Cryptanalysis of Full PRIDE Block Cipher

Yibin Dai and Shaozhen Chen

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
Zhengzhou Information Science and Technology Institute , Zhengzhou 450001, China
dybin321@163.com

Abstract. PRIDE is a lightweight block ciphers designed by Albrecht et al., appears in CRYPTO 2014. The designers claim that the construction of linear layers is nicely in line with a bit-sliced implementation of the Sbox layer and security. In this paper, we find 8 2-round iterative related-key differential characteristics, which can be used to construct 18-round related-key differentials. Then, by discussing the function $g_r^{(1)}$, we also find 4 2-round iterative related-key differential characteristics with $\Delta g_r^{(1)}(k_{1,2}) = 0x80$ and 4 2-round iterative characteristics with $\Delta g_r^{(1)}(k_{1,2}) = 0x20$ which cause three weak-key classes. Based on the related-key differentials, we launch related-key differential attack on full PRIDE. The data and time complexity are 2^{39} chosen plaintexts and 2^{60} encryptions, respectively. Moreover, by using multi related-key differentials, we improve the cryptanalysis, which requires $2^{41.4}$ chosen plaintexts and 2^{44} encryptions, respectively. Finally, by using 17-round related-key differentials, the cryptanalysis requires 2^{34} plaintexts and $2^{53.7}$ encryptions. These are the first results on full PRIDE.

Keywords: Cryptanalysis ; Block cipher; PRIDE; Iterative characteristics; Related-key differential

1 Introduction

Due to the rapidly growing impact of mobile phones, smart cards, RFID tags and sensor networks, lightweight cryptography which is suitable for such resource-constrained devices becomes more and more important. During the past few years, a number of lightweight block ciphers have been developed, including but not limited to PRESENT[7], PRINTcipher[12], LED[10], LBlcok[13], PRINCE[8], NSA standard SIMON and SPECK[2] etc.

PRIDE[1] is designed by Albrecht et al. in CRYPTO 2014, which significantly outperforms all existing block cipher of similar key sizes, with the exception of SIMON and SPECK. Both in the speed and memory, PRIDE is comparable to SIMON and SPECK. And so far, only Jingyuan Zhao , Xiaoyun Wang et al. give an analysis result with differential attack[14].

Based on related-key attack[3] and differential cryptanalysis[4], the related-key differential attack was introduced by Kelsey et al.[11] in 1996, in which it is assumed that the adversary has control over the key difference, along with the control over plaintext/ciphertext difference. Since its introduction, the related-key differential attack was used to break reduced-round variants of various block ciphers. Then, combined with other cryptanalysis such as boomerang attack, rectangle attack, impossible differential attack et al., there are many results, including AES[5,6], KASUMI[9] et al..

In this paper, we focus on the cryptanalysis of the new block cipher PRIDE against related-key attack. By investigating the key schedule algorithm, we can find 8 2-round iterative related-key differential characteristics. Then, we give a discussion of $g_r^{(1)}$. Based on the discussion, there exists 4 2-round iterative related-key differential characteristics with $\Delta g_r^{(1)}(k_{1,2}) = 0x80$, and 4 2-round iterative related-key differential characteristics with $\Delta g_r^{(1)}(k_{1,2}) = 0x20$ which cause 3 weak-key classes with $2^{126.4}$ or 2^{122} keys. All the 2-round iterative characteristics can extend to 18-round related-key differentials. Moreover, based on the 18-round related-key differentials and some observations of linear layer, we present an attack on full PRIDE with 2^{39} chosen plaintexts and 2^{60} encryptions. Furthermore, by using multiple related-key differentials, we improve the cryptanalysis which requires $2^{41.4}$ plaintexts and 2^{44} encryptions. Besides, by using 17-round related-key differentials, the cryptanalysis requires 2^{34} plaintexts and $2^{53.7}$ encryptions. These are the first results on full PRIDE. Our results are summarized and compared to the previous results in Table 1.

Table 1. Summary of Attacks on PRIDE

Cryptanalysis	Total Rounds	Attack Rounds	Data	Times	Reference
Differential	20	18	2^{60}CP	2^{64}	[14]
Related-key Differential	20	20	2^{39}CP	2^{60}	5.2
Related-key Differential	20	20	$2^{41.4}$CP	2^{44}	5.2
Related-key Differential	20	20	2^{34}CP	$2^{53.7}$	5.3

The rest of this paper is organized as follows. We introduce the notations in Section 2, and give a brief description of PRIDE in Section 3. Section 4 shows 4 2-round iterative related-key differential characteristics of PRIDE as well as others characteristics under 3 weak-key classes. We describe related-key differential attack on full PRIDE in Section 5. Finally, we concludes this paper.

2 Notations

The following notations are used in this paper:

I_r	the input of the r-th round
X_r	the state after $\oplus$ key of the r-th round
Y_r	the state after S-box of the r-th round
Z_r	the state after P-layer of the r-th round
W_r	the state after M-layer of the r-th round
O_r	the output of the r-th round
$X[n_1, \ldots, n_t]$	the $n_1, \ldots, n_t$-th nibbles of state

3 Description of PRIDE

PRIDE is a SPN structure block cipher with 64-bit block cipher and 128-bit key. The round function consists of three operations: The state is XORed with the round key, fed into 16 paralled 4-bit Sboxes and then permuted and processed by the linear layer, see Fig.1. The cipher has 20 rounds, of which the first 19 are identical, and linear layer of the last round is omitted, see Fig.2.

