SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

May 2017, Vol. 60 052108:1–052108:12
doi: 10.1007/s11432-015-5487-3

Cryptanalysis of full PRIDE block cipher

Yibin DAI[1,2*] & Shaozhen CHEN[1,2]

[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou* 450001, *China;*
[2]*Zhengzhou Information Science and Technology Institute, Zhengzhou* 450001, *China*

Received October 6, 2015; accepted December 18, 2015; published online September 13, 2016

Abstract PRIDE is a lightweight block cipher proposed at CRYPTO 2014 by Albrecht et al., who claimed that the construction of linear layers is efficient and secure. In this paper, we investigate the key schedule and find eight 2-round iterative related-key differential characteristics, which can be used to construct 18-round related-key differentials. A study of the first subkey derivation function reveals that there exist three weak-key classes, as a result of which all the differences of subkeys for each round are identical. For the weak-key classes, we also find eight 2-round iterative related-key differential characteristics. Based on one of the related-key differentials, we launch an attack on the full PRIDE block cipher. The data and time complexity are 2^{39} chosen plaintexts and 2^{92} encryptions, respectively. Moreover, by using multiple related-key differentials, we improve the cryptanalysis, which then requires $2^{41.6}$ chosen plaintexts and $2^{42.7}$ encryptions, respectively. Finally, we use two 17-round related-key differentials to analyze full PRIDE, which requires 2^{35} plaintexts and $2^{54.7}$ encryptions. These are the first results on full PRIDE, and show that the PRIDE block cipher is not secure against related-key differential attack.

Keywords cryptanalysis, block cipher, PRIDE, iterative characteristics, related-key differential

Citation Dai Y B, Chen S Z. Cryptanalysis of full PRIDE block cipher. Sci China Inf Sci, 2017, 60(5): 052108, doi: 10.1007/s11432-015-5487-3

1 Introduction

Recently, lightweight block ciphers have become more and more important owing to the emergence of low-resource devices such as sensor networks, RFID tags, mobile phones, and smart cards. During the last decade, a large number of lightweight block ciphers have been published for such resource-constrained environments, including PRESENT [1], PRINTcipher [2], LED [3], LBlcok [4], PRINCE [5], NSA standard SIMON, and SPECK [6].

PRIDE [7], proposed at CRYPTO 2014, is a software-optimized lightweight block cipher with a good linear layer. The design goals of PRIDE place no specific restrictions on its key schedule. In terms of both speed and memory, PRIDE is comparable to SIMON and SPECK for the same platform. Some cryptanalytic results have been obtained on PRIDE. Zhao et al. [8] analyzed the results of a differential attack. Yang et al. [9] then presented an improved differential analysis of 19-round PRIDE. Dinur [10] devised new cryptanalytic time–memory–data tradeoff attacks on FX-constructions and applied these to PRIDE.

* Corresponding author (email: dybin321@163.com)

Table 1 Summary of attacks on PRIDE

Cryptanalysis	Total rounds	Attack rounds	Data	Times	Reference
Differential	20	18	2^{60}CP	2^{64}	[8]
Differential	20	19	2^{62}CP	2^{63}	[9]
Related-key differential	20	20	2^{39}CP	2^{92}	Subsection 5.2
Multiple related-key differential	20	20	$2^{41.6}$CP	$2^{42.7}$	Subsection 5.2
Related-key differential	20	20	2^{34}CP	2^{88}	Subsection 5.3
Multiple related-key differential	20	20	2^{35}CP	$2^{54.7}$	Subsection 5.3

Based on related-key attack [11] and differential cryptanalysis [12], related-key differential attack was introduced by Kelsey et al. [13]. In this approach, the attacker can take control of the key difference and observe the operation of a cipher under several different keys. The utilization of the key difference to kill the state difference leads to more efficient characteristics and great improvements in some results. Combining related-key attack with other cryptanalysis approaches such as boomerang attack, rectangle attack, and impossible differential attack has led to a number of results on various block ciphers, including AES [14, 15] and KASUMI [16], among others.

