EPiC Series in Computing

Volume 106, 2025, Pages 99–113

Proceedings of the 20th Asia Joint Conference on Information Security

Improved Integral Cryptanalysis on Reduced-Round Piccolo

Naoki Shibayama and Yasutaka Igarashi

Tokyo University of Science, 2641 Yamazaki, Noda, Chiba 278-8510, Japan
7323703@ed.tus.ac.jp, yasutaka@rs.tus.ac.jp

Abstract

Piccolo is a 64-bit block cipher proposed by Shibutani *et al.* in 2011, supporting 80-bit and 128-bit keys. In higher order differential cryptanalysis, computer experiments have verified that Piccolo has a 6-round characteristic using the 32-nd order differential, which was theoretically extended to a 7-round characteristic using the 48-th order differential. The integral attack is cryptanalysis, similar to a higher order differential cryptanalysis. An investigation of integral characteristics by establishing the Mixed Integer Linear Programming (MILP) model based on bit-based division property has revealed the existence of a 7-round integral characteristic using a 63-rd order differential, and a search using the Satisfiability Problem (SAT) has found a same-round integral characteristic using the 56-th order differential. In this paper, we introduce the integral property based on the frequency distribution, clarify the reason for the 5-round integral characteristic using the 16-th order differential we found by computer experiment, and derive the 7-round integral characteristic by applying the 2-round extension to this. Then, we show that if the property of the frequency distribution can be used in the attack equation, the key can be identified more efficiently than the conventional method.

1 Introduction

Information and communication technology has developed notably in recent years. Lightweight block ciphers are essential in ensuring data security in resource-constrained scenarios like the Internet of Things.

Piccolo [1], the lightweight block cipher that can be implemented in hardware with a low circuit size, was proposed at CHES 2011. It has a 64-bit block length supporting key lengths of 80-bit and 128-bit. The rounds are 25 and 31 for 80-bit and 128-bit keys, respectively.

A higher order differential attack is a generic and one of the algebraic attacks on a block cipher. It exploits the property of a higher order differential proposed by Lai [2] and utilizes the degree of output. Knudsen *et al.* [3] proposed integral cryptanalysis as a similar higher order differential cryptanalysis method, generalizing square attack [4]. It exploits the integral property that the Exclusive-OR (XOR) sum of the output sets corresponding to multiple chosen plaintexts generally becomes zero. Later, Todo proposed the division property [6], [7], which generalized the integral property in 2015. Todo *et al.* further proposed the bit-based division

A. Yamada, H.K. Kim, Y. Wang and T.-T. Tsai (eds.), AsiaJCIS 2025 (EPiC Series in Computing, vol. 106), pp. 99–113

property (BDP) [8]. Subsequently, Xiang *et al.* found better integral characteristics of 6 lightweight block ciphers by establishing the MILP model based on BDP [9].

In a previous study, Shibayama *et al.* [10] reported that Piccolo has been found to have the 6-round characteristic using the 32-nd order differential by computer experiment and the 7-round characteristic using the 48-th order differential, a theoretical 1-round extension of the 6-round one to the plaintext direction. Exploiting the 7-round characteristic, the 48-th order differential attack on 11 rounds Piccolo is possible with 2^{51} blocks of plaintext and $2^{127.9}$ times of data processing. Then, Sato *et al.* [11] investigated the integral property using BDP with MILP and showed the existence of a 7-round integral characteristic using a 63-rd order differential. In addition, Utsumi *et al.* [12] found the same rounds' characteristic using the 56-th order differential by searching for BDP using SAT [13].

Our Contributions

This paper reports the integral cryptanalysis on reduced-round Piccolo. By introducing the integral property based on frequency distribution, we clarify the reason for the 5-round integral characteristic using the 16-th order differential we discovered by computer experiment. Then, we obtain the 7-round integral characteristic, which is a theoretical 2-round extension of the 5-round one and corresponds to the previous best higher order differential characteristic. Furthermore, we present that if the property of the frequency distribution can be used in the attack equation, the key can be identified more efficiently than the conventional method. We also show experimental results of the improved key recovery attack against the 6-round Piccolo.

Organization

This paper is organized as follows. Section 2 illustrates the specification of Piccolo. In Section 3, we introduce the definition of the integral property and an explanation of the attack equation. In Section 4, we show the results of the integral characteristics of Piccolo by computer experimentation and its extension. Then, Section 5 describes the key recovery attack for the reduced-round Piccolo using the property of the frequency distribution. Section 6 finally concludes the paper.

2 Piccolo

This section briefly describes the specification of the block cipher Piccolo. Piccolo has a block length of 64-bit, supporting 80-bit and 128-bit key lengths. The number of rounds varies depending on the key length, with 25 or 31 rounds for 80 or 128 bits, respectively. However, both variants of Piccolo share similar processes in the data processing part and key scheduling. Piccolo consists of a 16-bit word 4-line generalized Feistel network underlying lightweight functions, such as the F function and key scheduling, which are designed to be implemented in hardware with a small number of gates.

Fig. 1 shows the data processing part of Piccolo. $\mathbf{X}^{(1)}$ and $\mathbf{C}^{(r)}$ represent its input 64-bit plaintext and output ciphertext, where r=25 and 31 for 80-bit and 128-bit key lengths.

Let $\mathbf{X}^{(i)}$=$(X_0^{(i)}, X_1^{(i)}, X_2^{(i)}, X_3^{(i)})$, $X_j^{(i)} = (x_{j,0}^{(i)}, x_{j,1}^{(i)}, x_{j,2}^{(i)}, x_{j,3}^{(i)})$, $x_{j,\ell}^{(i)} \in \mathrm{GF}(2)^4$ and $\mathbf{C}^{(i)} = (C_0^{(i)}, C_1^{(i)}, C_2^{(i)}, C_3^{(i)})$, $C_j^{(i)} = (c_{j,0}^{(i)}, c_{j,1}^{(i)}, c_{j,2}^{(i)}, c_{j,3}^{(i)})$, $c_{j,\ell}^{(i)} \in \mathrm{GF}(2)^4$ be the i-th round input and output, respectively, where $1 \leq i \leq r$, $0 \leq j \leq 3$, $0 \leq \ell \leq 3$. $(WK_0, WK_1, \cdots, WK_3)$, $WK_j = (wk_{j,0}, wk_{j,1}, wk_{j,2}, wk_{j,3})$, $wk_{j,\ell} \in \mathrm{GF}(2)^4$ are four 16-bit whitening keys, $(RK_0, RK_1, \cdots, RK_{2r-1})$, $RK_{j'} = (rk_{j',0}, rk_{j',1}, rk_{j',2}, rk_{j',3})$, $rk_{j',\ell} \in \mathrm{GF}(2)^4$ are $2r$ 16-bit round keys, where

