k_4, k_7)$ is kept as a right key candidate.

Step 5. Do exhaustive search for all candidate keys to retrieve the right key.

The 15-round attack on Piccolo-128 sets $\theta_0 = 2^{-2.7}, \theta_1 = 2^{-4.5}$, as $m = 24$, then $z_1 \approx -1.7, \tau \approx 2^{24}$. Because $n = 64, l = 2^{24} - 1$, then according to Formula (1), the data complexity $N \approx 2^{55.6}$. Because 80 main key bits are guessed in total in the given steps, there are $2^{80} \times 2^{-4.5} = 2^{75.5}$ key candidates survive after step 4. There are $128 - 80 = 48$ main key bits still needed to be

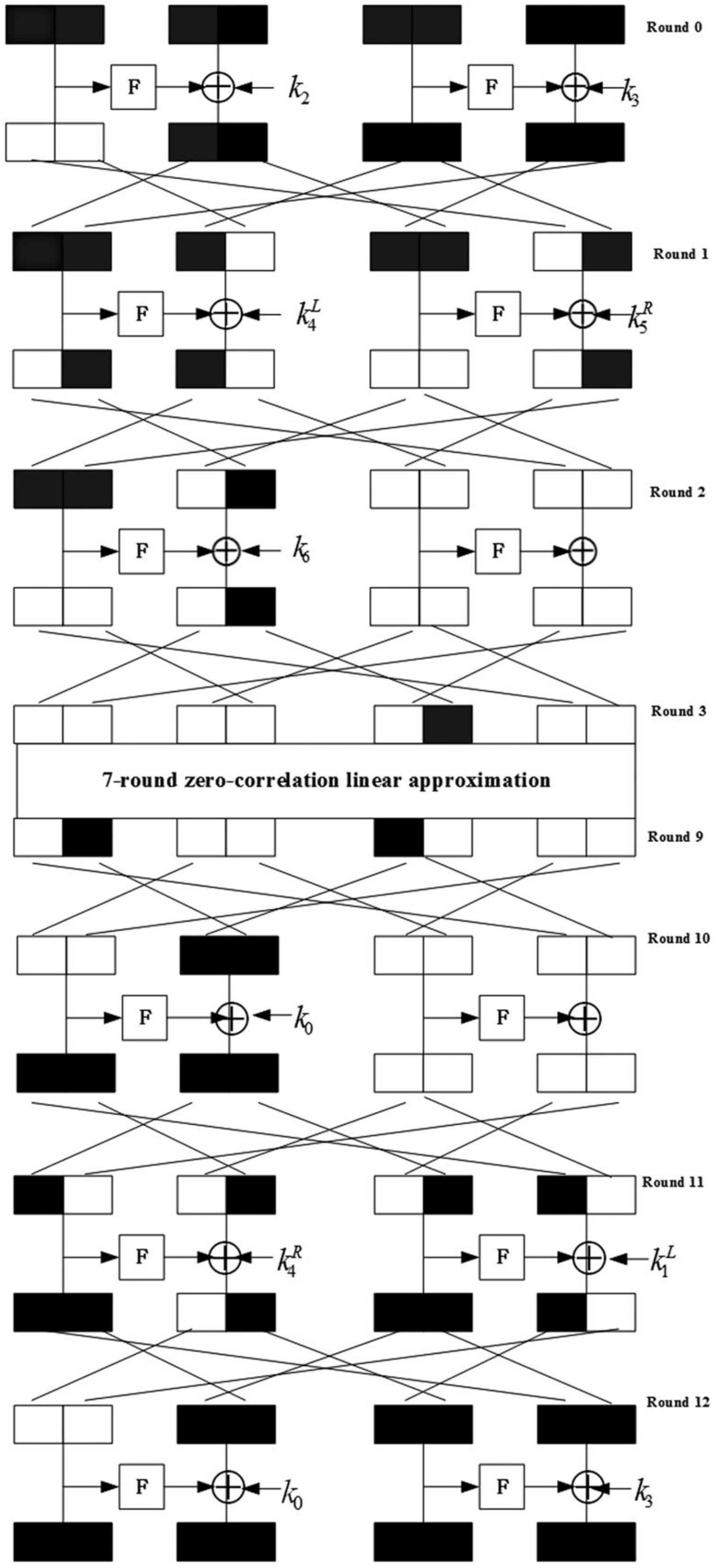

Figure 4. Attack on 13-round Piccolo-128.