In this paper, we focus on cryptanalysis of the new block cipher PRIDE under related-key attack. By observing the key schedule and linear layer, we find eight 2-round iterative related-key differential characteristics. We then discuss the first subkey derivation function $g_r^{(1)}$ and find that there exist two differences $\Delta g_r^{(1)}(k_{1,2}) = 0\text{x}80$ and $\Delta g_r^{(1)}(k_{1,2}) = 0\text{x}20$ for which all the differences of subkeys for each round are identical. Also, the difference $\Delta g_r^{(1)}(k_{1,2}) = 0\text{x}20$ leads to three weak-key classes with $2^{126.4}$ or 2^{122} keys. Based on this discovery, we find that there are another eight 2-round iterative related-key differential characteristics. All the 2-round iterative characteristics can extend to 17- or 18-round related-key differentials. Moreover, based on one of the 18-round related-key differentials and some observations on the linear layer, we present an attack on full PRIDE with 2^{39} chosen plaintexts and 2^{92} encryptions. By using multiple related-key differentials, we improve the cryptanalysis, which then requires $2^{41.6}$ plaintexts and $2^{42.7}$ encryptions. Finally, we utilize two 17-round related-key differentials to analyze full PRIDE, which requires 2^{35} plaintexts and $2^{54.7}$ encryptions. These are the first results on full PRIDE, and they show that the PRIDE block cipher is not secure against related-key differential attack. These results also suggest that designers should take the key schedule into consideration, as has been done by Huang and Lai [17] in their investigation of the effective key length for a block cipher against a meet-in-the-middle attack. Our results, given in Subsections 5.2 and 5.3, are summarized and compared with previous results in Table 1.

The rest of this paper is organized as follows. Section 2 introduces our notation and Section 3 gives a brief description of the lightweight block cipher PRIDE. Section 4 describes some 2-round iterative related-key differential characteristics of PRIDE as well as other characteristics under three weak-key classes. Section 5 describes related-key differential attack on full PRIDE. Finally, Section 6 gives our conclusion.

2 Notation

The following notation is used in this paper:

I_r: the input value of the rth round;

X_r: the state after the $\oplus$ key of the rth round;

Y_r: the state after the S-box of the rth round;

Z_r: the state after the P-layer of the rth round;

W_r: the state after the M-layer of the rth round;

O_r: the output of the rth round;

$X[n_1, \ldots, n_t]$: the $n_1, \ldots, n_t$th nibbles of the state;

ΔM: the difference between M and M'.

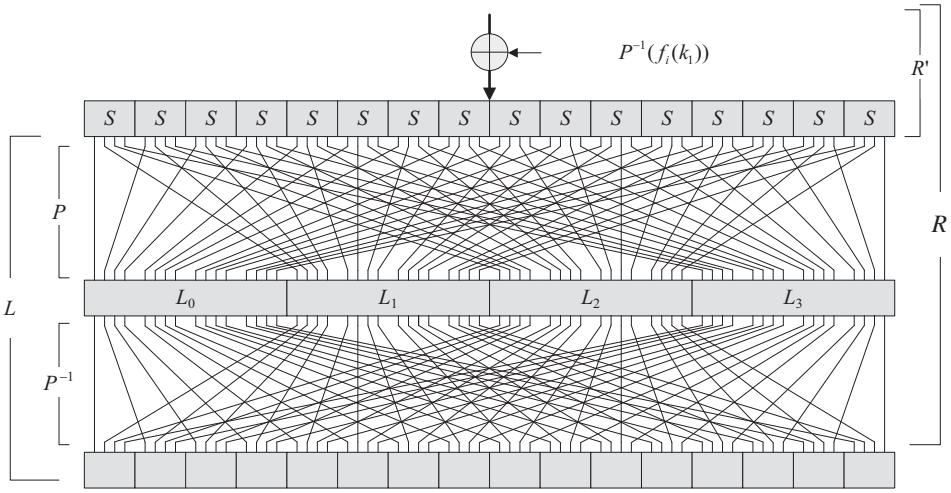

Figure 1 The round function of PRIDE.

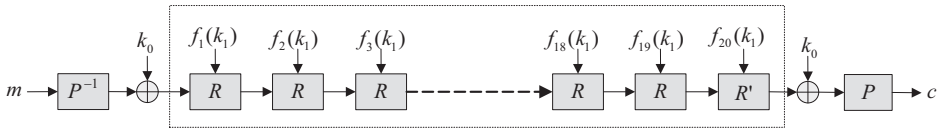

Figure 2 Overall structure of PRIDE.