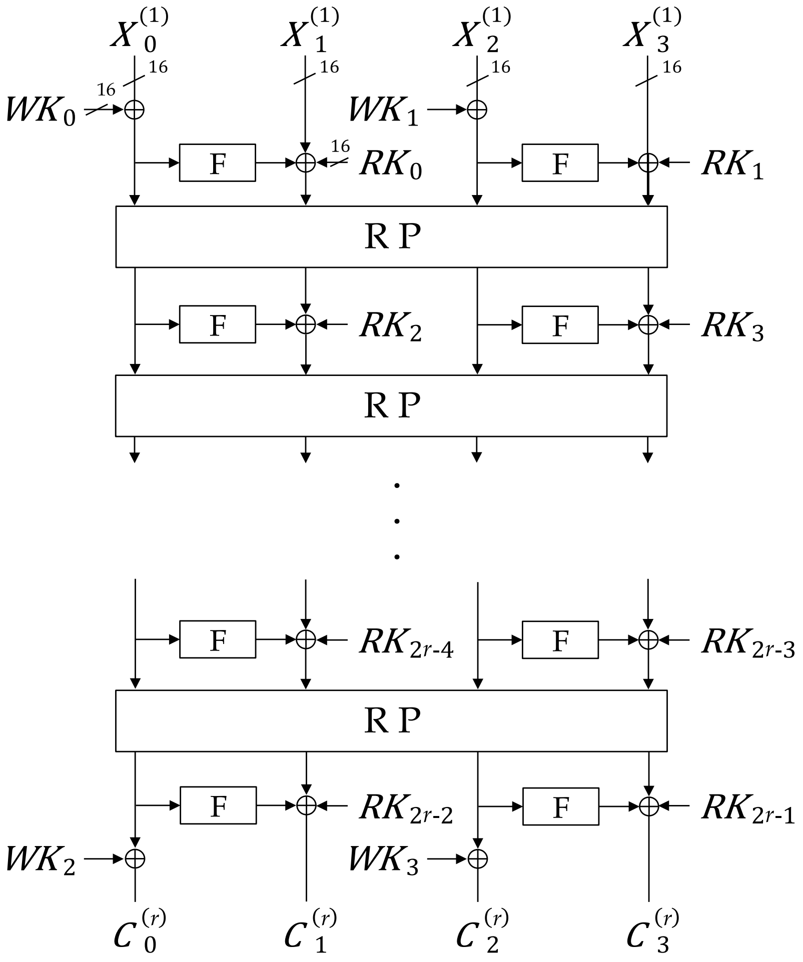

Figure 1: Data processing part of Piccolo.

Table 1: S-box S.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	E	4	B	2	3	8	0	9	1	A	7	F	6	C	5	D

$0 \leq j^{'} < 2r$. The symbol $\oplus$ represents the XOR operation in the figure. The F function is the 16-bit bijective nonlinear function with SPS structure shown in Fig. 2. It consists of two S-box layers, each applying four 4-bit S-boxes in parallel and a matrix layer between the two S-box layers. Table 1 shows the S-box S in hexadecimal format, and the diffusion matrix $\mathbf{M}$ is given by (1).

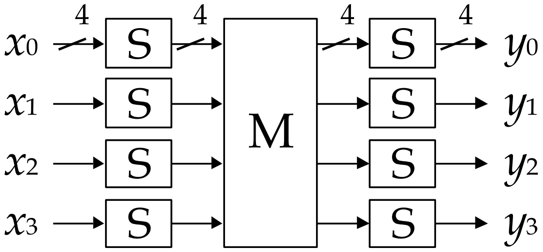

Figure 2: F function.

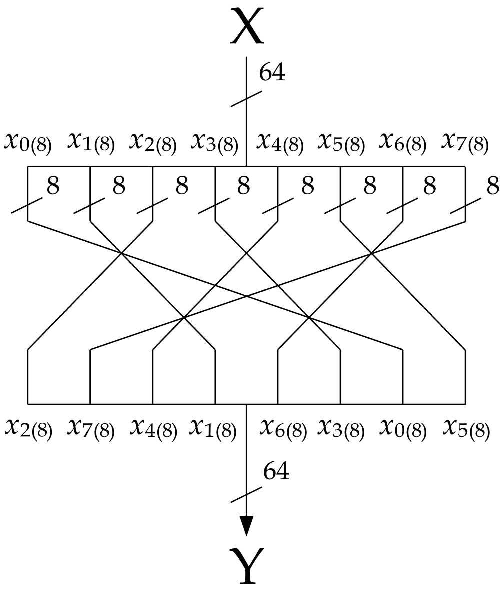
X
64
$x_{0(8)}$ $x_{1(8)}$ $x_{2(8)}$ $x_{3(8)}$ $x_{4(8)}$ $x_{5(8)}$ $x_{6(8)}$ $x_{7(8)}$
8
$x_{2(8)}$ $x_{7(8)}$ $x_{4(8)}$ $x_{1(8)}$ $x_{6(8)}$ $x_{3(8)}$ $x_{0(8)}$ $x_{5(8)}$
64
Y

Figure 3: Round Permutation.

$$\mathbf{M} = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}, \tag{1}$$

where the multiplication between matrices and vectors is performed over GF(2^4) defined by an irreducible polynomial z^4+z+1. Also, RP denotes the round permutation in each round except the final round. In RP, even bytes ($x_{0(8)}$, $x_{2(8)}$, $x_{4(8)}$, $x_{6(8)}$) are shifted left ($x_{2(8)}$, $x_{4(8)}$, $x_{6(8)}$, $x_{0(8)}$), while odd bytes ($x_{1(8)}$, $x_{3(8)}$, $x_{5(8)}$, $x_{7(8)}$) are shifted right ($x_{7(8)}$, $x_{1(8)}$, $x_{3(8)}$, $x_{5(8)}$), as shown in Fig. 3.

Since the relations between the round keys will not be used in our attack, we omit the key schedule algorithm here. Please refer to [1] for the details of the specification.

3 Integral Attack

The idea of integral attack comes from the square attack, which was first proposed by Daemen *et al.* [4], and then formulated by Knudsen and Wagner in 2002 [3].

3.1 Integral Property

An integral attack generally takes advantage of the property that the XOR of all outputs corresponding to the selected inputs becomes zero.

Definition 1 (**Integral property**)

Let a set of 2^ℓ elements of ℓ bits values be $\mathbf{X}$=$\{X_i|X_i{\in}\{0,1\}^\ell, 0{\le}i{<}2^\ell\}$. We categorize a set $\mathbf{X}$ into the following four properties.

- Constant (C) : if $\forall i, j$, $X_i = X_j$,
- All (A) : if $\forall i, j$, $i \neq j \Leftrightarrow X_i \neq X_j$,
- Balance (B) : if $\bigoplus_i X_i = 0$,
- Unknown (U) : Others.