DOI: 10.1002/sec

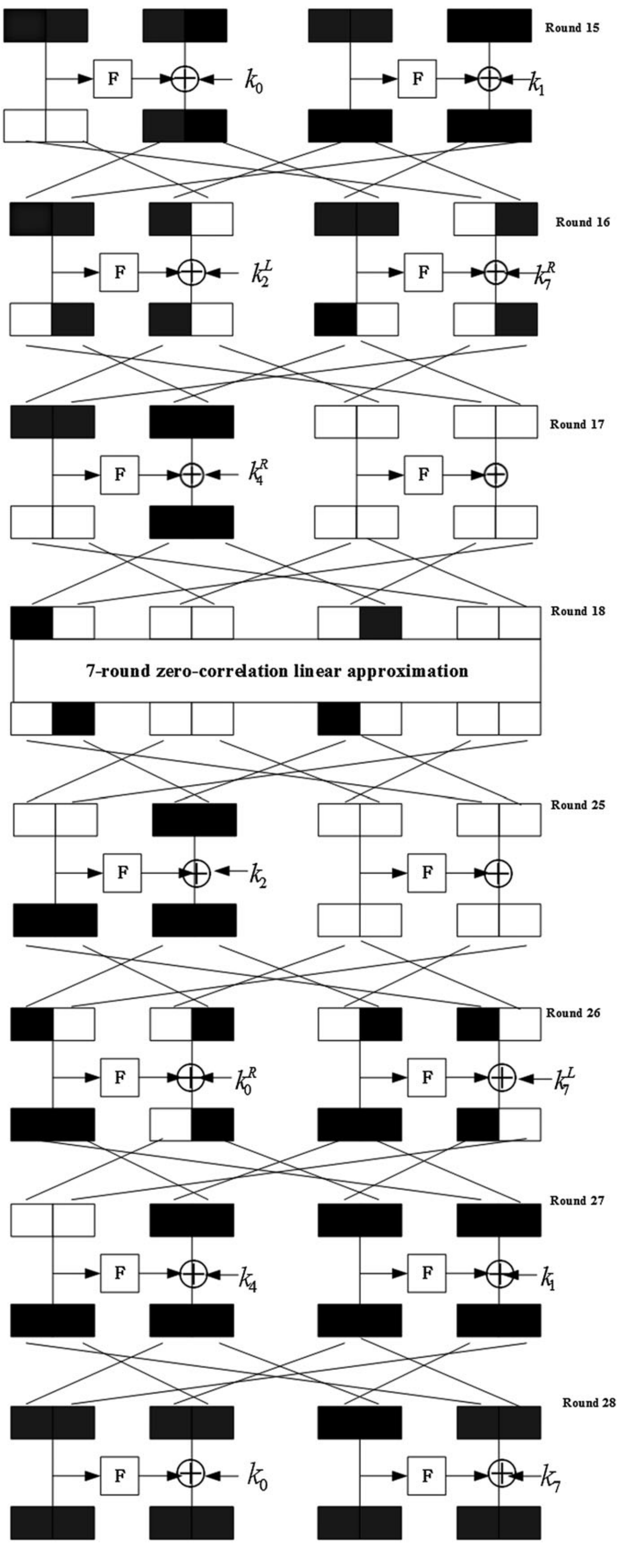

Figure 5. Attack on 14-round Piccolo-128.

