Linear Cryptanalysis Reduced Round of Piccolo-80

Tomer Ashur[1], Orr Dunkelman[2], and Nael Masalha[2]

[1] Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and iMinds, Belgium
[2] Department of Computer Science, University of Haifa, Haifa, Israel

Abstract. Piccolo is a 64-bit lightweight block cipher suitable for constrained environments such as wireless sensor networks. In this paper we evaluate the security of Piccolo-80 against linear cryptanalysis, we present a 6-round linear approximation of Piccolo-80 with probability $1/2 + 2^{-29.04}$. We use this approximation to attack 7-round Piccolo-80 (with whitening keys) with data complexity of 2^{61} known plaintexts and time complexity of 2^{61}. Its extension to an 8-round attack merely increases the time complexity to 2^{70}. This is the best linear attack against Piccolo-80 and it is also applicable to Piccolo-128 as the difference between the two variates is only the number of rounds and the key schedule algorithm. Moreover, we show that the bias in the approximation of the F-function, in some cases, is related to the MSB of the input. We utilize this relation to efficiently extract the MSBs of the whitening keys in the first round.

Key words: Piccolo, Linear Cryptanalysis.

1 Introduction

Due to the continuously evolving technology of constrained hardware devices, such as RFID tags and wireless sensor nodes, there is a huge demand to provide cryptographic security to such resource-constrained devices. As a result, new lightweight block ciphers suitable for such devices have been studied and Piccolo was proposed in CHES 2011 [16].

Piccolo is a 64-bit lightweight block cipher, it supports 80- and 128-bit secret keys. According to the length of the secret key, they are denoted Piccolo-80 and Piccolo-128, respectively. The respective number of rounds of Piccolo-80 and Piccolo-128 is 25 and 31. The iterative structure of Piccolo is a variant of generalized Feistel networks and has 4 branches, each of 16 bits. Its security was evaluated against several cryptanalytic techniques, such as Meet-in-the-Middle (MITM) [7], biclique [6], and impossible differential [3]. In this paper we evaluate the security of Piccolo-80 against linear cryptanalysis, and show a 7-round attack, on the full first 7 rounds (i.e. with whitening keys) of Piccolo-80, using 6-round linear approximation, with data complexity of 2^{61} known plaintexts, and time complexity of 2^{61}. We then extend this attack to 8-round, with data

complexity of 2^{61} known plaintexts, and time complexity of 2^{70}. We experimentally verified the attack on the *first two rounds* and the *first four rounds*. We also show that one can use conditional linear cryptanalysis [5] to attack piccolo. We found that the bias in the approximation of the F-function might be related to the MSB of the input, thus we can increase the bias of the 6-round linear approximation by discarding plaintexts that have specific values of the bits that go to the MSBs of the F-functions in the first round.

Linear cryptanalysis is considered one of the most powerful cryptanalysis techniques. It was introduced by Matsui in [12] as an attack on the full 16-round DES, and later, an improved version is successfully applied to recover the key of the full 16-round DES [13]. Linear cryptanalysis studies statistical linear relations between bits of the plaintext, the ciphertext and the key. These relations are used to compute values of bits of the key, when enough plaintexts and their corresponding ciphertexts are known.

This paper is organized as follows. In Section 2, we briefly introduce the structure of Piccolo. In Section 3 we review the related work. The 7-round and 8-round linear attacks on Piccolo-80 are presented in Section 4. We report the experimental verification of our results in Section 5. Finlay, Section 6 concludes the paper.

2 A Brief Description of Piccolo

Before presenting the structure of Piccolo-80 and Piccolo-128, we give the following notations which are used throughout this paper:

$\|A\|$:	The bit length of A.
$A\|B$:	The concatenation of A and B.
A^L:	The left half of A.
A^R:	The right half of A.
$A[i]$:	The i^{th} bit of A.
$A[i, j, \ldots, k]$:	$A[i] \oplus A[j] \oplus \ldots \oplus A[k]$.

Piccolo is a 64-bit block cipher supporting 80- and 128-bit keys. As shown in Figure 1, the structure of Piccolo is a variant of generalized Feistel networks. The 80- and 128-bit key variates are referred to as Piccolo-80 and Piccolo-128, respectively. The difference between the two key modes lies in the number of rounds and the key schedule. The number of rounds is $r = 25$ for Piccolo-80 and $r = 31$ for Piccolo-128.

The data processing part takes a 64-bit block $X \in \{0,1\}^{64}$, four 16-bit whitening keys $wk_i \in \{0,1\}^{16}$ $(0 \leq i < 4)$ and $2r$ 16-bit round subkeys $rk_i \in \{0,1\}^{16}$ $(0 \leq i < 2r)$ as inputs, and outputs a 64-bit block $Y \in \{0,1\}^{64}$.
Let $P = (P_0, P_1, P_2, P_3)$ be a 64-bit plaintext, where $P_i \in \{0,1\}^{16}$ $(0 \leq i < 3)$,