Table 2 The S-box of PRIDE

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S(x)	0	4	8	f	1	5	e	9	2	7	a	c	b	d	6	3

3 Description of PRIDE

PRIDE is an SPN-type lightweight block cipher with a block size of 64 bits and a 128-bit key. The round function consists of three operations: the state is XORed with the subkey, fed into 16 identical 4-bit S-boxes in parallel, and then permuted and processed by the linear layer (see Figure 1). The cipher has 20 rounds, the first 19 of which are identical, and the linear layer of the last round is not necessary (see Figure 2).

The PRIDE S-box is given in Table 2.

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

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

The definitions of P (Table A1), P^{-1} (Table A2), and L_i are given in detail in the Appendix A.

The 128-bit master key K of the block cipher PRIDE is divided into two 64-bit parts $(k_0||k_1)$. k_0 is used for pre- and post-whitening. k_1 is divided into eight 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 $f_r(k_1)$, defined by

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

Table 3 2-round iterative related-key differential characteristics

Notation	The difference of the intermediate state
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

where the subkey derivation functions are

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

which are simply modulo-256 additions with one of four constants.

4 Related-key differential attack on PRIDE

In this section, after investigating the key schedule of the block cipher PRIDE, we present eight 2-round iterative related-key differential characteristics. We then discuss $g_r^{(1)}$ and find four 2-round iterative related-key differentials with $\Delta g_r^{(1)}(k_{1,2}) = 0\text{x}80$ and four 2-round characteristics under some weak-key classes.

4.1 Related-key differential characteristics of PRIDE

Because there are four nonlinear functions $g_r^{(i)}$ $(i = 1, 2, 3, 4)$ in the key schedule, we first consider related keys for which the input difference of $g_r^{(i)}$ is the same. Assume that we are given a key $K = k_0||k_1$ and a related key $K' = k_0||k_1'$, where

$$k_1' = k_{1,1} \oplus 0\text{x}88||k_{1,2}||k_{1,3}||k_{1,4}||k_{1,5}||k_{1,6}||k_{1,7}||k_{1,8},$$

that is, $\Delta k_1 = k_1 \oplus k_1' = 0\text{x}88||0||0||0||0||0||0||0$, which leads to the following equation:

$$\Delta f_r(k_1) = 0\text{x}88||0||0||0||0||0||0||0,\ r = 1, \ldots, 20.$$

At the same time, we have

$$\Delta P^{-1}(f_r(k_1)) = 0\text{x}80||0||0\text{x}80||0||0||0||0||0,\ r = 1, \ldots, 20,$$

so that all the differences of subkeys for each round are identical.

Theorem 1. Assume that there are two related keys (K, K') as presented above. Then there exist 2-round iterative related-key differential characteristics with probability 2^{-4}.

Proof. According to the difference distribution of the PRIDE S-box, $S(0\text{x}8) = 0\text{x}8$ 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 4 Eight 2-round iterative characteristics

2-round characteristic	$\Delta P^{-1}(f_r(k_1))$	$\Delta f_r(k_1)$
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

Therefore, there exist 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 two active S-boxes 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 show that there are two S-boxes in every two rounds. Thus, we can also consider characteristics on which one round has a nonactive S-box while the other has two S-boxes. In fact, such 2-round iterative related-key differential characteristics do exist. For example, a 2-round iterative related-key differential characteristic with $\Delta k_1 = 8800000000000000$ can be represented as follows:

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

which can be used to construct 17- and 18-round related-key differentials with probabilities 2^{-32} and 2^{-36}, respectively. All the related-key differentials can be used in an attack on full PRIDE.

There are a total of eight 2-round iterative related-key differential characteristics, as listed in Table 4.

Corollary 1. Assume that there are two related keys (K, K') as presented above. Then there exist $2n$-round related-key differential characteristics with probability 2^{-4n}.

It is obvious that if $2^{-4n} > 2^{-64}$, then the related-key differentials can be used to attack the block cipher PRIDE. Because $2n = 20$ for the PRIDE block cipher, the related-key differentials can be applied to analyze full PRIDE.

4.2 Other iterative characteristics

Based on the analysis in Subsection 4.1, if we change the positions of the input difference and the key difference, then there also exist other 2-round iterative related-key differential characteristics with probability 2^{-4}. However, when the positions are changed, it is obvious that only the first 16 bits of k_1 are nonzero, which means that the input difference of $g_r^{(1)}$ is nonzero. In order to retain the iterative characteristics, it is necessary that all the differences of subkeys for each round are identical. Therefore, we first discuss $g_r^{(1)}$.