In this paper, the symbols c, $A_{(1)}$, b, and u indicate the integral property of 1-bit values, which are Constant, All, Balance, and Unknown, respectively. Then, if the integral property of 1-nibble value $x_{j,\ell}^{(i)}$ is Constant, we present this as $\{x_{j,\ell}^{(i)}\}$ = C. Multiple-nibble values are expressed similarly. If the integral property of 2^ℓ elements of ℓ-bit values is All, it is expressed as $\mathrm{A}_{(\ell)}$. Moreover, when $A_{(\ell)}$ is divided into $m\,(\geq 2)$ nibbles, we denote this as follows.

$$\mathrm{A}_{(\ell)} = (\mathrm{A}^0\,\mathrm{A}^1\,\cdots\,\mathrm{A}^{m-1}), \tag{2}$$

where $\ell = 4m$. For example, 8-th order differential $\mathrm{A}_{(8)}$ is written as $(\mathrm{A}^0\,\mathrm{A}^1)$. Furthermore, if the integral property of each nibble value in the word (=4-nibble) value is the same, for example, $\{X_j^{(i)}\} = (\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{A}^2\,\mathrm{A}^3)$, this can be expressed as $\{X_j^{(i)}\} = \mathbf{A}$.

Let $f_i(X_j)$ be the number of occurrences (frequency distribution) of $X_j = i$, where $0 \leq i < 2^m$, $0 \leq j < 2^\ell$, $X_j \in \mathrm{GF}(2)^m$, and $\sum f_i(X_j) = 2^\ell$. Moreover, let $f_i^{(2)}(X_j)$ be the number of occurrences of $X_j = i$ modulo 2, which is also known as the modulo 2 frequency distribution. Hence, $f_i^{(2)}(X_j)$ is zero if $f_i(X_j)$ is even and one if it is odd.

Definition 2 (**Integral property based on frequency distribution**)

We define the following two properties of the set of 2^ℓ elements of $m\,({<}\ell)$ bits values $\{X_j|X_j \in \{0,1\}^m, 0 \leq j < 2^\ell\}$.

- all (a) : if $\forall i, j$, $f_i(X_j) = 2^{\ell-m}$,
- Even (E) : if $\forall i, j$, $f_i^{(2)}(X_j) = 0$.

For example, let (x_0, x_1) be 2-nibble data, and its integral property is ($\mathrm{A}^0\,\mathrm{A}^1$). Consequently, the value of $0, 1, \cdots, 2^8-1$ appears once in (x_0, x_1). On the other hand, if its integral property is (a a), the value of $0, 1, \cdots, 2^4-1$ appears 2^4 times in x_0 and x_1, respectively. Here, if $\ell = m$, the property 'all' is the same as the property All. In addition, the property 'all' satisfies the property Even, and has a more distinctive feature than the property Even because the number of occurrences of all possible m-bit data is equal.

Property 1

If the integral property of the data is Constant, All, Balance, 'all,' or Even, the XOR sum is 0.

The attacker first encrypts a set of chosen plaintexts and investigates the propagation of the integral property. Suppose 2^ℓ chosen plaintexts are used, and the integral property of the output from a reduced r-round cipher is Constant, All, Balance, 'all,' or Even. In that case, we say that the cipher has an r-round integral characteristic using the ℓ-th order differential. Then, the attacker estimates the key by exploiting the characteristic from Property 1.

3.2 Attack Equation

Consider a block cipher with an iterative r-round. Let $H(X)\in\mathrm{GF}(2)^m$ be a part of the $(r-1)$-th round output, and $C(X)\in\mathrm{GF}(2)^n$ be the ciphertext corresponding to the plaintext $X\in\mathrm{GF}(2)^n$. The $(r-1)$-th round intermediate value $H(X)$ is expressed as

$$H(X) = E_{r-1}(X; K_1, K_2, \cdots, K_{r-1}), \tag{3}$$

where $K_i\in\mathrm{GF}(2)^s$ is the i-th round key and $E_i(\cdot)$ is a function of $\mathrm{GF}(2)^n \times \mathrm{GF}(2)^{s\times i} \rightarrow \mathrm{GF}(2)^m$.

The following equation can be given if Property 1 is observed for E_{r-1}.

$$\bigoplus_{x\in\{X\}} H(x) = 0 \tag{4}$$

Let $\widetilde{E}(\cdot)$ be a decryption function that calculates $H(X)$ from a ciphertext $C(X)$.

$$H(X) = \widetilde{E}(C(X); K_r), \tag{5}$$

where K_r denotes the r-th round key to decrypt $H(X)$ from $C(X)$. We can derive the following equation from (4) and (5).

$$\bigoplus_{c\in\{C(X)\}} \widetilde{E}(c; K_r) = 0 \tag{6}$$

Since equation (6) holds with probability one if the estimation of the key K_i is correct and with probability 2^{-m} if the estimation is wrong, the attacker can recover the key K_r by solving (6). In the following, (6) is called an attack equation.

4 Integral Characteristics of Piccolo

In this section, we explain the distinguisher of Piccolo by using the higher order differential and BDP.

4.1 Previous Results

4.1.1 Higher order differential

Shibayama *et al.* [10] applied a search algorithm of higher order differential and discovered the characteristics from the 1-st round input to the 6-th round output can be expressed as follows.

$$\begin{aligned} &(\texttt{A32-i}) \quad (\,\mathbf{C\,C\,A\,A}\,) \xrightarrow{6r} (\,\mathbf{U\,U\,U\,a}\,), \\ &(\texttt{A32-ii}) \quad (\,\mathbf{A\,A\,C\,C}\,) \xrightarrow{6r} (\,\mathbf{U\,a\,U\,U}\,). \end{aligned}$$

In the above characteristics, the left-hand side and the right-hand side of the formula signify the input property and the 6-th round output property, respectively. Then, by applying a round extension [5] to these, they derived the following 7-round characteristics using the 48-th order differential, theoretically extended by one round to the plaintext direction.

$$\begin{aligned} &(\texttt{A48-i}) \quad (\,(\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{C}\,\mathrm{C})\,\mathbf{A}\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^2\,\mathrm{A}^3)\,\mathbf{A}\,) \xrightarrow{7r} (\,\mathbf{U\,U\,U\,a}\,), \\ &(\texttt{A48-ii}) \quad (\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^0\,\mathrm{A}^1)\,\mathbf{A}\,(\mathrm{A}^2\,\mathrm{A}^3\,\mathrm{C}\,\mathrm{C})\,\mathbf{A}\,) \xrightarrow{7r} (\,\mathbf{U\,a\,U\,U}\,). \end{aligned}$$