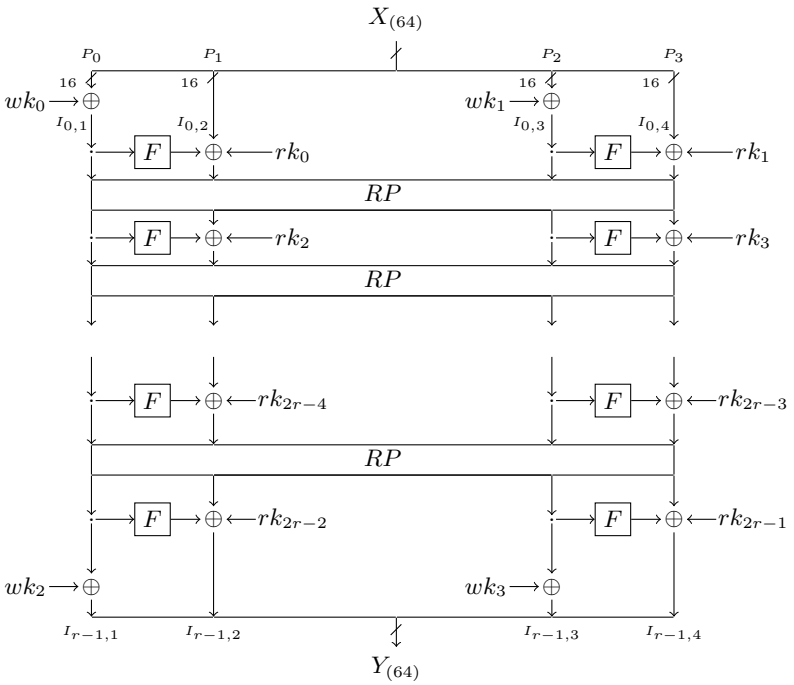

Fig. 1. The Structure of Piccolo

and let (wk_0, wk_1) be a prewhitening key, then the input value $I_0 = (I_{0,0}, I_{0,1}, I_{0,2}, I_{0,3})$ of round 0 is computed as follows:

$$I_{0,0} = P_0 \oplus wk_0, I_{0,1} = P_1, I_{0,2} = P_2 \oplus wk_1, I_{0,3} = P_3.$$

To generate I_{i+1} from I_i $(i = 0, ..., r-2)$, each round is composed of two F-functions $F : \{0,1\}^{16} \rightarrow \{0,1\}^{16}$ and a round permutation $RP : \{0,1\}^{64} \rightarrow \{0,1\}^{64}$.

The F-functions consists of two S-box layers separated by diffusion matrix (see Figure 2). The S-box layer consists of four 4-bit bijective S-boxes S. The round permutation RP (see Figure 3) takes a 64-bit input value $X = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ and generates a 64-bit output value $Y = (x_2, x_7, x_4, x_1, x_6, x_3, x_0, x_5)$.

The 64-bit ciphertext $C = (C_0, C_1, C_2, C_3)$, where $C_i \in \{0,1\}^{16}$ $(0 \leq i < 3)$, is generated as follows:

$$C_0 = I_{r-1,0} \oplus wk_2, \quad C_1 = F(I_{r-1,0}) \oplus I_{r-1,1} \oplus wk_{2r},$$
$$C_2 = I_{r-1,2} \oplus wk_3, \quad C_3 = F(I_{r-1,2}) \oplus I_{r-1,3} \oplus wk_{2r+1}.$$

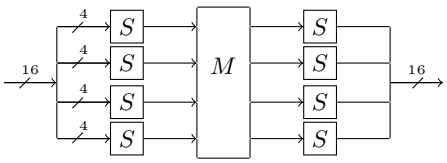

Fig. 2. The F Function of Piccolo

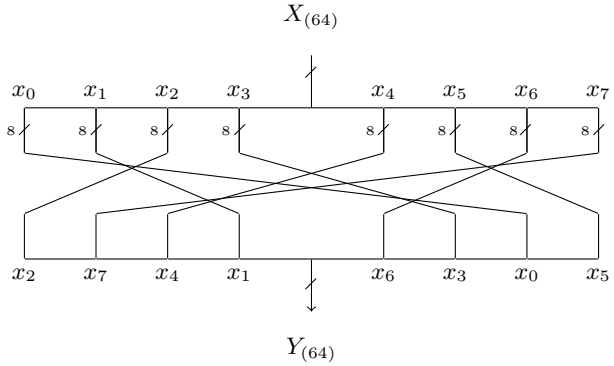

Fig. 3. The Round Permutation (RP) of Piccolo

The key schedule of Piccolo-80 is simple. First, the 80-bit secret key K is defined as follows. Let $k_j = (k_j^L, k_j^R)$ $(j = 0, 1, 2, 3, 4)$, where $k_j \in \{0,1\}^{16}$, $k_j^L \in \{0,1\}^8$ and $k_j^R \in \{0,1\}^8$.

$$K = (k_0, k_1, k_2, k_3, k_4).$$

Four whitening keys (wk_0, wk_1, wk_2, wk_3) and 25 round keys (rk_{2i}, rk_{2i+1}) are generated as follows $(i = 0, 1, ..., 24)$. Let (con_{2i}^{80}) and (con_{2i+1}^{80}) be 16-bit round constants.

– The whitening keys are

$$wk_0 = k_0^L||k_1^R,\ wk_1 = k_1^L||k_0^R,$$
$$wk_2 = k_4^L||k_3^R,\ wk_3 = k_3^L||k_4^R.$$

– The round keys are

$$(rk_{2i}, rk_{2i+1}) = (con_{2i}^{80}, con_{2i+1}^{80}) \oplus \begin{cases} (k_2, k_3), (i \bmod 5) \equiv 0 \text{ or } 2, \\ (k_0, k_1), (i \bmod 5) \equiv 1 \text{ or } 4, \\ (k_4, k_4), (i \bmod 5) \equiv 3, \end{cases}$$

$$(con_{2i}^{80}|con_{2i+1}^{80}) = (c_{i+1}|c_0|c_{i+1}|\{00\}_2|c_{i+1}|c_0|c_{i+1}) \oplus \{0f1e2d3c\}_{16}$$

where c_i is a 5-bit representation of i, e.g., $c_{13} = \{01101\}_2$. The key schedule of Piccolo-128 is very similar, the interested reader is referred to [16].

3 Previous Analysis of Piccolo

Several cryptanalytic results on Piccolo were previously proposed. First, the designers of Piccolo evaluated its security against various attacks and attacked Piccolo-80 up to 17 rounds and Piccolo-128 up to 21 rounds by using related-key attacks [16]. In addition, they used a Meet-in-the-Middle (MITM) attack on 14-round Piccolo-80 and a 21-round Piccolo-128 without whitening keys.