Assume that the key difference occurs in $k_{1,2}$ and that $\Delta k_{1,2} = \delta$; the differences after the function $g_i^{(1)}$ are δ_i, $i = 1, \ldots, 20$. The 2-round iterative characteristics require that all the differences of subkeys for each round be 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 shows that there are five cases meeting the condition that all the differences of subkeys for each round are identical. However, the difference 0xa0 cannot 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 as presented in Table 6.

Of course, according to Tables 5 and 6, we see that there are four 2-round iterative related-key differential characteristics with $\Delta k_{1,2} = 0$x80 and four 2-round iterative characteristics in the weak-key

Table 5 Key differences and values for $g_r^{(1)}$

$\Delta k_{1,2}$	$\Delta g_r^{(1)}(k_{1,2})$	Key values	Number of keys
0x20	0x20	0x0-0xb, 0x20-0x2b, 0x40-0x4b, 0x60-0x6b, 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 6 Other eight 2-round iterative characteristics

2-round characteristic	$\Delta P^{-1}(f_r(k_1))$	$\Delta f_r(k_1)$
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

class with $\Delta k_{1,2} = 0\text{x}20$, which has $2^{126.4}(= 12 \times 8 \times 2^{120})$ keys, or with $\Delta k_{1,2} = 0\text{x}60, 0\text{xe}0$, which has $2^{122}(= 4 \times 2^{120})$ keys.

5 Key recovery of the block cipher PRIDE

In this section, we first give some observations that can be used to filter the data. We then present an attack on full PRIDE using 2^{41} chosen plaintexts and 2^{92} encryptions. By using multiple related-key differentials, the cryptanalysis requires $2^{41.6}$ chosen plaintexts and $2^{42.7}$ encryptions. Finally, if we use 17-round related-key differentials with probability 2^{-32} to analyze full PRIDE, the complexity of the cryptanalysis is 2^{35} chosen plaintexts and $2^{54.7}$ 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^{-2}. 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^{-2}.

Since $L_0^{-1}(*000\ *000\ 0000\ *000) = (*000\ *000\ *000\ *000)$, $(*000\ *000\ *000\ *000) = (0000\ 0000\ *000\ 0000)$ holds with probability 2^{-2}. The situation for L_3^{-1} is similar to that for 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 $\Delta Z = L_1^{-1}(\Delta W) = (0000\ 00**\ ***0\ 0000)$, where $\Delta W = (0000\ 0*00\ 0000\ **00)$, it is possible to construct a linear equation set as follows:

$$\begin{cases} \Delta W[6] \oplus \Delta W[13] = 0, \\ \Delta W[6] \oplus \Delta W[14] = 0. \end{cases} \tag{1}$$

If these two equations are satisfied, then $\Delta Z_r = (0000\ 0000\ *000\ 0000)$ holds with probability 2^{-2}. The proof for L_2^{-1} is similar to that for L_1^{-1}.

Table 7 Cryptanalysis on full PRIDE

Notation	The difference of the intermediate state
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

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

Since $L_0^{-1}(*000\ *000\ *000\ *000) = (*000\ *000\ *000\ *000)$, $(*000\ *000\ *000\ *000) = (*000\ *000\ 0000\ 0000)$ holds with probability 2^{-2}. This is because there are two equations: $\Delta W[1] \oplus \Delta W[5] \oplus \Delta W[13] = 0$ and $\Delta W[1] \oplus \Delta W[5] \oplus \Delta W[9] = 0$, holding with probability 2^{-2}. The situation for L_3^{-1} is similar to that for 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 $\Delta Z = L_1^{-1}(\Delta W) = (***0\ ***0\ **00\ **00)$, where $\Delta W = (*00*\ *00*\ *000\ *000)$, it is possible to construct a linear equation set that has the following simple form:

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

If these four equations are satisfied, then $\Delta Z_r = (*000\ *000\ 0000\ 0000)$ holds with probability 2^{-4}. The proof for L_2^{-1} is similar to that for L_1^{-1}.

5.2 Key-recovery attack using an 18-round path

5.2.1 *Key recovery with one characteristic*

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

$$8880000000000000 \xrightarrow{P^{-1},\oplus\Delta k_1} 8000800080000000 \xrightarrow{18r} 8000800080000000.$$

We add two rounds after the characteristic (see Table 7) and analyze the full PRIDE.