4.1.2 BDP

Sato *et al.* [11] investigated the number of rounds of the best characteristics using the 8-th, 12-th, 24-th, 32-nd, 48-th, and 63-rd order differential with MILP. Then, they showed that 7-round integral characteristics were obtained using a 63-rd order differential. Moreover, they claimed that their computer experiments found no 7-round integral characteristics using the 48-th order differential. However, one part of the constraints used in MILP is erroneous[1], and the path of the characteristics available for the attack is not described at all. For this reason, we expect Sato *et al.*'s BDP search method using MILP to be improved. Furthermore, Utsumi *et al.* [12] also found the following 7-round integral characteristic using SAT.

$$(\texttt{A56}) \quad (\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^0\,\mathrm{A}^1)\,\mathbf{A\,A\,A}\,) \xrightarrow{7r} (\,\mathbf{U\,B\,U}\,((bbuu)(bbuu)(bbuu)(bbuu))\,)^2$$

4.2 Search Results

In our search, the secret keys were set randomly, and the integral characteristics using the word-oriented 16-th and 32-nd order differential were investigated.

Using the 16-th order differential, we found 5-round integral characteristics:

$$\begin{aligned} &(\texttt{A16-i}) \quad (\,\mathbf{C}\,(\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{C}\,\mathrm{C})\,\mathbf{C}\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^2\,\mathrm{A}^3)\,) \xrightarrow{5r} (\,\mathbf{U\,U\,U\,a}\,), \\ &(\texttt{A16-ii}) \quad (\,\mathbf{C}\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^0\,\mathrm{A}^1)\,\mathbf{C}\,(\mathrm{A}^2\,\mathrm{A}^3\,\mathrm{C}\,\mathrm{C})\,) \xrightarrow{5r} (\,\mathbf{U\,a\,U\,U}\,). \end{aligned}$$

The path of (A16-i) is depicted in the circuit from the 3-rd round input to the 7-th round output of Fig. 4. The keys' inputs are omitted in Fig. 4 because those do not influence the characteristic. Then, using the 32-nd order differential, we obtained the 6-round integral characteristics consistent with those of (A32-i) and (A32-ii).

[1] In [11], the 13-th linear equation '$t_4 - t_{10} - t_{28} - t_{50} - t_{77} - y_{12} = 0$' for XOR operation in the matrix **M** is incorrect; '$t_4 + t_{10} + t_{28} + t_{50} + t_{77} - y_{12} = 0$' is correct.

[2] While the output pattern of the characteristic before applying RP is shown in [12], the one after applying RP is shown here in the same way as another characteristic.

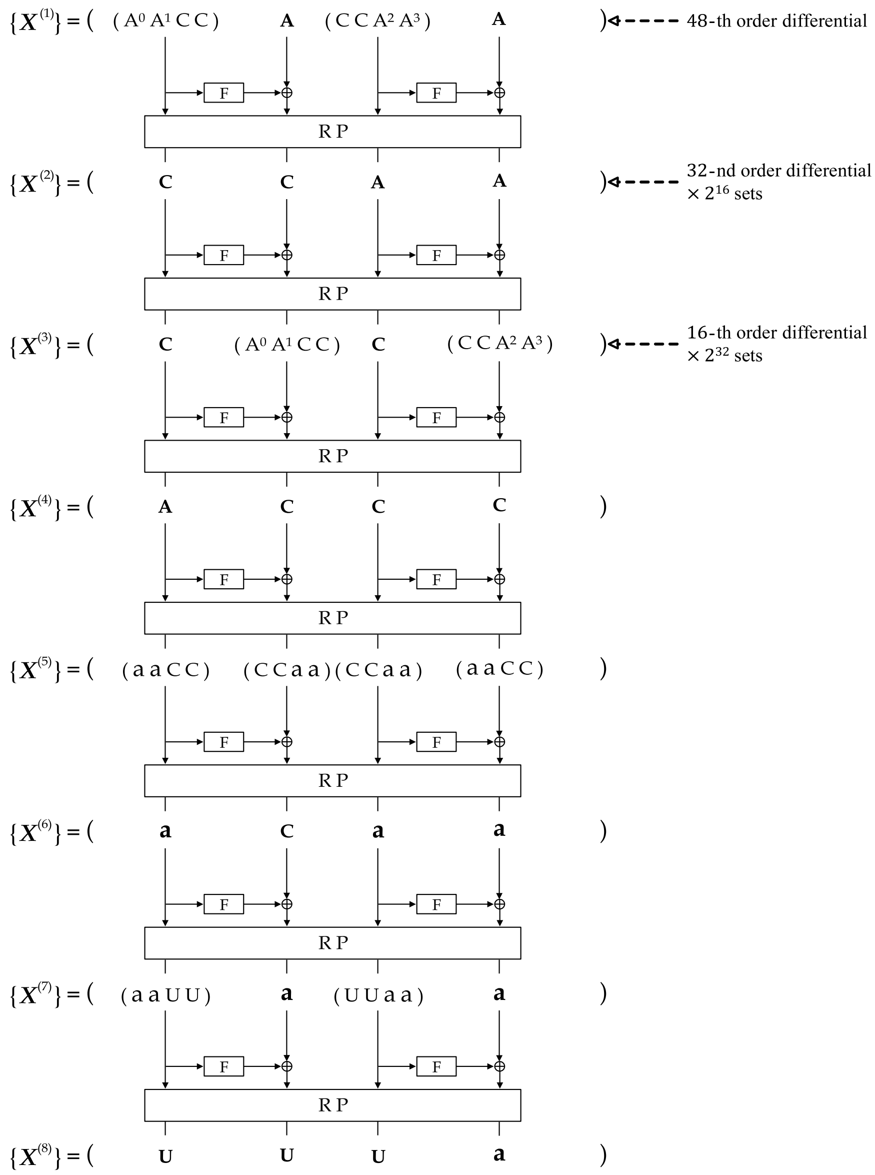
{X(1)} = ((A0 A1 C C) A (C C A2 A3) A)
48-th order differential
F
RP
{X(2)} = (C C A A)
32-nd order differential × 2^16 sets
{X(3)} = (C (A0 A1 C C) C (C C A2 A3))
16-th order differential × 2^32 sets
{X(4)} = (A C C C)
{X(5)} = ((a a C C) (C C a a) (C C a a) (a a C C))
{X(6)} = (a C a a)
{X(7)} = ((a a U U) a (U U a a) a)
{X(8)} = (U U U a)

Figure 4: The 5-round characteristic using the 16-th order differential and its extension.