Related-key differential attack on 14-round Piccolo-80 and 21-round Piccolo-128 without whitening keys, are introduced in [14]. The data and time complexities of the attack against Piccolo-80 are $2^{68.19}$ and $2^{68.19}$, respectively, and against Piccolo-128 are $2^{117.77}$ and $2^{117.77}$, respectively.

A Meet-in-the-Middle (MITM) attack on 14-round Piccolo-80 and a 17-round Piccolo-128 without whitening keys, are also proposed in [17]. The data and time complexities of the attack against Piccolo-80 are 2^{48} and $2^{75.39}$, respectively, and against Piccolo-128 are 2^{48} and $2^{126.87}$, respectively.

Biclique cryptanalysis [6] of the full Piccolo-80 without postwhitening keys and a 28-round Piccolo-128 without prewhitening keys was introduced in [18]. These attacks are with data complexity of 2^{48} and 2^{24} chosen ciphertexts, and with time complexity of $2^{78.95}$ and $2^{126.79}$ encryptions, respectively. Later, biclique cryptanalysis of the full round Piccolo-80 and Piccolo-128 was introduced in [11]. These attacks have data complexity of 2^{48} and 2^{24} chosen ciphertexts, and with time complexity of $2^{79.13}$ and $2^{127.35}$ encryptions.

Impossible differential cryptanalysis [3] on Piccolo without whitening keys, is introduced in [1], 12-round and 13-round impossible differential attack on Piccolo-80 and 15-round attack on Piccolo-128. The data and time complexity of the attack against Piccolo-80 is $2^{36.34}$ and $2^{55.18}$ for 12-round and $2^{43.25}$ and $2^{69.7}$ for 13-round. The data and time complexity for 15-round cryptanalysis of Piccolo-128 are $2^{58.7}$ and $2^{125.4}$, respectively.

Multidimensional zero-corellation linear cryptanalysis on Piccolo-128 without whitening keys, was introduced in [9], with 13-round, 14-round and 15-round. The data complexities are $2^{56.8}$, $2^{52.43}$, and $2^{55.6}$, respectively, and time complexities are $2^{117.2}$, $2^{123.09}$, and $2^{126.55}$, respectively. Table 1 shows our results along with the previous cryptanalysis results in the single-key model on Piccolo-80.

Method	Rounds	Whitening Keys Pre/Post	Data	Time
Imp. Diff. [1]	13	None	$2^{43.25}$ CP	$2^{69.7}$
RK Diff. [14]	14	None	$2^{68.19}$ CP	$2^{68.19}$
MITM [10]	14	None	2^{64} KP	2^{73}
MITM [17]	14	None	2^{48} KP	$2^{75.39}$
Biclique [18]	25	Pre	2^{48} CP	$2^{78.95}$
Biclique [11]	25	Both	2^{48} CP	$2^{79.13}$
Linear [Section 4.3]	7	Both	2^{61} KP	2^{61}
Linear [Section 4.4]	8	Both	2^{61} KP	2^{70}
Conditional Linear [Section 4.5]	8	Both	2^{14} CP	2^{14}
Conditional Linear [Section 4.6]	8	Both	2^{54} CP	2^{54}

CP: Chosen Plaintext, KP: Known Pliantext, RK: Related Key, MITM: Meet in the Middle

Table 1. Summary of Attacks on Piccolo-80 in the single-key model

4 A Linear Attack on Reduced Round of Piccolo-80

We now introduce a linear approximation of 6 rounds of Piccolo. First, we construct a linear approximation of the F-function, then we use it to create a 6-round linear approximation.

4.1 Linear Approximation of the F-Function

We start by studying the linear approximation of the F-function. Our approach is to treat the F-function as a black box, i.e., to ignore the internal description of the S-box layers and the diffusion matrix M, and to handle the F-function as a 16-bit S-box. This approach solves any dependency issue between the first layer of S-boxes to the second layer, making the analysis more accurate than merely choosing the number of active S-boxes. The linear approximations of the F-function were found by iterating all the input and output masks. Table 2 lists the highest bias entries of the linear approximations table of the F-function.

4.2 Linear Approximation of 6 Round Piccolo-80

We now extend the linear approximation of the F-function to 6-round linear approximation by concatenating linear approximations, as described in [12] and [2]. Namely, we try to minimize the number of active F-functions as much as possible.

Linear approximation of F	Bias
$0029_x \rightarrow 8808_x$	2^{-5}
$2229_x \rightarrow 0008_x$	2^{-5}
$2922_x \rightarrow 0800_x$	2^{-5}
$1022_x \rightarrow 0088_x$	2^{-5}
$9022_x \rightarrow 0088_x$	2^{-5}
$4046_x \rightarrow 8900_x$	2^{-5}
$C046_x \rightarrow 8900_x$	2^{-5}
$2222_x \rightarrow 8888_x$	-2^{-5}
$2430_x \rightarrow 0608_x$	-2^{-5}
$8862_x \rightarrow 000D_x$	$2^{-5.2}$
$A862_x \rightarrow 000D_x$	$2^{-5.2}$