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 remain $2^6 (= 2^{38} \times 2^{-32})$ 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 check whether the difference of the decrypted nibbles is $\Delta X_{20} = *00*, 00*0, *00*, 0*00, *00*, 00*$

$0, **0*$, or $0*00$. The probabilities are 2^{-2}, 2^{-3}, 2^{-2}, 2^{-3}, 2^{-3}, 2^{-3}, 2^{-1}, and 2^{-3}, respectively. There remain $2^6 \times 2^{-20} = 2^{-14}$ pairs.

(b) Decrypt the remaining pairs through the L-layer. According to Observations 1 and 2, the probability of satisfying the conditions ΔZ_{19} is $2^{-8}(= 2^{-2} \times 2^{-2} \times 2^{-2} \times 2^{-2})$. Therefore, there remain $2^{-14} \times 2^{-8} = 2^{-22}$ pairs.

(c) Guessing 32-bit $k_0[3, 4, 7, 8, 11, 12, 15, 16]$, one can obtain the output value of round 19. Then guessing $(M \circ P)^{-1}(f_{20}(k_1))[9]$, one can compute the input difference of the 9th S-box. Check if the output difference of $\Delta X_{19}[9]$ is 0x8. On average, $2^{-22} \times 2^{-4} = 2^{-26}$ pairs of data remain. If the number of remaining pairs is greater than 2, the corresponding key is correct.

(d) Exhaustively search the remaining information of k_1 that has not been guessed or distinguished in the earlier steps.

Complexity analysis. The data collection step requires 2^{39} chosen plaintexts and 2^{39} encryptions. In the key-guessing procedure, Step (a) requires $2 \times 2^6 \times 2^{32} \times 1/20 = 2^{35}$ encryptions. Step (b) only executes linear layers, and we omit it here. Step (c) requires $2 \times 2^{32} \times 2^{-22} \times 2^{36} \times 1/20 = 2^{39}$ encryptions. After Step (c), there are about 2^{32} 68-bit keys (64-bit k_0 and 4-bit k_1) for a pair, so Step (d) requires $2^{60} \times 2^{32} = 2^{92}$ encryptions.

Therefore, the attack requires 2^{39} chosen plaintexts and 2^{92} encryptions.

5.2.2 *Key recovery with multiple characteristics*

In this subsection, we obtain a cryptanalytic result on full PRIDE with multiple related-key differentials. According to Table 4, there exist eight iterative related-key differential characteristics. First, we examine the following two cases to analyze full PRIDE:

$$\textbf{Case 1.}\quad 8000800080000000 \xrightarrow{2r,\Delta k_1=8800000000000000} 8000800080000000,$$
$$\textbf{Case 2.}\quad 0080008000800000 \xrightarrow{2r,\Delta k_1=2200000000000000} 0080008000800000.$$

These lead to two related-key differentials:

$$8880000000000000 \xrightarrow{P^{-1},\oplus\Delta k_1} 8000800080000000 \xrightarrow{18r} 8000800080000000,$$
$$2220000000000000 \xrightarrow{P^{-1},\oplus\Delta k_1} 0080008000800000 \xrightarrow{18r} 0080008000800000.$$

For each case, we apply the attack procedure presented in Subsection 5.2.1. Before Step (d), for Case 1, the procedure has guessed $k_0[1, 2, 5, 6, 9, 10, 13, 14]$ and $(M \circ P)^{-1}(f_{20}(k_1))[9]$, and for Case 2, it has guessed $k_0[3, 4, 7, 8, 11, 12, 15, 16]$ and $(M \circ P)^{-1}(f_{20}(k_1))[11]$. Therefore, if we use the two cases, the 64-bit key k_0 and the 8-bit key $(M \circ P)^{-1}(f_{20}(k_1))[9, 11]$ have been guessed before Step (d), and then there is the 56-bit key information of k_1 that has not been 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 and related-key differentials, the time complexity of the attack can be reduced. For a time–data tradeoff, six cases are required. For example, we could add four more cases as follows:

$$\textbf{Case 3.}\quad 8000800000008000 \xrightarrow{2r,\Delta k_1=8800000000000000} 8000800000008000,$$
$$\textbf{Case 4.}\quad 0080008000000080 \xrightarrow{2r,\Delta k_1=2200000000000000} 0080008000000080,$$
$$\textbf{Case 5.}\quad 0800080000000800 \xrightarrow{2r,\Delta k_1=4400000000000000} 0800080000000800,$$
$$\textbf{Case 6.}\quad 0800080008000000 \xrightarrow{2r,\Delta k_1=4400000000000000} 0800080008000000.$$