4.3 Analysis of 16-th Order Differential

By closely analyzing nibble values, we show why the above 5-round integral characteristics using the 16-th order differential hold. In Fig. 4, let $x^{(1)}_{1,0}$, $x^{(1)}_{1,1}$, $x^{(1)}_{3,2}$, and $x^{(1)}_{3,3}$ be the variable for the 3-rd round input, in which the 16-th order differential is input, and $c^{(5)}_{3,k}$ $(0 \leq k \leq 3)$ be the output after the 7-th round encryption, in which the property 'all' appears. Here, we explain why the property 'all' appears in $c^{(5)}_{3,k}$ of the characteristic of (A16-i).

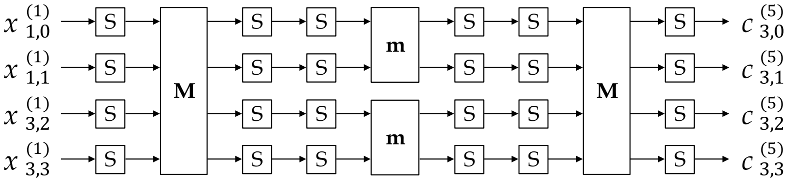

Figure 5: Equivalent circuit from $(x_{1,0}^{(1)}, x_{1,1}^{(1)}, x_{3,2}^{(1)}, x_{3,3}^{(1)})$ to $c_{3,k}^{(5)}$ $(0 \leq k \leq 3)$.

Fig. 5 shows the equivalent circuit from $x_{1,0}^{(1)}$, $x_{1,1}^{(1)}$, $x_{3,2}^{(1)}$, and $x_{3,3}^{(1)}$, where the 16-th order differential is input to $c_{3,k}^{(5)}$. Then, the matrix $\mathbf{m}$ in the figure is a submatrix of the matrix $\mathbf{M}$ and is represented by

$$\mathbf{m} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}. \tag{7}$$

Although additions of variables in constant terms are included, they were omitted because they do not affect the characteristic. In Fig. 5, since the S-box is bijective nonlinear and the matrices $\mathbf{M}$ and $\mathbf{m}$ are linear, the 16-bit data $(x_{1,0}^{(1)}, x_{1,1}^{(1)}, x_{3,2}^{(1)}, x_{3,3}^{(1)})$ and $C_3^{(5)}$ are one-to-one correspondence. Therefore, by inputting the 16-th order differential to $(x_{1,0}^{(1)}, x_{1,1}^{(1)}, x_{3,2}^{(1)}, x_{3,3}^{(1)})$, the values $0, 1, \cdots, 2^{16}-1$ appear once in the word data $C_3^{(5)}$. Since the value of $0, 1, \cdots, 2^4-1$ appears 2^4 times in the nibble data $c_{3,k}^{(5)}$, the property 'all' appears in $c_{3,k}^{(5)}$.

Likewise, the reasons for the characteristic of (A16-ii) can be clarified.

4.4 32-nd and 48-th Order Differential

This subsection describes the characteristics derived by applying a round extension to the 5-round integral characteristics using the 16-th order differential.

Let $\mathrm{F}_{\mathrm{J}}^{(i)}(\cdot) = (f_{\mathrm{J},0}^{(i)}(\cdot), f_{\mathrm{J},1}^{(i)}(\cdot), f_{\mathrm{J},2}^{(i)}(\cdot), f_{\mathrm{J},3}^{(i)}(\cdot))$, $f_{\mathrm{J},\ell}^{(i)}(\cdot) \in \mathrm{GF}(2)^4$ be the output of the F function in the i-th round, where $\mathrm{J} \in \{\mathrm{L}, \mathrm{R}\}$, $0 \leq \ell \leq 3$. Focusing on the structure of Piccolo, except for adding the constant terms in the keys, the relations between the 1-st round input $x_{j,\ell}^{(1)}$ $(0 \leq j \leq 3)$ and the 2-nd round input $x_{j,\ell}^{(2)}$ are given by

$$\begin{aligned} (x_{0,0}^{(2)}, x_{0,1}^{(2)}) &= (f_{\mathrm{L},0}^{(1)}(X_0^{(1)}) \oplus x_{1,0}^{(1)}, f_{\mathrm{L},1}^{(1)}(X_0^{(1)}) \oplus x_{1,1}^{(1)}), & (8) \\ (x_{0,2}^{(2)}, x_{0,3}^{(2)}) &= (f_{\mathrm{R},2}^{(1)}(X_2^{(1)}) \oplus x_{3,2}^{(1)}, f_{\mathrm{R},3}^{(1)}(X_2^{(1)}) \oplus x_{3,3}^{(1)}), & (9) \\ X_1^{(2)} &= (x_{2,0}^{(1)}, x_{2,1}^{(1)}, x_{0,2}^{(1)}, x_{0,3}^{(1)}), & (10) \\ (x_{2,0}^{(2)}, x_{2,1}^{(2)}) &= (f_{\mathrm{R},0}^{(1)}(X_2^{(1)}) \oplus x_{3,0}^{(1)}, f_{\mathrm{R},1}^{(1)}(X_2^{(1)}) \oplus x_{3,1}^{(1)}), & (11) \\ (x_{2,2}^{(2)}, x_{2,3}^{(2)}) &= (f_{\mathrm{L},2}^{(1)}(X_0^{(1)}) \oplus x_{1,2}^{(1)}, f_{\mathrm{L},3}^{(1)}(X_0^{(1)}) \oplus x_{1,3}^{(1)}), & (12) \\ X_3^{(2)} &= (x_{0,0}^{(1)}, x_{0,1}^{(1)}, x_{2,2}^{(1)}, x_{2,3}^{(1)}). & (13) \end{aligned}$$

First, we describe the 6-round integral characteristic theoretically derived by extension of the characteristic of (A16-i) to 1-round of the plaintext direction. From (8) $\sim$ (13), if $\{X_0^{(1)}\} =$

$\{X_1^{(1)}\} = \mathbf{C}$,

$$\begin{aligned}
(x_{0,0}^{(2)}, x_{0,1}^{(2)}) &= (c_0, c_1),\\
(x_{0,2}^{(2)}, x_{0,3}^{(2)}) &= (f_{\mathrm{R},2}^{(1)}(X_2^{(1)}) \oplus x_{3,2}^{(1)}, f_{\mathrm{R},3}^{(1)}(X_2^{(1)}) \oplus x_{3,3}^{(1)}),\\
X_1^{(2)} &= (x_{2,0}^{(1)}, x_{2,1}^{(1)}, c_2, c_3),\\
(x_{2,0}^{(2)}, x_{2,1}^{(2)}) &= (f_{\mathrm{R},0}^{(1)}(X_2^{(1)}) \oplus x_{3,0}^{(1)}, f_{\mathrm{R},1}^{(1)}(X_2^{(1)}) \oplus x_{3,1}^{(1)}),\\
(x_{2,2}^{(2)}, x_{2,3}^{(2)}) &= (c_4, c_5),\\
X_3^{(2)} &= (c_6, c_7, x_{2,2}^{(1)}, x_{2,3}^{(1)}),
\end{aligned}$$

where $c_0, c_1, \cdots, c_7$ are constants. Since the F function is a bijective nonlinear function, the 32-bit data $(X_2^{(1)}, X_3^{(1)})$ and $(x_{0,2}^{(2)}, x_{0,3}^{(2)}, x_{1,0}^{(2)}, x_{1,1}^{(2)}, x_{2,0}^{(2)}, x_{2,1}^{(2)}, x_{3,2}^{(2)}, x_{3,3}^{(2)})$ are one-to-one correspondence. Hence, by inputting the 32-nd order differential;

$$\{\mathbf{X}^{(1)}\} = (\,\mathbf{C}\,\mathbf{C}\,\mathbf{A}\,\mathbf{A}\,),$$

the following 32-nd order differential appears in the 2-nd round input after 1-round encryption.