Table 2. High Bias Linear Approximations of the F-function

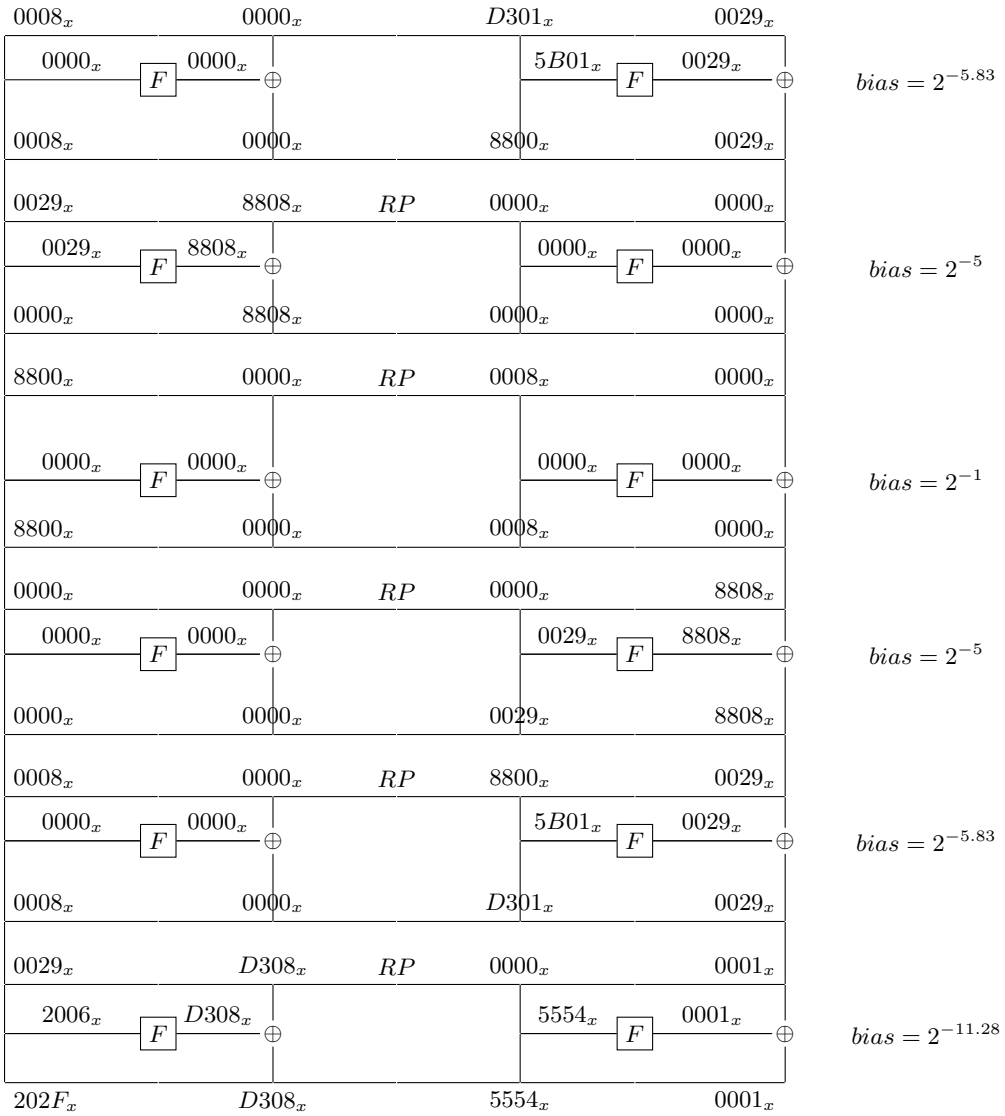

Fig. 4. A 6-Round Linear Approximation of Piccolo-80 with bias=$2^{-29.04}$

Figure 4 describes a 6-round linear approximation. The input mask of the approximation is $\lambda_p = 0008\ 0000\ D301\ 0029_x$ and the output mask is $\lambda_c = 202F\ D308\ 5554\ 0001_x$. This approximation contains 6 active F-functions. The first round contains one active F-function with the linear approximation ($5B01_x \rightarrow 0029_x$) and a bias of $2^{-5.83}$. The second round contains one active F-function with linear approximation ($0029_x \rightarrow 8808_x$) and a bias of 2^{-5}. There are no active F-functions in the third round. The fourth round is similar to the second one with exchanged active and non-active F-functions. The fifth round is the same as the first one. The sixth round contains two active F-functions, the left one with linear approximation ($2006_x \rightarrow D308_x$) and a bias of $2^{-6.5}$ and the right active F-function with linear approximation ($5554_x \rightarrow 0001_x$) and a bias of $2^{-5.87}$. Figure 4 shows the bias of each round in the right side, based on the Pilling-up Lemma [12], we conclude that the total bias of this approximation is $2^{-29.04}$.

The 6 round linear approximation was built by applying the linear approximation ($0029_x \rightarrow 8808_x$), which has maximal bias, to the left side F-function in the second round, and leaving the right side F-function inactive. Then, we extended it up to the first round, by searching the highest biased linear approximation of the F-function with output mask (0029_x). The third round is trivial as it includes no active F-functions. The fourth and fifth rounds are mirror to the second and first rounds. In the sixth round, we searched for the highest biased linear approximations of the F-function with output mask ($D308_x$), for the left side F-functions, and 0001_x for the right side F-function.

Equations (1) and (2) describe the linear relation between plaintext, ciphertext and round subkey bits for the first 6 rounds of Piccolo. The bias of Equation (1) is $2^{-29.04}$. Equation (3) assumes that the xor of the key bits involved in the linear approximation, but not contained in wk_2 and wk_3 equals 0. This assumption only affects the bias sign.

$$\sum_k = P[0,3,5,16,24,25,28,30,31,51] \oplus C[0,18,20,22,24,26,28,30,35,40,41,44,46,47,48,49,50,51,53,61] \quad (1)$$

$$\sum_k = k_1^L[0,1,4,6,7] \oplus k_0^R[0,3] \oplus k_3^R[0,3,5] \oplus k_0^L[3,7] \oplus k_4^L[3,7] \oplus k_4^R[3] \oplus k_1^R[5] \oplus k_2^L[0,1,4,6,7] \oplus k_2^R[3] \quad (2)$$

$$0 = k_1^L[0,1,4,6,7] \oplus k_0^R[0,3] \oplus k_0^L[3,7] \oplus k_1^R[5] \oplus k_2^L[0,1,4,6,7] \oplus k_2^R[3] \quad (3)$$

4.3 A Linear Attack on 7 Rounds of Piccolo-80

According to [12], once an $(n-1)$-round linear approximation is discovered for a given cipher, it is conceivable to attack the cipher by recovering bits of the nth round subkey. In our case, we extract bits from the whitening keys wk_2 and wk_3 in the seventh round, see Figure 5. We shall refer to the subkeys to be recovered from the seventh round as the *target partial subkeys*.