The PRIDE S-box is given in Table.2.

Table 2. S-box of block cipher PRIDE

x	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
S(x)	0x0	0x4	0x8	0xf	0x1	0x5	0xe	0x9	0x2	0x7	0xa	0xc	0xb	0xd	0x6	0x3

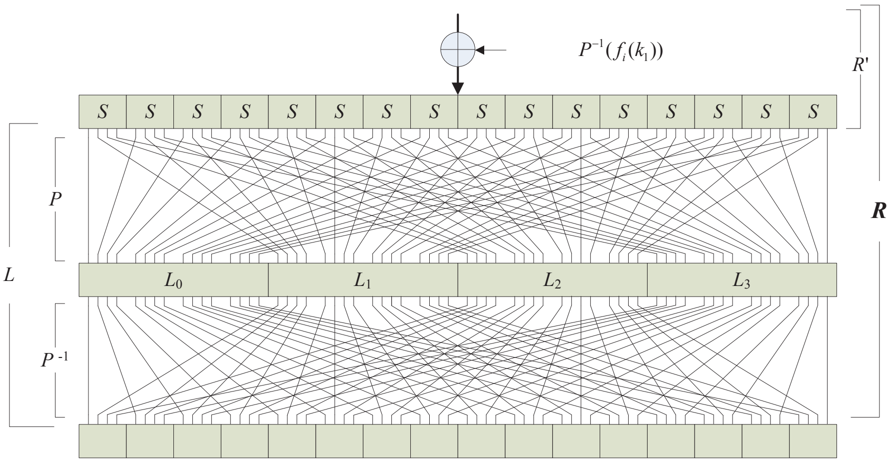

Fig. 1. The Round Function of PRIDE

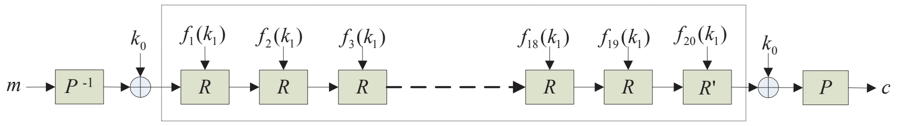

Fig. 2. Overall structure of PRIDE

The linear layer L of block cipher PRIDE is divided into 3 parts: a permutation layer P, a matrix layer M and another permutation P^{-1} which is the inverse of P. The matrix layer M shows $M = L_0 \times L_1 \times L_2 \times L_3$. The linear layer is defined as following :

$$L := P^{-1} \circ (M) \circ P$$

The detailed definitions of P, P^{-1}, L_i are in Appendix.

The 128-bit master key K of block cipher PRIDE is divided into two 64-bit parts $(k_0||k_1)$. k_0 is used for pre-whitening and post-whitening, while k_1 is divided into 8 8-bit words

$$k_1 = k_{1,1}||k_{1,2}||k_{1,3}||k_{1,4}||k_{1,5}||k_{1,6}||k_{1,7}||k_{1,8}$$

and used to generate the subkeys $f_r(k_1)$. $f_r(k_1)$ is defined as follows:

$$f_r(k_1) = k_{1,1}||g_r^{(1)}(k_{1,2})||k_{1,3}||g_r^{(2)}(k_{1,4})||k_{1,5}||g_r^{(3)}(k_{1,6})||k_{1,7}||g_r^{(4)}(k_{1,8})$$

as the subkey derivation function with four byte-local modifiers of the key as

$$g_r^{(1)}(x) = (x + 193r) \mod 256$$
$$g_r^{(2)}(x) = (x + 165r) \mod 256$$
$$g_r^{(3)}(x) = (x + 81r) \mod 256$$
$$g_r^{(4)}(x) = (x + 197r) \mod 256$$

which simply add one of four constants to every other byte of k_1.

4 Related-key differential attack on PRIDE

In this section, by investigating the key schedule of block cipher PRIDE, we present 2-round iterative related-key differential characteristics, which can be used to constructed 18-round related-key differential characteristics. And we can find 8 2-round iterative related-key differential characteristic. Then, we give a discussion of $g_r^{(1)}$, and find 4 2-round iterative related-key differentials with $\Delta g_r^{(1)}(k_{1,2}) = 0x80$ and 4 2-round characteristics under some weak-key classes.

4.1 Related-key Differential Characteristics of PRIDE

Because there are four non-linear function $g_r^{(i)}(i = 1, 2, 3, 4)$ in key schedule algorithm, we firstly consider related keys which has no difference occurred in the input of $g_r^{(i)}$. Assume that given a key $K = k_0||k_1$ and the related key $K' = k_0||k'_1$, where

$$k'_1 = k_1 \oplus 0x88||k_2||k_3||k_4||k_5||k_6||k_7||k_8$$

, that is, $\Delta k_1 = k_1 \oplus k'_1 = 0x88||0||0||0||0||0||0||0$ which lead to the following equation:

$$\Delta f_r(k_1) = 0x88||0||0||0||0||0||0||0,\ r = 1, \dots, 20$$

At the same time, we can get

$$\Delta P^{-1}(f_r(k_1)) = 0x80||0||0x80||0||0||0||0||0,\ r = 1, \dots, 20$$

,so that all the subkeys are identical.