$$\{\mathbf{X}^{(2)}\} = (\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^0\,\mathrm{A}^1)\,(\mathrm{A}^2\,\mathrm{A}^3\,\mathrm{C}\,\mathrm{C})\,(\mathrm{A}^4\,\mathrm{A}^5\,\mathrm{C}\,\mathrm{C})\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^6\,\mathrm{A}^7)\,)$$

Thus, the 32-nd order differential $(\,\mathbf{C}\,\mathbf{C}\,\mathbf{A}\,\mathbf{A}\,)$ in the 1-st round input will lead to 2^{16} sets of the 16-th order differential $(\,\mathbf{C}\,(\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{C}\,\mathrm{C})\,\mathbf{C}\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^2\,\mathrm{A}^3)\,)$ of the input property of (A16-i), which appear in the 2-nd round input, and we can get the following 6-round characteristic.

$$(\texttt{A32-i}) \quad (\,\mathbf{C}\,\mathbf{C}\,\mathbf{A}\,\mathbf{A}\,) \xrightarrow{6r} (\,\mathbf{U}\,\mathbf{U}\,\mathbf{U}\,\mathbf{a}\,)$$

Similarly, by extending the characteristic of (A16-ii), we can derive the characteristic of (A32-ii). The computer experiments also confirmed the same characteristics, verifying that the characteristics had been properly extended using the 32-nd order differential.

Next, we discuss the extension of the characteristic of (A32-i) by a similar approach. From (8) $\sim$ (13), if $\{x_{0,2}^{(1)}\} = \{x_{0,3}^{(1)}\} = \{x_{2,0}^{(1)}\} = \{x_{2,1}^{(1)}\} = \mathrm{C}$,

$$\begin{aligned}
x_{0,0}^{(2)} &= f_{\mathrm{L},0}^{(1)}(x_{0,0}^{(1)}, x_{0,1}^{(1)}, c_0, c_1) \oplus x_{1,0}^{(1)},\\
x_{0,1}^{(2)} &= f_{\mathrm{L},1}^{(1)}(x_{0,0}^{(1)}, x_{0,1}^{(1)}, c_0, c_1) \oplus x_{1,1}^{(1)},\\
x_{0,2}^{(2)} &= f_{\mathrm{R},2}^{(1)}(c_2, c_3, x_{0,2}^{(1)}, x_{0,3}^{(1)}) \oplus x_{3,2}^{(1)},\\
x_{0,3}^{(2)} &= f_{\mathrm{R},3}^{(1)}(c_2, c_3, x_{0,2}^{(1)}, x_{0,3}^{(1)}) \oplus x_{3,3}^{(1)},\\
X_1^{(2)} &= (c_0, c_1, c_2, c_3),\\
x_{2,0}^{(2)} &= f_{\mathrm{R},0}^{(1)}(c_2, c_3, x_{0,2}^{(1)}, x_{0,3}^{(1)}) \oplus x_{3,0}^{(1)},\\
x_{2,1}^{(2)} &= f_{\mathrm{R},1}^{(1)}(c_2, c_3, x_{0,2}^{(1)}, x_{0,3}^{(1)}) \oplus x_{3,1}^{(1)},\\
x_{2,2}^{(2)} &= f_{\mathrm{L},2}^{(1)}(x_{0,0}^{(1)}, x_{0,1}^{(1)}, c_0, c_1) \oplus x_{1,2}^{(1)},\\
x_{2,3}^{(2)} &= f_{\mathrm{L},3}^{(1)}(x_{0,0}^{(1)}, x_{0,1}^{(1)}, c_0, c_1) \oplus x_{1,3}^{(1)},\\
X_3^{(2)} &= (x_{0,0}^{(1)}, x_{0,1}^{(1)}, x_{2,2}^{(1)}, x_{2,3}^{(1)}),
\end{aligned}$$

where c_0, c_1, c_2, c_3 are constants. Since the F function is bijective, the 48-bit data $(x^{(1)}_{0,0}, x^{(1)}_{0,1}$ $, X^{(1)}_1, x^{(1)}_{2,2}, x^{(1)}_{2,3}, X^{(1)}_3)$ and $(X^{(2)}_0, X^{(2)}_2, X^{(2)}_3)$ are one-to-one correspondence. By inputting the following 48-th order differential;

$$\{\mathbf{X}^{(1)}\} = (\,(\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{C}\,\mathrm{C})\,\mathbf{A}\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^2\,\mathrm{A}^3)\,\mathbf{A}\,),$$

the below 48-th order differential appears in the 2-nd round input.

$$\{\mathbf{X}^{(2)}\} = (\,\mathbf{A}\,\mathbf{C}\,\mathbf{A}\,\mathbf{A}\,)$$

Therefore, the 48-th order differential $(\,(\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{C}\,\mathrm{C})\,\mathbf{A}\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^2\,\mathrm{A}^3)\,\mathbf{A}\,)$ in the 1-st round input will lead to 2^{16} sets of the 32-nd order differential $(\,\mathbf{C}\,\mathbf{C}\,\mathbf{A}\,\mathbf{A}\,)$ of the input property of (`A32`-i), which appear in the 2-nd round input. Accordingly, we can get the 7-round characteristic;

$$(\texttt{A48}\text{-i})\quad (\,(\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{C}\,\mathrm{C})\,\mathbf{A}\,(\mathrm{C}\,\mathrm{C}\,\mathrm{A}^2\,\mathrm{A}^3)\,\mathbf{A}\,) \xrightarrow{7r} (\,\mathbf{U}\,\mathbf{U}\,\mathbf{U}\,\mathbf{a}\,).$$

Similarly, by extending the characteristic of (`A32`-ii), we can derive the characteristic of (`A48`-ii). As a result, the 7-round characteristics using the 48-th order differential, equivalent to a theoretical 2-round extension of the 5-round integral characteristic using the 16-th order differential to the plaintext direction, have been reported in [10], as shown in Fig. 4.