At the same time, four nibble keys $(M \circ P)^{-1}(f_{20}(k_1))[10, 13, 14, 15]$ need to be guessed (k_0 has been guessed in the two cases above), and then there is 40-bit information of k_1 that has not been guessed.

Table 8 Cryptanalysis of full PRIDE

Notation	The difference of the intermediate state
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

Therefore, when the four additional cases are used, the attack requires $6 \times 2^{39} = 2^{41.6}$ chosen plaintexts, and its time complexity is

$$2^{41.6} + 6 \times 2^{35} + 6 \times 2^{39} + 2^{40} \approx 2^{42.7}\text{encryptions},$$

which is the best time–data trade-off.

5.3 Key-recovery attack using a 17-round path

In this subsection, we recover the key by using another 2-round iterative related-key differential characteristic

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

which leads to a 17-round (rounds 2–18) related-key differential with probability 2^{-32}.

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

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

The attack procedure is as follows:

(1) **Data collection.** Encrypt 2^n structures, in each of which plaintexts traverse in nibbles 1 and 5 and have fixed values in the remaining nibbles. There are 2^8 plaintexts in the structure, which leads to 2^{15} pairs. For the ciphertexts, the adversary chooses the pairs that satisfy the output difference in Table 6. There remain $2^{-25}(= 2^{15} \times 2^{-40})$ pairs.

(2) **Key recovery.**

(a) Guess the 8-bit key $k_0 \oplus P^{-1}(f_1(k_1))[1, 5]$, partially encrypt the 1st and 5th nibbles of plaintext, and sieve 2^8 pairs whose S-box output difference $\Delta Y_1[1] = \Delta Y_1[5] =$ 0x8, which leaves 2^{-33} pairs remaining.

(b) Guess $k_0[1, 4, 5, 8, 9, 13]$ one by one (here, we can obtain $P^{-1}(f_1(k_1))[1, 5]$), partially decrypt the corresponding nibbles of ciphertext, and check whether the difference of the decrypted nibbles is $\Delta X_{20}[1, 4, 5, 8, 9, 13] = ****, 0**0, ****, 0**0, ****$, or $****$. The probabilities are 1, 2^{-2}, 1, 2^{-2}, 1, and 1, respectively. There remain $2^{-33} \times 2^{-4} = 2^{-37}$ pairs.

(c) Decrypt the remaining pairs through the L-layer. According to Observations 3 and 4, the probability of satisfying the condition ΔZ_{19} is $2^{-12}(= 2^{-2} \times 2^{-2} \times 2^{-4} \times 2^{-4})$. Therefore, there remain $2^{-37} \times 2^{-12} = 2^{-49}$ pairs.

(d) Guess the 40-bit $k_0[2,3,6,7,10,11,12,14,15,16]$ and the 8-bit $(M\circ P)^{-1}(f_{20}(k_1))[1,5]$. Decrypt the remaining pairs, and check whether the output difference of $\Delta X_{19}[1,5]$ is 0x8. On average, $2^{-49}\times 2^{-8} = 2^{-57}$ pairs of data remain. Here, we guess 64-bit information of k_0 and 16-bit information of k_1 in all.

(e) Exhaustively search the remaining 48-bit information of k_1 that is not guessed in the earlier steps.

In the attack procedure, since the probability of our related-key differential is 2^{-32}, we require n to be 26 and expect two remaining pairs to distinguish the right key from the wrong keys. At this point, about 2^{-31} pairs are expected to remain for the wrong keys.

Complexity analysis. The data collection step 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, and we omit it here. Step (d) requires $2^{32}\times 2\times 2^{-23}\times 2^{48}\times 1/20 = 2^{53.7}$ encryptions. After Step (d), there are about 2^{40} 80-bit keys (64-bit k_0 and 16-bit k_1) for a pair, so Step (e) requires $2^{40}\times 2^{48} = 2^{88}$ encryptions.