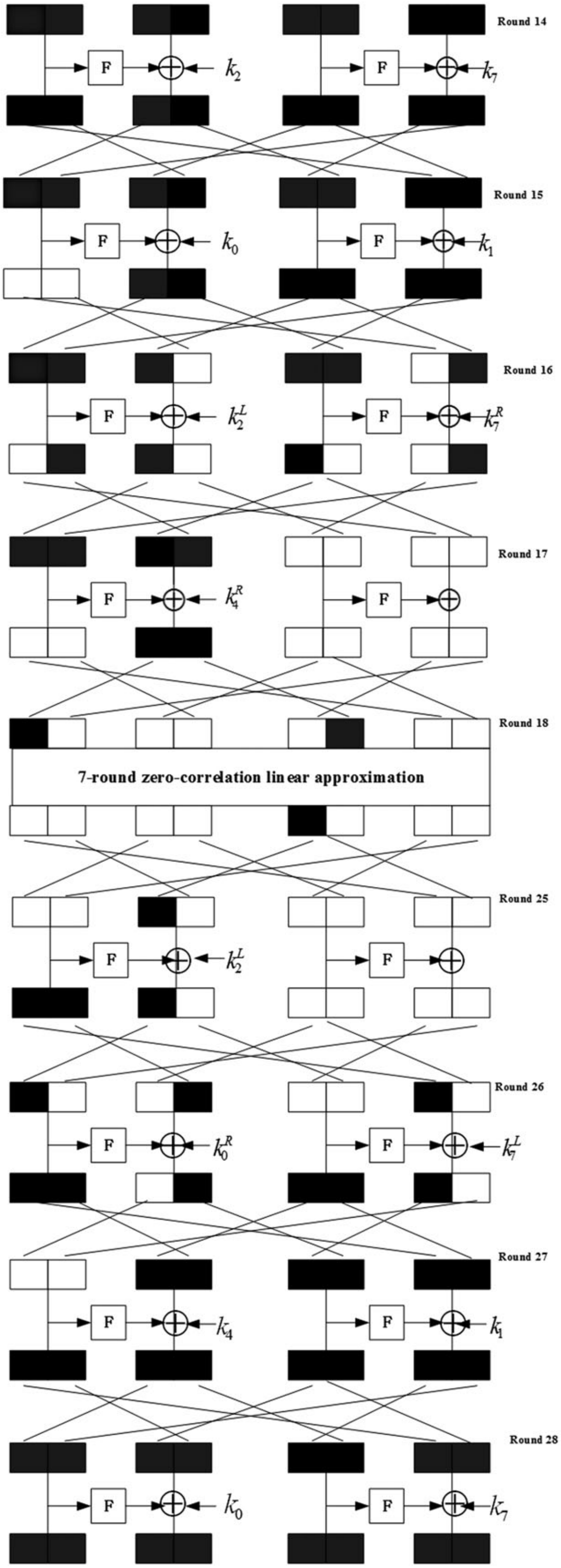

Figure 6. Attack on 15-round Piccolo-128.

]

guessed because the scale of the main key in Piccolo-128 is 128. As $N \approx 2^{55.6}$, Step 1 to Step 4 cost $2^{134.3}$ table look-ups. Because there are $16 \times 15 \approx 2^{7.9}$ table look-ups in 15-round Piccolo-128 as each round has 16 table look-ups, therefore, the total time complexity of the attack on 15-round Piccolo-128 is $2^{134.3}/2^{7.9} + 2^{75.5} \times 2^{48} \approx 2^{126.55}$ 15-round encryptions.

5. CONCLUSIONS

Piccolo is a lightweight block cipher, which adopts generalized Feistel network. In this paper, the security of Piccolo family against multidimensional zero-correlation linear cryptanalysis is evaluated for the first time. This paper firstly present two classes of 7-round zero-correlation linear approximations of Piccolo by taking advantage of the fact that the branch number of the linear layer in F-Function is 5. Based on the key schedule of Piccolo-128 and partial sum technique, the attacks on 13-round/14-round/15-round Piccolo-128 are given in this paper. Specially, because the key bits not involved in nonlinear functions do not affect the distribution that T_K follows, only the key bits that involved in the nonlinear F-Function needed to be guessed, and the order of the guessed key bits can be switched, which leads a reduction in the time complexity. Finally, the attacks on rounds 0–12/rounds 15–28/rounds 14–28 of Piccolo-128 need $2^{56.8}/2^{52.43}/2^{55.6}$ known-plaintexts, while the time complexities of those attacks are $2^{117.2}$, $2^{123.09}$, $2^{126.55}$, respectively. Besides, this paper adopts the statistic T_K used by Hermlin *et al.* in multidimensional linear cryptanalysis to evaluate the data complexity in multidimensional zero-correlation linear cryptanalysis, which can also be used in the cryptanalyses of other ciphers without loss of generality.

The attacks presented in this paper are the first known-plaintexts attacks on Piccolo-128 so far. From our analysis, it is obviously to obtain that the round permutation increases the difficulty to attack Piccolo, because it ensures each 16-bit block can not be involved in the same F-function in the next round. Our attacks take advantage of the fact that round keys of the 14th (resp. 26th) round and 16th (resp. 28th) round are the same; therefore, the time complexities of our attacks will be theoretically increased if the round keys of nearby rounds are not the same. Our attacks presented in this paper are only theoretical cryptanalysis results. Because the total number of rounds of Piccolo-128 is 31, whereas our attack can only achieve 15 rounds theoretically; therefore, our attacks are neither applied to the full-round cipher nor practical.

ACKNOWLEDGEMENTS

This research was supported by National Natural Science Foundation of China(Grant no.61402523, 61272488). We would like to thank editors and anonymous referees for their helpful comments and suggestions.