5 Key Recovery Attack on Reduced-round Piccolo

This section shows that using the property 'all' in the attack equation can identify the key more efficiently than the conventional method.

5.1 Improved Attack Equation

From Definition 2, the property 'all' also satisfies the property Even. We describe the attack equation using these properties.

Using the ℓ-th order differential, the following attack equation holds if the property 'all' is observed in the $m\,(< \ell)$ bits intermediate variable $H(X)$.

$$f_i(\widetilde{E}(C(X); K_r)) = 2^{\ell-m}, \tag{14}$$

where $0 \leq i < 2^m$. (14) assumes that the number of occurrences of all possible m-bit values are equally $\frac{N}{2^m}$ for $N\,(= 2^\ell)$ outputs. In a random function, because the number of occurrences of a certain m-bit values is closely approximated by a normal distribution $\mathcal{N}(\frac{N}{2^m}, \frac{N}{2^m}(1 - \frac{1}{2^m}))$, the probability that the number of occurrences of a certain m-bit values becomes accurate $\frac{N}{2^m}$ is $(2^{-(m-1)}(1 - 2^{-m})\pi N)^{-\frac{1}{2}}$. Here, if the number of occurrences of the $2^m - 1$ m-bit values is determined, the number of occurrences of the remaining one can be uniquely determined by subtracting their sum from the total N. In other words, the degree of freedom of the frequency distribution of all possible m-bit values is $2^m - 1$. Therefore, the probability that the number of occurrences of all possible m-bit values becomes $\frac{N}{2^m}$, i.e., the probability that (14) holds for a false key, is $(2^{-(m-1)}(1 - 2^{-m})\pi N)^{-\frac{2^m-1}{2}}$. This probability is significantly smaller than the probability 2^{-m} that the conventional attack equation using the property Balance holds with a false key.

Next, we explain the attack equation using the property Even. If the property Even is observed in $H(X)$, the attack equation is given by

$$f_i^{(2)}(\widetilde{E}(C(X); K_r)) = 0. \tag{15}$$

The above equation implies that the modulo 2 frequency distribution for all possible m-bit values is 0, i.e., the number of occurrences of all possible m-bit values is even. In a random function, the probability that the number of occurrences of a certain m-bit values becomes even is $\frac{1}{2}$. Furthermore, since the degree of freedom of the modulo 2 frequency distribution for all possible m-bit values is $2^m - 1$, the probability that (15) holds with a false key is $2^{-(2^m-1)}$. If $m = 1$, the probability is the same as the conventional one since $2^{-(2^m-1)} = 2^{-m}$; otherwise, $2^{-(2^m-1)} < 2^{-m}$.

5.2 Attack Model

We demonstrate the key recovery attack against the 6-round Piccolo using the attack equation shown in 5.1. Here, we use the property 'all' appearing in the nibble data $c_{3,0}^{(5)}$ of the fifth round output of the characteristic of (A16-i).

Fig. 6 shows the equivalent circuit from the 6-th round output $(c_{1,0}^{(6)}, c_{1,1}^{(6)}, c_{3,2}^{(6)}, c_{3,3}^{(6)}, c_{2,0}^{(6)})$ to the 5-th round output $c_{3,0}^{(5)}$. In the figure, S^{-1} denotes the inverse function of the S-box, and the square box with a number (2 or 3) denotes the multiplication by the number. Also, as shown in the figure, the seventh round keys $rk_{12,0}, rk_{12,1}, rk_{13,2}, rk_{13,3}$, and the whitening key WK_2 can move before the S^{-1}, which is a nonlinear operation, where $RK_{11}^{'} = (rk_{11,0}^{'}, rk_{11,1}^{'}, rk_{11,2}^{'}, rk_{11,3}^{'}) = (rk_{12,0} \oplus wk_{2,0}, rk_{12,1} \oplus wk_{2,1}, rk_{13,2} \oplus wk_{2,2}, rk_{13,3} \oplus wk_{2,3})$. From $\{c_{3,0}^{(5)}\} = \mathrm{a}$ and (14), the $m\,(1 \le m \le 4)$-bit attack equation is given by

$$f_i(c_{3,0}^{(5)}[m]) = 2^{16-m}, \tag{16}$$

$$\begin{aligned} c_{3,0}^{(5)} &= \mathrm{S}^{-1}(2\mathrm{S}^{-1}(c_{1,0}^{(6)} \oplus rk_{11,0}^{'}) \oplus 3\mathrm{S}^{-1}(c_{1,1}^{(6)} \oplus rk_{11,1}^{'}) \\ &\quad \oplus \mathrm{S}^{-1}(c_{3,2}^{(6)} \oplus rk_{11,2}^{'}) \oplus \mathrm{S}^{-1}(c_{3,3}^{(6)} \oplus rk_{11,3}^{'})) \oplus c_{2,0}^{(6)}, \end{aligned}$$

where $0 \le i < 2^m$ and $x[m]$ denotes the lower m-bit of data x. Then, the keys to be identified are the four 4-bit keys $rk_{11,j}^{'}$ $(0 \le j \le 3)$. From 5.1 and $\ell = 16$, the probabilities that (14) holds for a false key are $2^{-8.33}$, $2^{-24.35}$, $2^{-54.11}$, and $2^{-109.19}$, in the case of $1 \le m \le 4$. Thus, to reduce the number of 2^{16} candidate keys to the true key, it is sufficient to have $2\,(> \frac{16}{8.33})$ sets of the 16-th order differential for $m = 1$ and 1 set for the rest of the case. On the other hand, the conventional attack equation requires $\lceil \frac{16}{m} \rceil$ sets of the 16-th order differential.

5.3 Experiments

First, using the property 'all,' the 16-bit key $RK_{11}^{'}$ is identified from (16) by computer experiment. Here, the average number of the remaining key candidates is calculated using the n-pair of m-bit attack equation with 2^{10} trials. Next, the same experiment is performed using the property Even. At this time, the attack equation is the replacement of $f_i(\cdot)$ by $f_i^{(2)}(\cdot)$ on the left side and 2^{16-m} by 0 on the right side in (16). Then, since the probability that this equation holds for a false key is $2^{-(2^m-1)}$, we use the $\lceil \frac{16}{2^m-1} \rceil$ sets of the 16-th order differential.