The bias of the linear approximation, described in Figure 4, is $2^{-29.04}$, therefore, according to [15], the attack requires 2^{61} plaintext/ciphertext pairs, in order to retrieve the maximum-biased key, with 98% success rate. The basic algorithm of the attack, described in Algorithm 1, is based on the basic M2 algorithm of [12].

Algorithm 1 Basic Attack Procedure

Data: $\{(p_i, c_i)\}$
Result: wk_2 and wk_3

$wk_2 \leftarrow 0$
$wk_3 \leftarrow 0$
$max\_bias \leftarrow 0$

for each $candidate\_wk_2, candidate\_wk_3 \in \{0,1\}^{16}$ **do**
    $current\_bias \leftarrow 0$
    for each pair (p_i, c_i) **do**
        Decrypt c_i and find A, B, C, D (described in Figure 5)
        if Equation 1 holds **then**
            Increment $current\_bias$ by 1
        else
            Decrement $current\_bias$ by 1
        end if
    end for
    if $|current\_bias| \geq max\_bias$ **then**
        $wk_2 \leftarrow candidate\_wk_2$
        $wk_3 \leftarrow candidate\_wk_3$
        $max\_bias \leftarrow |current\_bias|$
    end if
end for

Output wk_2 and wk_3

The time complexity of this algorithm is the time needed to partially decrypt 2^{61} ciphertexts under 2^{32} subkeys for one round. Thus, the total time complexity is about $\frac{1}{7} \cdot 2^{61} \cdot 2^{32} \approx 2^{90.19}$ Piccolo encryptions, with data complexity of 2^{61} plaintexts, and 2^{61} memory for plaintexts. Obviously, in the case of Piccolo-80 this time complexity is greater than that of exhaustive search. A better algorithm in terms of time complexity is based on the algorithm described in [4], this algorithm utilizes that, in the naive Algorithm 1, for each ciphertext we look only on 32 bits, and decrypt many times the same value under the same key. The resulting algorithm is given as Algorithm 2.

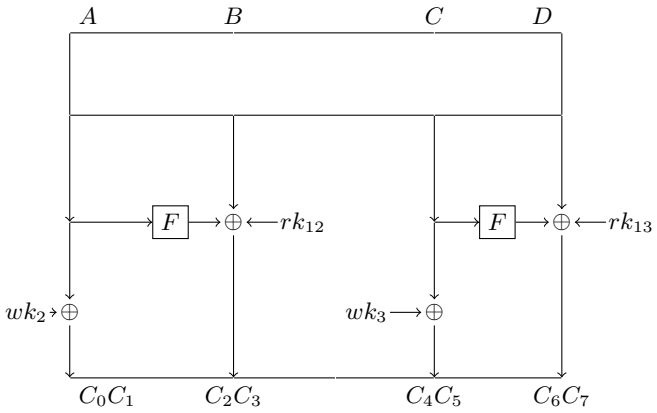

Fig. 5. Decryption of the Seventh Round

Algorithm 2 Improved Attack Procedure

Data: $\{(p_i, c_i = c_0^i c_1^i | c_2^i c_3^i | c_4^i c_5^i | c_6^i c_7^i)\}$
Result: wk_2 and wk_3

Initialize an array A of 2^{32} counters.

for each pair (p_i, c_i) **do**
    $parity \leftarrow p_i[0..63] \oplus c_2^i c_3^i[0..15] \oplus c_6^i c_7^i[0..15]$
    if $parity = 0$ **then**
        Increment $A[c_0^i c_1^i | c_4^i c_5^i]$ by 1
    else
        Decrement $A[c_0^i c_1^i | c_4^i c_5^i]$ by 1
    end if
end for

$wk_2 \leftarrow 0$
$wk_3 \leftarrow 0$
$max\_bias \leftarrow 0$

for each $candidate\_wk_2, candidate\_wk_3 \in \{0,1\}^{16}$ **do**
    $current\_bias \leftarrow 0$
    for each $c_0^i c_1^i | c_4^i c_5^i$ **do**
        Decrypt $c_0^i c_1^i$ and calculate the left F-function parity.
        Decrypt $c_4^i c_5^i$ and calculate the right F-function parity.
        if Equation 1 holds **then**
            Increment $current\_bias$ by $A[c_0^i c_1^i | c_4^i c_5^i]$
        else
            Decrement $current\_bias$ by $A[c_0^i c_1^i | c_4^i c_5^i]$
        end if
    end for
    if $|current\_bias| \gtrsim max\_bias$ **then**
        $wk_2 \leftarrow candidate\_wk_2$
        $wk_3 \leftarrow candidate\_wk_3$
        $max\_bias \leftarrow |current\_bias|$
    end if
end for

Output wk_2 and wk_3

The time complexity of this algorithm is the time needed to partially decrypt 2^{32} ciphertexts under 2^{32} subkeys for one round. Thus, the total time complexity is about $\frac{1}{7} \cdot 2^{32} \cdot 2^{32} \approx 2^{61.19}$ Piccolo encryptions, with data complexity of 2^{61} plaintexts, and memory of 2^{32} counters. We further improve the time complexity of the analysis phase, to $32 \cdot 2^{32} = 2^{37}$, using the fast Fourier transform, suggested in [8], to speed up the computation of the bias for every subkey candidate. Thus, the total time complexity of the algorithm is 2^{61}. The matrix C, in our case, is defined by the following function:

[t]

$$C(wk_2|wk_3, c_0c_1|c_4c_5) = parity(F(wk_2|wk_3 \oplus c_0c_1|c_4c_5))$$

According to proposition 1 and demonstration 1 in [8], C is *level*-32 circulant with type $\underbrace{(2, 2, ..., 2)}_{32 \text{ times}}$, thus we can use the fast algorithm to achieve the improved analysis time. While this seems a futile improvement (form $2^{61.19}$ to 2^{61}) it is used in 8-round attack described next, where it saves a lot.