Theorem 1. *Given the two keys (K, K') presented above, then there exists 2-round iterative related-key differential characteristics holding with probability 2^{-4}.*

Proof. According to the difference distribution of PRIDE S-box, that $S(0x8) = 0x8$ holds with probability 2^{-2}, which can be used to find 2-round iterative related-key differential characteristics with probability 2^{-4}, see Table.3.

Table 3. 2-round iterative related-key differential characteristics

ΔI_r	1000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔX_r	0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔY_r	0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔZ_r	0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔW_r	1000 1000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔI_{r+1}	1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000
ΔX_{r+1}	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000
ΔY_{r+1}	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000
ΔZ_{r+1}	0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔW_{r+1}	1000 1000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔI_{r+2}	1000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000

So there exists 2-round iterative related-key differential characteristics under ΔK:

$$8000800080000000 \xrightarrow{1r} 8000800000008000 \xrightarrow{1r} 8000800080000000,$$

where $\Delta k_0 = 0$ and $\Delta k_1 = 8800000000000000$. Then, according to Table.3, there are 2 active S-box in the 2-round path, so the probability of the 2-round iterative related-key differential characteristics is 2^{-4}.

The 2-round iterative related-key differential characteristics shows that there are 2 S-boxes in every two rounds. So that we also can consider the characteristics: one round has non active S-box, another has 2 S-boxes. In fact, there exists such 2-round iterative related-key differential characteristics with $\Delta k_1 = 8800000000000000$:

$$8000800000000000 \xrightarrow{1r} 0000000000000000 \xrightarrow{1r} 8000800000000000,$$

which can be used to construct 17-round or 18-round related-key differentials and then lead to an attack on full PRIDE.

There are totally 8 2-round iterative related-key differential characteristics listed in table.4.

Table 4. 8 2-round iterative characteristics

2-round characteristics	$\Delta P^{-1}(f_r(k_1))$	$\Delta f_r(k_1)$
8000 8000 8000 0000 $\xrightarrow{2r}$ 8000 8000 8000 0000	8000 8000 0000 0000	8800 0000 0000 0000
0800 0800 0800 0000 $\xrightarrow{2r}$ 0800 0800 0800 0000	0800 0800 0000 0000	4400 0000 0000 0000
0080 0080 0080 0000 $\xrightarrow{2r}$ 0080 0080 0080 0000	0080 0080 0000 0000	2200 0000 0000 0000
0008 0008 0008 0000 $\xrightarrow{2r}$ 0008 0008 0008 0000	0008 0008 0000 0000	1100 0000 0000 0000
8000 8000 0000 0000 $\xrightarrow{2r}$ 8000 8000 0000 0000	8000 8000 0000 0000	8800 0000 0000 0000
0800 0800 0000 0000 $\xrightarrow{2r}$ 0800 0800 0000 0000	0800 0800 0000 0000	4400 0000 0000 0000
0080 0080 0000 0000 $\xrightarrow{2r}$ 0080 0080 0000 0000	0080 0080 0000 0000	2200 0000 0000 0000
0008 0008 0000 0000 $\xrightarrow{2r}$ 0008 0008 0000 0000	0008 0008 0000 0000	1100 0000 0000 0000

Corollary 1 *Given the two keys (K, K') presented above, then there exists $2n$-round related-key differential characteristics holding with probability 2^{-4n}.*

It is obviously that if $2^{-4n} > 2^{-64}$, the related-key differential characteristics can be used to attack on block cipher PRIDE. Because of $2n = 20$ for PRIDE block cipher, the related-key differential characteristics can apply to cryptanalyze on full PRIDE.

4.2 Others iterative Characteristics

Based on the analysis in Section 4.1, by changing the position of the input difference and key difference, there also exists others 2-round iterative related-key differential characteristics with probability 2^{-4}. However, when it changes the position, we find that only first 16-bit of k_1 is nonzero, this means that the input difference of $g_r^{(1)}$ is nonzero. In order to keep iterative characteristics holding, it requires every round subkeys identical. Therefore, we firstly give a discussion of $g_r^{(1)}$.

Assume that key difference occurs in $k_{1,2}$ and $\Delta k_{1,2} = \delta$, the difference after the function $g_i^{(1)}$ is δ_i, $i = 1, \ldots, 20$. The 2-round iterative characteristics requires the round subkeys identical, that is $\delta_1 = \delta_2 = \cdots = \delta_{20}$. We have computationally generated all differences and values for $k_{1,2}$, see Table 5.

Table 5. Key difference and value for $g_r^{(1)}$

$\Delta k_{1,2}$	$\Delta g_r^{(1)}(k_{1,2})$	key values	number of key
0x20	0x20	0x0-0xb, 0x20-0x2b, 0x40-0x4b, 0x60-0x6b, 0x80-0x8b, 0xa0-0xab, 0xc0-cxb, 0xe0-0xeb, 0x80-0x8b, 0xa0-0xab, 0xc0-cxb, 0xe0-0xeb	$12 \times 8 = 96$
0x80	0x80	0x0-0xff	256
0xa0	0xa0	0x0-0xb, 0x20-0x2b, 0x40-0x4b, 0x60-0x6b, 0x80-0x8b, 0xa0-0xab, 0xc0-cxb, 0xe0-0xeb	$12 \times 8 = 96$
0x60	0x20	0x3f,0x5f,0xbf,0xdf	4
0xe0	0x20	0x1f,0x7f,0x9f,0xff	4

Table 5 shows that there are 5 cases meeting the condition that all round subkeys are identical. But the difference $0xa0$ can not be used to construct the 2-round iterative related-key differential characteristics with probability 2^{-4}. When the input difference of $g_r^{(1)}$ is nonzero, the 2-round iterative related-key differential characteristics are presented in Table 6.