REFERENCES

1. Shibutani K, Hiwatari A, Akishita T. Piccolo: an ultra-lightweight blockcipher. *Cryptographic Hardware and Embedded Systems-CHES*, Nara, Japan, 2011; 342–357.
2. Jeong K, Kang H, Lee C, Sung J, Hong S. *Biclique cryptanalysis of lightweight block ciphers PRESENT, Piccolo and LED*: Wollongong, Australia, 2012. IACR Cryptology ePrint Archive 2012/621.
3. Ahmadi S, Ahmadian Z, Mohajeri J, Aref M. Low-data complexity biclique cryptanalysis of block ciphers with application to Piccolo and HIGHT. *IEEE Transactions on Information Forensics Security 2014* 2014; **9**(10): 1641–1652.
4. Song J, Lee K, Lee H. Biclique cryptanalysis on lightweight block cipher: HIGHT and Piccolo. *International Journal of Computer Mathematics 2013* 2013; **90**(12): 2564–2580.
5. Wang YF, Wu W, Yu X. Biclique Cryptanalysis of Reduced-Round Piccolo Block Cipher. *Information Security Practice and Experience 2012*, Springer Berlin Heidelberg, Hangzhou China, 2012; 337–352.
6. Isobe T, Shibutani K. Security analysis of the lightweight block ciphers XTEA, LED and Piccolo. *Proceedings of the 17th Australasian Conference on Information Security and Privacy*, Springer-Verlag, 2012; 71–86.
7. Tolba M, Abdelkhalek A, Youssef AM. Meet-in-the-Middle Attacks on Reduced Round Piccolo. *The fourth International Workshop on Lightweight Cryptography for Security & Privacy*, Eminonu, Istanbul, Turkey, 2015; 3–20.
8. Azimi A, Ahmadian Z, Mohajeri J, Aref M. Impossible differential cryptanalysis of Piccolo lightweight block cipher. *11th International ISC Conference on IEEE 2014*, 2014; 89–94.
9. Minier M. On the security of Piccolo lightweight block cipher against related-key impossible differentials. *INDOCRYPT 2013*, Mumbai, India, 2013; 308–318.
10. Wu S, Wang M. Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers. In *INDOCRYPT 2012*. Springer Berlin Heidelberg: Kolkata, India, 2012; 283–302.
11. Bogdanov A, Rijmen V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Designs Codes Cryptography* 2014; **70**(3): 369–383.
12. Abdelraheem MA, Alizadeh J, Alkhzaimi HA. *et al.* Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48. *INDOCRYPT 2015*, Bangalore, India, 2015; 153–179.

13. Alizadeh J, Alkhzaimi HA, Aref MR, Bagheri N, Gauravaram P, Kumar A. Cryptanalysis of SIMON variants with connections. *Radio Frequency Identification: Security and Privacy Issues*, Oxford, UK, 2014; 90–107.
14. Liu M, Chen J. Improved linear attacks on the chinese block cipher standard. *Journal of Computer Science and Technology* 2014; **29**(6): 1123–1133.
15. Bogdanov A, Wang M. Zero correlation linear cryptanalysis with reduced data complexity. In *Fast Software Encryption 2012*. Springer Berlin Heidelberg: Washington DC, USA, 2012; 29–48.
16. Bogdanov A, Leander G, Nyberg K. Integral and multidimensional linear distinguishers with correlation zero. *Proceedings of the 18th international conference on The Theory and Application of Cryptology and Information Security 2012*, Beijing, China, 2012; 244–261.
17. Wen L, Wang M, Bogdanov A, Chen H. Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard. *Information Processing Letters* 2014; **114** (6): 322–330.
18. Wen L, Wang M, Bogdanov A. Multidimensional zero-correlation linear cryptanalysis of E2. *Progress in Cryptology- AFRICACRYPT*, Morocco, France, 2014; 147–164.
19. Bogdanov A, Geng H, Wang M, Wen L, Collard B. Zero-Correlation Linear Cryptanalysis with FFT and Improved attacks on ISO Standards Camellia and CLEFIA. In *Selected Areas in Cryptography - SAC 2013, British Columbia*. Springer Berlin Heidelberg: Canada, 2013; 306–323.
20. Wang YF, Wu W. Improved Multidimensional Zero-Correlation Linear Cryptanalysis and Applications to LBlock and TWINE. In *Australasian Conference on Information Security and Privacy 2014*. Springer International Publishing: Wollongong, Australia, 2014; 1–16.
21. Hermelin M, Cho JY, Nyberg K. *Multidimensional Extension of Matsuis Algorithm 2*. Springer: Berlin Heidelberg, 2009.
22. Hermelin M, Cho JY, Nyberg K. Multidimensional linear cryptanalysis of reduced round serpent. *Information Security and Privacy 2008*, Wollongong, Australia, 2008; 203–215.
23. Bogdanov A, Rijmen V. *Zero correlation linear cryptanalysis of block ciphers*, 2011. IACR Eprint Archive Report 2011/123.
24. Jin CH, Zheng HR, Zhang SW, Shi JH. *Cryptography*. Higher Education Press 2010: Beijing, 2010.