Therefore, the attack requires 2^{34} chosen plaintexts and 2^{88} encryptions.

We can also apply the time–data tradeoff method to analyze full PRIDE. We add another case:

$$0080008000000000 \xrightarrow{1r} 0000000000000000 \xrightarrow{1r} 0080008000000000,$$

which leads to a 17-round related-key differential:

$$0080008000000000 \xrightarrow{16r} 0080008000000000 \xrightarrow{1r} 0000000000000000.$$

At this point, the procedure needs to guess 24-bit $k_0[2,3,6,7,11,15]$, 8-bit $k_0\oplus P^{-1}(f_1(k_1))[3,7]$, and 8-bit $(M\circ P)^{-1}(f_{20}(k_1))[3,7]$. Then, there remain 16-bit k_0 and 32-bit k_1 information to be guessed, which requires 2^{48} encryptions. Therefore, the attack requires $2\times 2^{34} = 2^{35}$ chosen plaintexts and its time complexity is $2\times 2^{53.7} = 2^{54.7}$ encryptions.

6 Conclusion

We first investigated and found some weaknesses of the key schedule. By utilizing these weaknesses, we found eight 2-round iterative related-key differential characteristics that could be used to construct 18-round related-key differentials for the block cipher PRIDE. Then, after considering the function $g_r^{(1)}$, we also found four 2-round iterative related-key differential characteristics with $\Delta g_r^{(1)}(k_{1,2}) = 0x80$ and four 2-round iterative related-key differential characteristics in three weak-key classes with $2^{126.4}$ or 2^{122} keys. Based on one of the related-key differentials, we attacked full PRIDE using 2^{39} chosen plaintexts and 2^{92} encryptions. Using multiple related-key differentials, the analysis required $2^{41.6}$ plaintexts and $2^{42.7}$ encryptions. Using the 17-round related-key differentials, the complexity of the cryptanalysis was 2^{35} plaintexts and $2^{54.7}$ encryptions. These are the first results on full PRIDE, and show that the PRIDE block cipher is not secure against a related-key differential attack.

Acknowledgements This work was supported by Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-13-010).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Bogdanov A, Knudsen L R, Leader G, et al. PRESENT: an ultra-lightweight block cipher. In: Proceedings of Cryptographic Hardware and Embedded Systems. Berlin/Heidelberg: Springer-Verlag, 2007. 450–466
2 Knudsen L R, Leander G, Poschmann A, et al. PRINTcipher: a block cipher for IC printing. In: Proceedings of Cryptographic Hardware and Embedded Systems. Berlin/Heidelberg: Springer-Verlag, 2010. 16–32
3 Guo L, Peyrin T, Poschmann A, et al. The LED block cipher. In: Proceedings of Cryptographic Hardware and Embedded Systems. Berlin/Heidelberg: Springer-Verlag, 2011. 326–341
4 Wu W L, Zhang L. LBlock: a lightweight block cipher. In: Proceedings of Applied Cryptography and Network Security. Berlin/Heidelberg: Springer-Verlag, 2011. 327–344

5 Borghoff J, Canteaut A, Güneysu T, et al. PRINCE–a low-latency block cihper for pervasive computing applications-extended abstract. In: Proceedings of ASIACRYPT. Berlin/Heidelberg: Springer-Verlag, 2012. 208–225
6 Beaulieuand R, Shors D, Smith J, et al. Performance of the SIMON and SPECK Family of Lightweight Block Ciphers. Technical Peport, National Security Agency, 2014
7 Albrecht M R, Driessen B, Kavun E B, et al. Block ciphers–focus on the linear layer (feat. PRIDE). In: Proceedings of CRYPTO. Berlin/Heidelberg: Springer-Verlag, 2014. 57–76
8 Zhao J Y, Wang X Y, Wang M Q, et al. Differential analysis on block cipher PRIDE. Cryptology ePrint Archive, 2014, 2014: 525
9 Yang Q Q, Hu L, Sun S W, et al. Improved differential analysis of block cipher PRIDE. In: Proceedings of IPSEC. Berlin/Heidelberg: Springer-Verlag, 2015. 209–219
10 Dinur I. Cryptanalytic time-memory-data tradeoffs for FX-constructions with applications to PRINCE and PRIDE. In: Proceedings of EUROCRYPT. Berlin/Heidelberg: Springer-Verlag, 2015. 231–253
11 Biham E. New types of cryptanalytic attacks using related keys. J Cryptology, 1994, 7: 229–246
12 Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems. J Cryptology, 1991, 4: 3–72
13 Kelsey J, Schneier B, Wagner D. Key schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In: Proceedings of CRYPTO. Berlin/Heidelberg: Springer-Verlag, 1996. 237–251
14 Biryukov A, Dunkelman O, Keller N, et al. Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In: Proceedings of EUROCRYPT. Berlin/Heidelberg: Springer-Verlag, 2010. 299–319
15 Biryukov A, Khovratovich D. Related-key cryptanalysis of the full AES-192 and AES-256. In: Proceedings of ASIACRYPT. Berlin/Heidelberg: Springer-Verlag, 2009. 1–18
16 Dunkelman O, Keller N, Shamir A. A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. In: Proceedings of CRYPTO. Berlin/Heidelberg: Springer-Verlag, 2010. 393–410
17 Huang J L, Lai X J. What is the effective key length for a block cipher: an attack on every practical block cipher. Sci China Inf Sci, 2014, 57: 072110