Of course, according to Table 5 and Table 6, we say that there are 4 2-round iterative related-key differential characteristics with $\Delta k_{1,2} = 0x80$, and 4 2-round iterative characteristics

Table 6. Other 8 2-round iterative characteristics

2-round characteristics	$\Delta P^{-1}(f_r(k_1))$	$\Delta f_r(k_1)$
0000 8000 8000 8000 $\xrightarrow{2r}$ 0000 8000 8000 8000	0000 8000 8000 0000	0880 0000 0000 0000
0000 0080 0080 0080 $\xrightarrow{2r}$ 0000 0080 0080 0080	0000 0080 0080 0000	0220 0000 0000 0000
8000 8000 8000 0000 $\xrightarrow{2r}$ 8000 8000 8000 0000	8000 0000 8000 0000	8080 0000 0000 0000
0080 0080 0080 0000 $\xrightarrow{2r}$ 0080 0080 0080 0000	0080 0000 0080 0000	2020 0000 0000 0000
0000 8000 8000 0000 $\xrightarrow{2r}$ 0000 8000 8000 0000	0000 8000 8000 0000	0880 0000 0000 0000
0000 0080 0080 0000 $\xrightarrow{2r}$ 0000 0080 0080 0000	0000 0080 0080 0000	0220 0000 0000 0000
8000 0000 8000 0000 $\xrightarrow{2r}$ 8000 0000 8000 0000	8000 0000 8000 0000	8080 0000 0000 0000
0080 0000 0080 0000 $\xrightarrow{2r}$ 0080 0000 0080 0000	0080 0000 0080 0000	2020 0000 0000 0000

under the weak-key class with $\Delta k_{1,2} = 0x20$ which has $2^{126.4}(= 12 \times 8 \times 2^{120})$ keys, or with $\Delta k_{1,2} = 0x60, 0xe0$ which has $2^{122}(= 4 \times 2^{120})$ keys, See Table.5.

All the 2-round iterative related-key differential characteristics presented above can extend to 18-round related-key differentials which lead to the attack on full PRIDE.

5 Key Recovery of Block Cipher PRIDE

In this section, we firstly give some observations which can be used to filter the data. Then, we present an attack on full PRIDE using 2^{41} chosen plaintexts and 2^{60} encryptions. Besides, by using multiple related-key differentials, the cryptanalysis requires $2^{41.4}$ chosen plaintexts and 2^{44} encryptions. Finally, if use 17-round related-key differentials, the complexity of the cryptanalysis is 2^{34} chosen plaintexts and $2^{53.7}$ encryptions.

5.1 Some Observations

Observation 1 *If the input difference of L_0^{-1} is $\Delta W = (*000\ *000\ 0000\ *000)$, then its output difference is $\Delta Z = (0000\ 0000\ *000\ 0000)$ with probability 2^{-3}. If the input difference of L_3^{-1} is $\Delta W = (*000\ *000\ 0000\ *000)$, then its output difference is $\Delta Z = (0000\ 0000\ *000\ 0000)$ with probability 2^{-3}.*

Since $L_0^{-1}(*000\ *000\ 0000\ *000) = (*000\ *000\ *000\ *000)$, and (*000 *000 *000 *000)=(0000 0000 *000 0000) with probability 2^{-3}. L_3^{-1} situation is similar as L_0^{-1}.

Observation 2 *If the input difference of L_1^{-1} is $\Delta W = (0000\ 0{*}00\ 0000\ {*}{*}00)$, then its output difference is $\Delta Z = (0000\ 0000\ *000\ 0000)$ with probability 2^{-2}. If the input difference of L_2^{-1} is $\Delta W = (0{*}00\ 0000\ {*}{*}00\ 0000)$, then its output difference is $\Delta Z = (0000\ 0000\ *000\ 0000)$ with probability 2^{-2}.*

Since $\Delta Z^T = L_1^{-1}(\Delta W) = (0000\ 00{*}{*}\ {*}{*}{*}0\ 0000)$, where $\Delta W = (0000\ 0{*}00\ 0000\ {*}{*}00)$, it can construct a linear equation set as follows:

$$\begin{cases} \Delta W[6] \oplus \Delta W[13] = 0 \\ \Delta W[6] \oplus \Delta W[14] = 0 \end{cases} \quad (1)$$

If the 2 three equations are satisfied, $\Delta Z_r = (0000\ 0000\ *000\ 0000)$. And the probability is 2^{-2}. The proof of L_2^{-1} is similar as L_1^{-1}.