4.4 A Linear Attack on 8 Rounds of Piccolo-80

We now present the attack on the first eight rounds and extract the key bits of the four whitening keys wk_0, wk_1, wk_2 and wk_3. Equation 1, is used as a relation between input bits of the second round to output bits of the seventh round. The attack is described in Algorithm 3.

The time complexity of this algorithm is the time needed to partially encrypt 2^{32} plaintexts under 2^{32} subkeys for one round and partially decrypt 2^{32} ciphertexts under 2^{32} subkeys for one round. Thus, the total time complexity is about $\frac{2}{8} \cdot 2^{64} \cdot 2^{64} \approx 2^{128}$ encryptions, with data complexity of 2^{61} plaintexts, and memory of 2^{64} counters. We further improve the time complexity of the analysis phase to $64 \cdot 2^{64} = 2^{70}$, using the fast Fourier transform. The matrix C, in this case, is defined by the following function:

$$C(wk_0|wk_1|wk_2|wk_3, p_0p_1|p_4p_5|c_0c_1|c_4c_5) = parity(F(wk_0|wk_1|wk_2|wk_3 \oplus p_0p_1|p_4p_5|c_0c_1|c_4c_5))$$

The matrix C is *level*-64 circulant with type $\underbrace{(2, 2, ..., 2)}_{64 \text{ times}}$.

4.5 Input MSB of the F-Function as a Partitioning Distinguisher

While studying the linear behavior of the F-function in Section 4.1, we observed that in part of the linear approximations, the bias is influenced by the most significant bit MSB of the input. For example, the bias of the approximation $(5B01_x \rightarrow 0029_x)$, described in the first round of Figure 4, equals $2^{-5.83}$. Now we divide the input of the F-function into two disjoint sets, the first set includes input values whose MSB equals 0 and the second set includes input values whose MSB equals 1. Recalculating the bias of $(5B01_x \rightarrow 0029_x)$, for each one of the

Algorithm 3 8-Round Attack Procedure

Data: $\{(p_i = p_0^i p_1^i | p_2^i p_3^i | p_4^i p_5^i | p_6^i p_7^i, c_i = c_0^i c_1^i | c_2^i c_3^i | c_4^i c_5^i | c_6^i c_7^i)\}$
Result: wk_0, wk_1, wk_2 and wk_3

Initialize an array A of 2^{64} counters.

for each pair (p_i, c_i) **do**
    $parity \leftarrow p_2^i p_3^i[0..15] \oplus p_6^i p_7^i[0..15] \oplus c_2^i c_3^i[0..15] \oplus c_6^i c_7^i[0..15]$
    if $parity = 0$ **then**
        Increment $A[p_0^i p_1^i | p_4^i p_5^i | c_0^i c_1^i | c_4^i c_5^i]$ by 1
    else
        Decrement $A[p_0^i p_1^i | p_4^i p_5^i | c_0^i c_1^i | c_4^i c_5^i]$ by 1
    end if
end for

$wk_0 \leftarrow 0$
$wk_1 \leftarrow 0$
$wk_2 \leftarrow 0$
$wk_3 \leftarrow 0$
$max\_bias \leftarrow 0$

for each $candidate\_wk_0, candidate\_wk_1, candidate\_wk_2, candidate\_wk_3 \in \{0,1\}^{16}$ **do**
    $current\_bias \leftarrow 0$
    for each $p_0^i p_1^i | p_4^i p_5^i | c_0^i c_1^i | c_4^i c_5^i$ **do**
        Encrypt $p_0^i p_1^i$ and calculate the left F-function parity.
        Encrypt $p_4^i p_5^i$ and calculate the right F-function parity.
        Decrypt $c_0^i c_1^i$ and calculate the left F-function parity.
        Decrypt $c_4^i c_5^i$ and calculate the right F-function parity.
        if Equation 1 holds **then**
            Increment $current\_bias$ by $A[p_0^i p_1^i | p_4^i p_5^i | c_0^i c_1^i | c_4^i c_5^i]$
        else
            Decrement $current\_bias$ by $A[p_0^i p_1^i | p_4^i p_5^i | c_0^i c_1^i | c_4^i c_5^i]$
        end if
    end for
    if $|current\_bias| \gneq max\_bias$ **then**
        $wk_0 \leftarrow candidate\_wk_0$
        $wk_1 \leftarrow candidate\_wk_1$
        $wk_2 \leftarrow candidate\_wk_2$
        $wk_3 \leftarrow candidate\_wk_3$
        $max\_bias \leftarrow |current\_bias|$
    end if
end for

Output wk_0, wk_1, wk_2 and wk_3

input sets, gives bias $2^{-5.01}$ and $2^{-8.38}$, respectively. The total bias equals to the average of the other two biases. Table 3 lists several such linear approximations of the F-function.