Appendix A

$$L_0 = (L_0)^{-1} = \begin{pmatrix} 0000100010001000 \\ 0000010001000100 \\ 0000001000100010 \\ 0000000100010001 \\ 1000000010001000 \\ 0100000001000100 \\ 0010000000100010 \\ 0001000000010001 \\ 1000100010000000 \\ 0100010001000000 \\ 0010001000100000 \\ 0001000100010000 \\ 0000100010001000 \\ 0000010001000100 \\ 0000001000100010 \\ 0000000100010001 \end{pmatrix}, \; L_1 = \begin{pmatrix} 1100000000010000 \\ 0110000000001000 \\ 0011000000000100 \\ 0001100000000010 \\ 0000110000000001 \\ 0000011010000000 \\ 0000001101000000 \\ 1000000100100000 \\ 1000000000011000 \\ 0100000000001100 \\ 0010000000000110 \\ 0001000000000011 \\ 0000100010000001 \\ 0000010011000000 \\ 0000001001100000 \\ 0000000100110000 \end{pmatrix}, \; L_2 = \begin{pmatrix} 0000110000000001 \\ 0000011010000000 \\ 0000001101000000 \\ 1000000100100000 \\ 1100000000010000 \\ 0110000000001000 \\ 0011000000000100 \\ 0001100000000010 \\ 0000100010000001 \\ 0000010011000000 \\ 0000001001100000 \\ 0000000100110000 \\ 1000000000011000 \\ 0100000000001100 \\ 0010000000000110 \\ 0001000000000011 \end{pmatrix},$$

$$(L_1)^{-1} = \begin{pmatrix} 0000001100000010 \\ 1000000100000001 \\ 1100000010000000 \\ 0110000001000000 \\ 0011000000100000 \\ 0001100000010000 \\ 0000110000001000 \\ 0000011000000100 \\ 0001000000011000 \\ 0000100000001100 \\ 0000010000000110 \\ 0000001000000011 \\ 0000000110000001 \\ 1000000011000000 \\ 0100000001100000 \\ 0010000000110000 \end{pmatrix}, \ (L_2)^{-1} = \begin{pmatrix} 0011000000100000 \\ 0001100000010000 \\ 0000110000001000 \\ 0000011000000100 \\ 0000001100000010 \\ 1000000100000001 \\ 1100000010000000 \\ 0110000001000000 \\ 0000000110000001 \\ 1000000011000000 \\ 0100000001100000 \\ 0010000000110000 \\ 0001000000011000 \\ 0000100000001100 \\ 0000010000000110 \\ 0000001000000011 \end{pmatrix}, \ L_3 = (L_3)^{-1} = \begin{pmatrix} 1000100000001000 \\ 0100010000000100 \\ 0010001000000010 \\ 0001000100000001 \\ 1000100010000000 \\ 0100010001000000 \\ 0010001000100000 \\ 0001000100010000 \\ 0000100010001000 \\ 0000010001000100 \\ 0000001000100010 \\ 0000000100010001 \\ 1000000010001000 \\ 0100000001000100 \\ 0010000000100010 \\ 0001000000010001 \end{pmatrix}.$$

Table A1 Permutation $P(x)$ of the 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 A2 Permutation $P^{-1}(x)$ of the 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