Observation 3 *If the input difference of L_0^{-1} is $\Delta W = (*000\ *000\ 0000\ *000)$, then its output difference is $\Delta Z = (*000\ *000\ 0000\ 0000)$ with probability 2^{-2}. If the input difference of L_3^{-1} is $\Delta W = (*000\ *000\ 0000\ *000)$, then its output difference is $\Delta Z = (*000\ *000\ 0000\ 0000)$ with probability 2^{-2}.*

Since $L_0^{-1}(*000\ *000\ 0000\ *000) = (*000\ *000\ *000\ *000)$, and (*000 *000 *000 *000)=(*000 *000 0000 0000) with probability 2^{-2}. L_3^{-1} situation is similar as L_0^{-1}.

Observation 4 *If the input difference of* L_1^{-1} *is* $\Delta W = (*00*\ *00*\ *000\ *000)$*, then its output difference is* $\Delta Z = (*000\ \ *000\ 0000\ 0000)$ *with probability* 2^{-4}*. If the input difference of* L_2^{-1} *is* $\Delta W = (*00*\ \ *00*\ \ *000\ \ *000)$*, then its output difference is* $\Delta Z = (*000\ \ *000\ 0000\ 0000)$ *with probability* 2^{-4}*.*

Since $\Delta Z^T = L_1^{-1}(\Delta W) = (***0\ \ ***0\ \ **00\ \ **00)$, where $\Delta W = (*00*\ \ *00*\ \ *000\ \ *000)$, it can construct a linear equation set which has simplified as follows:

$$\begin{cases} \Delta W[1] \oplus \Delta W[8] &= 0 \\ \Delta W[1] \oplus \Delta W[9] &= 0 \\ \Delta W[4] \oplus \Delta W[5] &= 0 \\ \Delta W[5] \oplus \Delta W[13] &= 0 \end{cases} \tag{2}$$

If the 4 three equations are satisfied, $\Delta Z_r = (*000\ \ *000\ 0000\ 0000)$. And the probability is 2^{-4}. The proof of L_2^{-1} is similar as L_1^{-1}.

5.2 Key-Recovery Attack By Using 18-Round Path

Key-Recovery with One characteristics Based on the 2-round iterative characteristics $8000800080000000 \xrightarrow{2r} 8000800080000000$, we can obtain 18-round related-key differential characteristics with probability 2^{-36} with $\Delta k_1 = 880000000000000$:

$$8880000000000000 \xrightarrow{P^{-1}, \oplus \Delta k_0} 8000800080000000 \xrightarrow{18r} 8000800080000000$$

We add 2-round after the characteristics (see Table.7), and analyze the full PRIDE.

Table 7. Cryptanalysis on Full PRIDE

ΔI_{19}	1000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔX_{19}	0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔY_{19}	0000 0000 0000 0000 0000 0000 0000 0000 **** 0000 0000 0000 0000 0000 0000 0000
ΔZ_{19}	0000 0000 *000 0000 0000 0000 *000 0000 0000 0000 *000 0000 0000 0000 *000 0000
ΔW_{19}	*000 *000 0000 *000 0000 0*00 0000 **00 0*00 0000 **00 0000 *000 *000 0000 *000
ΔI_{20}	*00* 00*0 0000 0000 *00* 0*00 0000 0000 00*0 00*0 0000 0000 **0* 0*00 0000 0000
ΔX_{20}	*00* 00*0 0000 0000 *00* 0*00 0000 0000 00*0 00*0 0000 0000 **0* 0*00 0000 0000
ΔY_{20}	**** **** 0000 0000 **** **** 0000 0000 **** **** 0000 0000 **** **** 0000 0000
$\oplus \Delta k_0$	**** **** 0000 0000 **** **** 0000 0000 **** **** 0000 0000 **** **** 0000 0000
ΔC	**00 **00 **00 **00 **00 **00 **00 **00 **00 **00 **00 **00 **00 **00 **00 **00

The attack procedure is as follows:

1. **Data Collection.** Encrypt 2^{38} pairs of plaintexts with a difference $0x8880000000000000$. For the 2^{38} pairs of ciphertexts, the adversary chooses the pairs that satisfy the output difference in table 6. There remains $2^6 (= 2^{38} \times 2^{-32})$ pairs.
2. **Key Recovery.**
   (a) Guess $k_0[1, 2, 5, 6, 9, 10, 13, 14]$ one by one, decrypt the corresponding nibbles of ciphertexts partially and verifies if the difference of the decrypted nibbles is $\Delta X_{20} = *00*, 00*0, *00*, 00*0, *00*, 00*0, **0*, 0*00$. The probability is 2^{-2}, 2^{-3}, 2^{-2}, 2^{-3}, 2^{-3}, 2^{-3}, 2^{-1}, and 2^{-3} respectively. There remains $2^6 \times 2^{-20} = 2^{-14}$ pairs.

(b) Decrypt the remaining pairs through $L-layer$. According to Observation 1 and 2, the probability satisfied the conditions ΔZ_{19} is $2^{-10}(=2^{-3}\times 2^{-3}\times 2^{-2}\times 2^{-2})$. Therefore, there remains $2^{-14}\times 2^{-10}=2^{-24}$ pairs.

(c) Guess 36-bit $k_0[3,4,7,8,11,12,15,16]$ and $(M\circ P)^{-1}(f_{20}(k_1))[9]$. Decrypt the remaining pairs, and check if the output difference of $\Delta X_{19}[9]$ is 0x8. On average $2^{-24}\times 2^{-4}=2^{-28}$ pair data remains. And if the remaining pairs is greater than 2, the corresponding key is right.