Linear approximation of F	Toatal Bias	Bias when MSB=0	Bias when MSB=1
$5B01_x \rightarrow 0029_x$	$2^{-5.83}$	$2^{-5.01}$	$2^{-8.38}$
$9022_x \rightarrow 0088_x$	$2^{-5.01}$	$2^{-6.05}$	$2^{-4.44}$
$1022_x \rightarrow 0088_x$	$2^{-5.01}$	$2^{-6.05}$	$-2^{-4.44}$
$4046_x \rightarrow 8900_x$	$2^{-5.01}$	$2^{-5.44}$	$2^{-4.71}$
$C046_x \rightarrow 8900_x$	$2^{-5.01}$	$2^{-5.44}$	$-2^{-4.71}$
$62A6_x \rightarrow 0D00_x$	$2^{-5.21}$	$2^{-4.87}$	$2^{-5.71}$
$E2A6_x \rightarrow 0D00_x$	$2^{-5.21}$	$2^{-4.87}$	$-2^{-5.71}$
$662A_x \rightarrow 00D0_x$	$2^{-5.21}$	$2^{-4.87}$	$2^{-5.71}$

Table 3. Bias as a Function of Input's MSB

Utilizing this behavior, the first round of Piccolo can be attacked to extract the MSB of the whitening keys wk_0 or wk_1. For simplicity, we assume that the first round contains only one active F-function on the right side with biases ϵ_{min} for the input set whose MSB equals 1 and ϵ_{max} for the input set whose MSB equals 0. Assuming we have $O(1/(|\epsilon_{max}| - |\epsilon_{min}|)^2)$ pairs of chosen plaintexts, with $X_4[7] = 0$, and their corresponding ciphertexts, we calculate the bias using the linear approximation of the first round, if the observed bias is greater than $\epsilon_{min} + |\epsilon_{max} - \epsilon_{min}|/2 - 2\cdot\sigma$, then we conclude that $X_4[7] \oplus wk_1[15] = 0$ and $wk_1[15] = 0$, otherwise, we conclude that $X_4[7] \oplus wk_1[15] = 1$ and $wk_1[15] = 1$. As an example, we show how to attack the first round, using the linear approximation described in Figure 6 and extract $wk_1[15]$. The input to the active F-function is $X_4X_5 \oplus wk_1$, this implies that the MSB input to F-function is $X_4[7] \oplus wk_1[15]$. Assuming that we have 2^{12} pairs of chosen plaintexts, with $X_4[7] = 0$, we calculate the bias according to Equation 4, if the received bias is greater than $2^{-8.38} + (2^{-5.03} - 2^{-8.38})/2 - 2 \cdot 2^{-1} \cdot 2^{-6} \approx 2^{-7.65}$, then we conclude that $X_4[7] \oplus wk_1[15] = 0$ and $wk_1[15] = 0$, otherwise, we conclude that $wk_1[15] = 1$.

$$P[0, 3, 5, 16, 24, 25, 28, 30, 31, 51] \oplus C[0, 3, 5, 27, 31, 51] = 0 \tag{4}$$

4.6 Extracting The MSB Values of The Whitening Keys wk_0 and wk_1

We now use the behavior described in Section 4.5, to extend the linear attack described in Section 4.3 and extract the MSBs of the whitening keys wk_0 and wk_1. We divide the input of the F-functions in the first round into four disjoint sets, according to the MSB values {00,01,10,11}, and recalculate the bias values $\{\epsilon_0, \epsilon_1, \epsilon_2, \epsilon_3\}$ of the linear approximation, for each one of the sets. For example, the bias of the 6-round linear approximation described in Figure 4 is $2^{-27.3}$ when the MSB of the right F-function input equals 0, and $2^{-34.04}$ when the MSB of

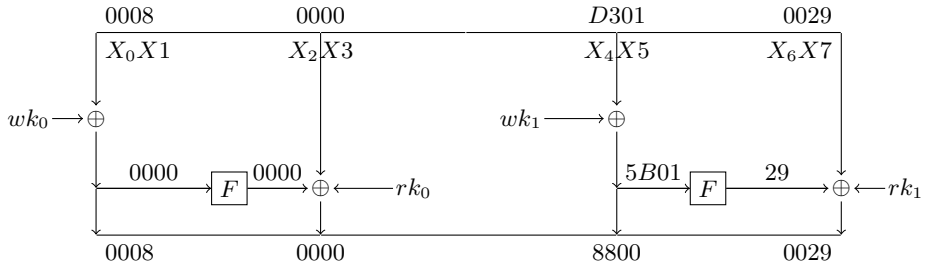

Fig. 6. Extracting MSB of Whitening Key wk_1

the input equals 1. There are only two values of the bias because there is only one active F-function in this case. The same attack used in Section 4.5 can be used to extract the MSB of wk_1.

5 Experimental Verification of a Reduced-Round Attack

In this section we describe the experimental verification of our proposed attacks, which ran on a single core of an Intel Xeon Platinum 8170 CPU, with $2.10GHz$ frequency and $125GB$ RAM. The attack program is based on C++11, compiled by g++ (GCC) version 5.4.0, running on Ubuntu 16.04.5 LTS.

5.1 Partial Verification of 2 Rounds and 4 Rounds Linear Attack

We start with the experimental verification of a reduced-round versions of the attack described in Section 4.3. The attack versions are based on 1-round and 3-round linear approximations, described in Figure 4, with an additional round for key recovery. This is a partial verification of the attack, as we only compute wk_2 in case of 2 rounds and wk_3 in case of 4 rounds.We repeated each version with three different values of plaintext/ciphertext pairs, and for each value it was verified by 100 random keys. Table 5.1 summarizes the results of the attack on the first two and the first four rounds.

5.2 Verification of MSB as a Partitioning Distinguisher

We now show the experimental verification results for the attack described in Section 4.5. Table 3 summarizes the results of the attack on two different linear approximations of the F-function. The experiment consisted of 2^8 random keys, and for each key we tried variable number of plaintexts/ciphertexts.