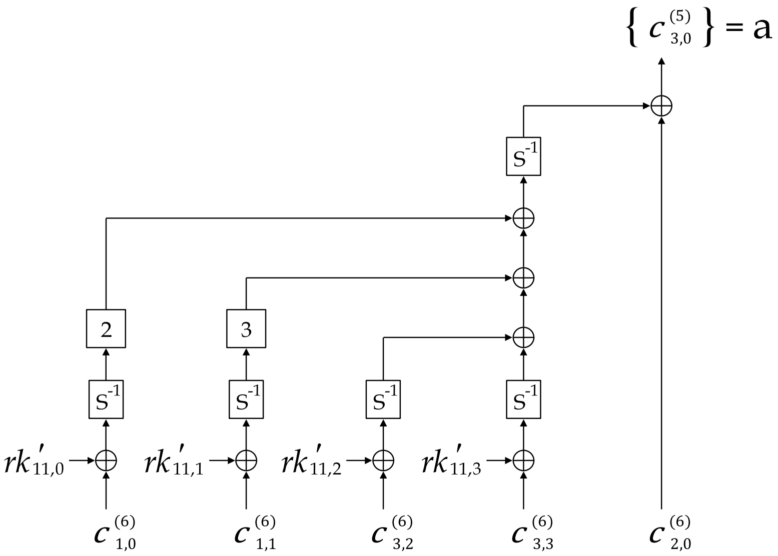

Figure 6: Equivalent circuit from the 6-round output $(c^{(6)}_{1,0}, c^{(6)}_{1,1}, c^{(6)}_{3,2}, c^{(6)}_{3,3}, c^{(6)}_{2,0})$ to the 5-th round output $c^{(5)}_{3,0}$.

Table 2: A number of remaining key candidates for n pairs of m-bit attack equation using the property 'all.'

n	m			
	1	2	3	4
1	205.45 (205.26)	1.00 (1.00)	1.00 (1.00)	1.00 (1.00)
2	1.63 (1.64)			

5.4 Results

Table 2 shows the results of the key recovery attack using the property 'all.' In the table, $(\cdot)$ represents the expected number of the remaining key candidates. From Table 2, the computer experiments' results were approximately consistent with the expectation. Then, Table 3 shows the results using the property Even, which are closely consistent with their expectations. Note that when $m = 1$, the probability that the attack equation using the property Even is the same as the conventional one using the property Balance. Thus, our computer experiments verify that the proposed attack equation using the properties 'all' and Even can identify the key with significantly less data than the conventional method.

Table 3: A number of remaining key candidate for n pairs of m-bit attack equation using the property Even.

n	m			
	1	2	3	4
1	32769.74 (32768.50)	8192.11 (8192.88)	512.35 (512.99)	3.07 (3.00)
2	16382.54 (16384.75)	1025.57 (1024.98)	5.03 (5.00)	1.00 (1.00)
3	8195.94 (8192.88)	127.99 (129.00)	1.04 (1.03)	
4	4100.84 (4096.94)	16.84 (17.00)		
5	2049.39 (2048.97)	2.98 (3.00)		
6	1024.91 (1024.98)	1.26 (1.25)		
7	513.02 (512.99)			
8	257.49 (257.00)			
9	129.46 (129.00)			
10	65.13 (65.00)			
11	32.67 (33.00)			
12	16.77 (17.00)			
13	8.98 (9.00)			
14	4.92 (5.00)			
15	2.96 (3.00)			
16	1.97 (2.00)			
17	1.50 (1.50)			

6 Conclusion

In this paper, we searched for integral characteristics on the block cipher Piccolo and found the 5-round integral characteristic using the 16-th order differential. We clarified the reason for this characteristic through a detailed analysis of the nibble values. We also showed the 6-round integral characteristic using the 32-nd order differential, equivalent to a theoretical 1-round extension of the 5-round one in the plaintext direction. This characteristic is consistent with the one verified by computer experiments. Then, we derived the 7-round integral characteristic using the 48-th order differential, a similar 1-round extension of the 6-round one that corresponded to the previous best higher order differential characteristic. As a result, the 7-round characteristic is equivalent to a 2-round extension of the 5-round one using the 16-th order differential. Furthermore, introducing the integral property based on the frequency distribution, we showed that if the property can be used in the attack equation, the key can be identified more efficiently than the conventional method. To verify this availability, we presented experimental results of the key recovery attack against the 6-round Piccolo.

Our future work will search for the integral characteristic by establishing a more accurate MILP model based on BDP.

References

[1] K. Shibutani, T. Isobe, H. Hiwatari, A. Mituda, T. Akishita, and T. Shirai, “Piccolo: An Ultra-Lightweight Blockcipher,” CHES2011, LNCS6917, pp. 342–357, 2011.

[2] X. Lai, “Higher Order Derivatives and Differential Cryptanalysis,” Communications and Cryptography, pp. 227–233, Kluwer Academic Publishers, 1994.

[3] L. R. Knudsen and D. Wagner, “Integral Cryptanalysis,” FSE2002, LNCS2365, pp. 112–127, Springer, Heidelberg, 2002.

[4] J. Daemen, L. Knudsen, and V. Rijmen, “The Block Cipher SQUARE,” FSE’97, LNCS1267, pp.149–165, 1997.

[5] K. Hwang, W. Lee, S. Lee, S. Lee, and J. Lim, “Saturation Attacks on Reduced Round Skipjack,” FSE2002, LNCS2365, pp. 100–111, Springer, Heidelberg, 2002.

[6] Y. Todo, “Structural Evaluation by Generalized Integral Property,” EUROCRYPT2015, Springer, LNCS9056, pp.287–314, 2015.

[7] Y. Todo, “Integral Cryptanalysis on Full MISTY1,” CRYPTO2015, LNCS9215, pp.413–432, Springer, Heidelberg, 2015.

[8] Y. Todo and M. Morii, “Bit-Based Division Property and Application to SIMON Family,” FSE2016, LNCS9783, pp.375–377, Springer, 2016.

[9] Z. Xiang, W. Zhang, Z. Bao, and D. Lin, “Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers,” ASIACRYPT2016, LNCS10031, pp.648–678, Springer, 2016.

[10] N. Shibayama and T. Kaneko, “New Higher Order Differential of Piccolo,” Technical Report of IEICE, Vol. 114, No. 115, ISEC2014-34, pp. 247–252, 2014 (in Japanese).

[11] H. Sato, M. Mimura, and H. Tanaka, “Analysis of Division Property using MILP method for Lightweight Blockcipher Piccolo,” AsiaJCIS2019, https://doi.org/10.1109/AsiaJCIS201948077.2019, pp. 48–55, 2019.

[12] S. Utsumi, K. Sakamoto, and T. Isobe, “Bit-level evaluation of Piccolo block cipher by satisfiability problem solver,” IET Information Security, https://doi.org/10.1049/ise2.12119, 2023.

[13] L. Sun, W. Wang, and M. Wang, “Automatic Search of Bit-Based Division Property for ARX Ciphers and Word-Based Division Property,” ASIACRYPT2017, LNCS10624, pp. 128–157, Springer, 2017.