(d) Exhaustively search the rest 60-bit information of k_1 which are not guessed in the former steps.

Complexity analysis. For the data collection step, there requires 2^{39} chosen plaintexts, and 2^{39} encryptions. Step (a) requires $2\times 2^6\times 2^{32}\times 1/20=2^{35}$ encryptions. Step (b) only executes linear layers, we omit here. Step (c) requires $2\times 2^{32}\times 2^{-24}\times 2^{36}\times 1/20=2^{41}$ encryption. In step (d), there are 60-bit information of k_1 which are not guessed, so it requires 2^{60} encryptions.

Therefore, the attack requires 2^{39} chosen plaintexts and 2^{60} encryptions.

Key-Recovery with Multiple Characteristics Due to the iterative property of related-key differentials, there are two cases which can be used to cryptanalyze PRIDE for the same related keys. For example, with the related keys satisfied $\Delta k_1=880000000000000$, the two cases are as follows:

$$\textbf{Case 1.}\quad 8000800080000000 \xrightarrow{1r} 8000800000008000 \xrightarrow{1r} 8000800080000000$$

$$\textbf{Case 2.}\quad 8000800000008000 \xrightarrow{1r} 8000800080000000 \xrightarrow{1r} 8000800000008000,$$

which lead to two related-key differentials:

$$8880000000000000 \xrightarrow{P^{-1},\oplus\Delta k_0} 8000800080000000 \xrightarrow{18r} 8000800080000000$$

$$8808000000000000 \xrightarrow{P^{-1},\oplus\Delta k_0} 8000800000008000 \xrightarrow{18r} 8000800000008000$$

For each of the cases, apply the attack procedure presented in section 5.2. On one hand, for **Case.1**, it needs to guess k_0 and $(M\circ P)^{-1}(f_{20}(k_1))[9]$. On the other hand, for **Case.2**, it needs to guess k_0 and $(M\circ P)^{-1}(f_{20}(k_1))[13]$. Note that the 64-bit k_0 are common, so there are 56-bit k_1 which are not guessed. Therefore, by using the two cases, the attack requires 2×2^{39} chosen plaintexts and 2^{56} encryptions.

Furthermore, if we use more related keys, the time complexity of the attack can be reduced. For example, we chosen another related keys satisfied $\Delta k_1=440000000000000$, there are 2 more cases:

$$\textbf{Case 3.}\quad 0800080008000000 \xrightarrow{1r} 0800080000000800 \xrightarrow{1r} 0800080008000000$$

$$\textbf{Case 4.}\quad 0800080000000800 \xrightarrow{1r} 0800080008000000 \xrightarrow{1r} 0800080000000800$$

At the same times, two nibbles key $(M\circ P)^{-1}(f_{20}(k_1))[10,14]$ need to be guessed and then 48-bit k_1 which are not guessed. Therefore, by using the two more cases, the attack requires $4\times 2^{39}=2^{41}$ chosen plaintexts and 2^{48} encryptions.

The best time-data trade-off method requires 5 cases which lead to an attack on full PRIDE using $5\times 2^{39}=2^{41.4}$ chosen plaintexts and 2^{44} encryptions.

5.3 Key-Recovery Attack By Using 17-Round Path

In this section, we recover the key by using another 2-round iterative related-key differential characteristics$8000800000000000 \xrightarrow{2r} 8000800000000000$, which lead to a 17-round (round 2-18) related-key differential with probability 2^{-32} with $\Delta k_1=880000000000000$:

$$8000800000000000 \xrightarrow{16r} 8000800000000000 \xrightarrow{1r} 0000000000000000$$

We add 1-round before the characteristics and 2-round after the characteristics (see Table.8), and then analyze the full PRIDE. Here, we omit the initial permutation P^{-1}-layer.

Table 8. Cryptanalysis on Full PRIDE

ΔI_1	**** 0000 0000 0000 **** 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔX_1	**** 0000 0000 0000 **** 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔY_1	1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔZ_1	1000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔW_1	1000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔI_2	1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔI_{19}	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔX_{19}	1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔY_{19}	**** 0000 0000 0000 **** 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔZ_{19}	*000 *000 0000 0000 *000 *000 0000 0000 *000 *000 0000 0000 *000 *000 0000 0000
ΔW_{19}	*000 *000 *000 *000 *00* *00* *000 *000 *00* *00* *000 *000 *000 *000 *000 *000
ΔI_{20}	**** 0000 0000 0**0 **** 0000 0000 0**0 **** 0000 0000 0000 **** 0000 0000 0000
ΔX_{20}	**** 0000 0000 0**0 **** 0000 0000 0**0 **** 0000 0000 0000 **** 0000 0000 0000
ΔY_{20}	**** 0000 0000 **** **** 0000 0000 **** **** 0000 0000 0000 **** 0000 0000 0000
$\oplus\Delta k_0$	**** 0000 0000 **** **** 0000 0000 **** **** 0000 0000 0000 **** 0000 0000 0000
ΔC	*00* *00* *000 *000 *00* *00* *000 *000 *00* *00* *000 *000 *00* *00* *000 *000

The attack procedure is as follows:

1. **Data Collection.** Encrypt 2^n structures, in each of which, plaintexts traverse in nibbles 1, 5 and fix value in the rest nibbles. There are 2^8 plaintexts in a structure which causes to 2^{15} pairs. For the ciphertexts, the adversary chooses the pairs that satisfy the output difference in table 6. There remains $2^{-25}(= 2^{15} \times 2^{-40})$ pairs.
2. **Key Recovery.**
   (a) Guess 8-bit keys $k_0 \oplus P^{-1}(f_1(k_1))[1, 5]$, encrypt the 1-st and 5-th nibbles of plaintexts partially, and sieve 2^8 pairs whose S-box output difference $\Delta Y_1[1] = \Delta Y_1[5] = 0x8$, which makes 2^{-33} pairs remain.
   (b) Guess $k_0[1, 4, 5, 8, 9, 13]$ one by one(here, we can obtain $P^{-1}(f_1(k_1))[1, 5]$), decrypt the corresponding nibbles of ciphertexts partially and verifies if the difference of the decrypted nibbles is $\Delta X_{20}[1, 4, 5, 8, 9, 13]$=****, 0**0, ****, 0**0, ****, ****. The probability is 1, 2^{-2}, 1, 2^{-2}, 1, and 1 respectively. There remains $2^{-33} \times 2^{-4} = 2^{-37}$ pairs.
   (c) Decrypt the remaining pairs through $L - layer$. According to Observation 3 and 4, the probability satisfied the conditions ΔZ_{19} is $2^{-12}(= 2^{-2} \times 2^{-2} \times 2^{-4} \times 2^{-4})$. Therefore, there remains $2^{-37} \times 2^{-12} = 2^{-49}$ pairs.
   (d) Guess 40-bit $k_0[2, 3, 6, 7, 10, 11, 12, 14, 15, 16]$ and 8-bit $(M \circ P)^{-1}(f_{20}(k_1))[1, 5]$. Decrypt the remaining pairs, and check if the output difference of $\Delta X_{19}[1, 5]$ is 0x8, respectively. On average $2^{-49} \times 2^{-8} = 2^{-57}$ pairs data remains. Here, we guess 64-bit k_0 and 16-bit information of k_1 in all.
   (e) Exhaustively search the rest 48-bit information of k_1 which are not guessed in the former steps.

In order to distinguish the right key from the wrong ones, we expect two pairs satisfy our related-key differential path which require n to be 26 since the probability of our differential path is 2^{-32}. In this way, about 2^{-31} pairs expected to left for the wrong keys.

Complexity analysis. For the data collection step, there requires $2^{26} \times 2^8 = 2^{34}$ chosen plaintexts, and 2^{34} encryptions. Step (a) requires $2 \times 2 \times 2^8 \times 1/20 = 2^{5.7}$ encryptions. Step (b) requires $2^8 \times 2 \times 2^{-7} \times 2^{24} \times 1/20 = 2^{21.7}$ encryptions. Step (c) only executes linear layers, we omit here. Step (d) requires $2^{32} \times 2 \times 2^{-23} \times 2^{48} \times 1/20 = 2^{53.7}$ encryptions. In step (e), there are 48-bit k_1 which are not guessed, so it requires 2^{48} encryptions.

Therefore, the attack requires 2^{34} chosen plaintexts and $2^{53.7}$ encryptions.

6 Conclusion

According to observing the key schedule algorithm and linear layer of PRIDE, we find 8 2-round iterative related-key differential characteristics which can be used to construct 18-round related-key differentials for block cipher PRIDE. Then, we also give 4 2-round iterative related-key differential characteristics with $\Delta g_r^{(1)}(k_{1,2}) = 0x80$ and 4 2-round iterative related-key differential characteristics under 3 weak-key classeses with $2^{126.4}$ or 2^{122} keys. Based on one of the related-key differentials, we attack on full PRIDE using 2^{39} chosen plaintexts and 2^{60} encryptions. Moreover, by using multi related-key differentials, we can improve the cryptanalysis which requires $2^{41.4}$ plaintexts and 2^{44} encryptions. Besides, by using the 17-round related-key differentials, the complexity of the cryptanalysis is 2^{34} plaintexts and $2^{53.7}$ encryptions. These are the first results on full PRIDE.

References

1. M.R. Albrecht, B. Driessen, E.B. Kavun, G. Leander, C. Paar, and T. Yalcin. Block ciphers - focus on the linear layer(feat. PRIDE). In J.A. Garay and R. Gennaro, editors, *CRYPTO 2014*, volume 8616 of *Lecture Notes in Computer Science*, pages 57–76. Springer, Berlin, 2014.
2. R. Beaulieuand, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers. Performance of the SIMON and SPECK family of lightweight block ciphers. Technical report, National Security Agency, 2014.
3. E. Biham. New types of cryptanalytic attacks using related keys. *J. Cryptology*, 7(4):229–246, 1994.
4. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.
5. A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 299–319. Springer, Berlin, 2010.
6. A. Biryukov and D. Khovratovich. Related-key cryptanalysis of the full AES-192 and AES-256. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 1–18. Springer, Berlin, 2009.
7. A. Bogdanov, L.R. Knudsen, G. Leader, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkielsoe. PRESENT: An ultra-lightweight block cipher. In P. Pailier and I. Verbauwhede, editors, *CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, Berlin, 2007.
8. J. Borghoff, A. Canteaut, T. Güneysu, E.B. Kavun, M. Knezevic, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S.S. Thomsen, and T. Yalcin. PRINCE- A low-latency block cihper for pervasive computing applications-extended abstract. In X. Wang and K. Sako, editors, *ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225. Springer, Berlin, 2012.
9. O. Dunkelman, N. Keller, and A. Shamir. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 393–410. Springer, Berlin, 2010.
10. J. Guo, T. Peyrin, A. Poschmann, and M.J.B. Robshaw. The LED block cipher. In B. Preneel and T. Takagi, editors, *CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer, Berlin, 2011.