Rounds	Plaintexts/ Ciphertexts (Per Key)	Attack Time		Succes Rate %	
		Algorithm 1	Algorithm 2	Actual	Expected [15]
2	$2^{13.66}$	15 minutes	32 minutes	28	25
2	$2^{14.66}$	31 minutes	34 minutes	84	71
2	$2^{15.66}$	62 minutes	35 minutes	99.60	98
4	$2^{21.66}$	70.6 hours	23 minutes	36	25
4	$2^{22.66}$	141.1 hours	23 minutes	87.50	69
4	$2^{23.66}$	282.5 hours	23 minutes	99.21	98

Exhuastive search time for two rounds is 1.18 hours and for four rounds is 2.11 hours

Table 4. Summary of 2 and 4 Rounds Attack Verification (100 trials)

Linear approximation of F	Low Bias ϵ_{min}	High Bias ϵ_{max}	Plaintexts/ Ciphertexts (Per Key)	Succes rate of guessing MSB of wk_1
$5B01_x \rightarrow 0029_x$	$2^{-8.38}$	$2^{-5.01}$	2^{12}	56.01%
$5B01_x \rightarrow 0029_x$	$2^{-8.38}$	$2^{-5.01}$	2^{13}	83.43%
$5B01_x \rightarrow 0029_x$	$2^{-8.38}$	$2^{-5.01}$	2^{14}	96.56%
$5B01_x \rightarrow 0029_x$	$2^{-8.38}$	$2^{-5.01}$	2^{15}	100%
$662A_x \rightarrow 00D0_x$	$2^{-5.71}$	$2^{-4.87}$	2^{12}	63.35%
$662A_x \rightarrow 00D0_x$	$2^{-5.71}$	$2^{-4.87}$	2^{13}	75.78%
$662A_x \rightarrow 00D0_x$	$2^{-5.71}$	$2^{-4.87}$	2^{14}	89.91%
$662A_x \rightarrow 00D0_x$	$2^{-5.71}$	$2^{-4.87}$	2^{16}	98.89%

Table 5. Summary of MSB Partitioning Distinguisher Attack Verification (256 trials)

6 Conclusion

In this paper, we proposed linear cryptanalysis of the lightweight block cipher Piccolo-80. We attacked seven and eight rounds of Piccolo-80 using a 6-round linear approximation with bias $2^{-29.04}$. The 7-round attack requires data complexity of 2^{61} known plaintexts. The time complexity is 2^{61} and memory complexity of 2^{32}. The 8-round attack requires data complexity of 2^{61} known plaintexts. The time complexity is 2^{70} and memory complexity of 2^{64}. The attack was verified on reduced versions of two and four rounds of Piccolo-80. In addition, we showed that the F-function bias might be related to the MSB of the input, and presented an attack that uses this property to extract the MSB's of the whitening keys wk_0 and wk_1.

References

1. Azimi, S.A., Ahmadian, Z., Mohajeri, J., Aref, M.R.: Impossible differential cryptanalysis of piccolo lightweight block cipher. In: Information Security and Cryptology (ISCISC), 2014 11th International ISC Conference on, IEEE (2014) 89–94

2. Biham, E.: On matsui's linear cryptanalysis. In: Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings. (1994) 341–355
3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. (1999) 12–23
4. Biham, E., Dunkelman, O., Keller, N.: Linear cryptanalysis of reduced round serpent. In: Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers. (2001) 16–27
5. Biham, E., Perle, S.: Conditional linear cryptanalysis - cryptanalysis of DES with less than 242 complexity. IACR Trans. Symmetric Cryptol. **2018**(3) (2018) 215–264
6. Bogdanov, A., Khovratovich, D., Rechberger, C.: Biclique cryptanalysis of the full AES. In: Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings. (2011) 344–371
7. Bogdanov, A., Rechberger, C.: A 3-subset meet-in-the-middle attack: Cryptanalysis of the lightweight block cipher KTANTAN. In: Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers. (2010) 229–240
8. Collard, B., Standaert, F., Quisquater, J.: Improving the time complexity of matsui's linear cryptanalysis. In: Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings. (2007) 77–88
9. Fu, L., Jin, C., Li, X.: Multidimensional zero-correlation linear cryptanalysis of lightweight block cipher piccolo-128. Security and Communication Networks **9**(17) (2016) 4520–4535
10. Isobe, T., Shibutani, K.: Security analysis of the lightweight block ciphers xtea, led and piccolo. In: Proceedings of the 17th Australasian Conference on Information Security and Privacy. ACISP'12, Berlin, Heidelberg, Springer-Verlag (2012) 71–86
11. Jeong, K., Kang, H., Lee, C., Sung, J., Hong, S.: Biclique cryptanalysis of lightweight block ciphers present, piccolo and LED. IACR Cryptology ePrint Archive **2012** (2012) 621
12. Matsui, M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings. (1993) 386–397
13. Matsui, M.: The first experimental cryptanalysis of the data encryption standard. In: Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings. (1994) 1–11
14. Minier, M.: On the security of piccolo lightweight block cipher against related-key impossible differentials. In: Proceedings of the 14th International Conference on Progress in Cryptology — INDOCRYPT 2013 - Volume 8250, New York, NY, USA, Springer-Verlag New York, Inc. (2013) 308–318
15. Selçuk, A.A.: On probability of success in linear and differential cryptanalysis. J. Cryptology **21**(1) (2008) 131–147
16. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: An ultra-lightweight blockcipher. In: Cryptographic Hardware and Embedded

Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings. (2011) 342–357
17. Tolba, M., Abdelkhalek, A., Youssef, A.M.: Meet-in-the-middle attacks on reduced round piccolo. In: Lightweight Cryptography for Security and Privacy - 4th International Workshop, LightSec 2015, Bochum, Germany, September 10-11, 2015, Revised Selected Papers. (2015) 3–20
18. Wang, Y., Wu, W., Yu, X.: Biclique cryptanalysis of reduced-round piccolo block cipher. In: Information Security Practice and Experience - 8th International Conference, ISPEC 2012, Hangzhou, China, April 9-12, 2012. Proceedings. (2012) 337–352