11. J. Kelsey, B. Schneier, and D. Wagner. Key schedule crypt-analysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In N. Koblitz, editor, *CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*, pages 237–251. Springer, Berlin, 1996.

12. L. Knudsen, G. Leander, A. Poschmann, and M. Robshaw. PRINTcipher: A block cipher for ic printing. In S. Mangard and F.-X Standaert, editors, *CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 16–32. Springer, Berlin, 2010.

13. W. Wu and L. Zhang. LBlock: A lightweight block cipher. In J. Lopez and G. Tsudik, editors, *ACNS 2011*, volume 6715 of *Lecture Notes in Computer Science*, pages 327–344. Springer, Berlin, 2011.

14. J. Zhao, X. Wang, M. Wang, and X. Dong. Differential analysis on block cipher PRIDE. Cryptology ePrint Archive, Report 2014/525. `http://eprint.iacr.org/2014/525.pdf/`.

$$L_0 = (L_0)^{-1} = \begin{pmatrix} 0000100010001000 \\ 0000010001000100 \\ 0000001000100010 \\ 0000000100010001 \\ 1000000010001000 \\ 0100000001000100 \\ 0010000000100010 \\ 0001000000010001 \\ 1000100010000000 \\ 0100010001000000 \\ 0010001000100000 \\ 0001000100010000 \\ 0000100010001000 \\ 0000010001000100 \\ 0000001000100010 \\ 0000000100010001 \end{pmatrix}, L_1 = \begin{pmatrix} 1100000000010000 \\ 0110000000001000 \\ 0011000000000100 \\ 0001100000000010 \\ 0000110000000001 \\ 0000011010000000 \\ 0000001101000000 \\ 1000000100100000 \\ 1000000000011000 \\ 0100000000001100 \\ 0010000000000110 \\ 0001000000000011 \\ 0000100010000001 \\ 0000010011000000 \\ 0000001001100000 \\ 0000000100110000 \end{pmatrix}$$

$$L_2 = \begin{pmatrix} 0000110000000001 \\ 0000011010000000 \\ 0000001101000000 \\ 1000000100100000 \\ 1100000000010000 \\ 0110000000001000 \\ 0011000000000100 \\ 0001100000000010 \\ 0000100010000001 \\ 0000010011000000 \\ 0000001001100000 \\ 0000000100110000 \\ 1000000000011000 \\ 0100000000001100 \\ 0010000000000110 \\ 0001000000000011 \end{pmatrix}, L_3 = (L_3)^{-1} = \begin{pmatrix} 1000100000001000 \\ 0100010000000100 \\ 0010001000000010 \\ 0001000100000001 \\ 1000100010000000 \\ 0100010001000000 \\ 0010001000100000 \\ 0001000100010000 \\ 0000100010001000 \\ 0000010001000100 \\ 0000001000100010 \\ 0000000100010001 \\ 1000000010001000 \\ 0100000001000100 \\ 0010000000100010 \\ 0001000000010001 \end{pmatrix}$$

$$(L_1)^{-1} = \begin{pmatrix} 0000001100000010 \\ 1000000100000001 \\ 1100000010000000 \\ 0110000001000000 \\ 0011000000100000 \\ 0001100000010000 \\ 0000110000001000 \\ 0000011000000100 \\ 1000000100000001 \\ 0001000000011000 \\ 0000100000001100 \\ 0000010000000110 \\ 0000001000000011 \\ 0000000110000001 \\ 1000000011000000 \\ 0100000001100000 \\ 0010000000110000 \end{pmatrix}, (L_2)^{-1} = \begin{pmatrix} 0011000000100000 \\ 0001100000010000 \\ 0000110000001000 \\ 0000011000000100 \\ 0000001100000010 \\ 1000000100000001 \\ 1100000010000000 \\ 0110000001000000 \\ 0000000110000001 \\ 1000000011000000 \\ 0100000001100000 \\ 0010000000110000 \\ 0001000000011000 \\ 0000100000001100 \\ 0000010000000110 \\ 0000001000000011 \\ 0000000110000001 \end{pmatrix}$$

Table 9. Permutation $P(x)$ of Block Cipher PRIDE

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$P(x)$	1	17	33	49	2	18	34	50	3	19	35	51	4	20	36	52
x	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$P(x)$	5	21	37	53	6	22	38	54	7	23	39	55	8	24	40	56
x	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$P(x)$	9	25	41	57	10	26	41	58	11	27	43	59	12	28	44	60
x	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
$P(x)$	13	29	45	61	14	30	46	62	15	31	47	63	16	32	38	64

Table 10. Permutation $P^{-1}(x)$ of Block Cipher PRIDE

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$P(x)$	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
x	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
$P(x)$	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62
x	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$P(x)$	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59	63
x	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
$P(x)$	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64