Differential Analysis on Block Cipher PRIDE

Jingyuan Zhao[1] , Xiaoyun Wang[1], Meiqin Wang[1], and Xiaoyang Dong[1]

[1]Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China

Abstract. The lightweight block cipher PRIDE designed by Albrecht et al., appears in CRYPTO 2014. The designers claim that their method of constructing linear layer is good both in security and efficiency. In this paper, we find 16 different 2-round iterative characteristics utilizing the weaknesses of S-box and linear layer, construct several 15-round differentials. Based on one of the differentials, we launch differential attack on 18-round PRIDE. The data, time and memory complexity are 2^{60}, 2^{66} and 2^{64}, respectively.

Keywords: Differential Analysis, Block Cipher, PRIDE

1 Introduction

Lightweight cryptography has become an attractive and active field nowadays, and a lot of lightweight block ciphers are published during the last decade, such as PRESENT[1], LED[2], PRINCE[3], NSA standard SIMON and SPECK[4] etc.

PRIDE[5] is designed by Albrecht et al. in CRYPTO 2014, and they aim to design a software-friendly and hardware-friendly lightweight block cipher which is comparable to SIMON and SPECK both in speed and memory size, so far as to outperform all the other existing block ciphers of similar key-sizes.

Differential analysis[6] proposed by Biham and Shamir is a basic and effective attack on block cipher. This method focuses on differences of plaintext pairs and their difference evolution during the encryption process. Analysts usually start from finding difference propagation of one round and extending it for more rounds, then the sequence of intermediate differences for all rounds and their associated probabilities is called differential characteristic. By adding several rounds before and after the differential characteristic, guessing subkeys used in these rounds, encrypting and decrypting plaintexts and ciphertexts, we can determine the right key by the advantage of the probability.

Our Contribution. In this paper, we concern the new lightweight block cipher PRIDE and study its security. We find that there are several weaknesses on PRIDE

- There are 3 fixed points in S-box, they are $S(0x5) = 0x5$, $S(0xa) = 0xa$, $S(0xd) = 0xd$.
- Difference propagations of S-box from 1-bit to 1-bit exist.

- For difference propagation of 1-bit to 1-bit cases in S-box, the diffusion of P can offset diffusion effort of P^{-1}.

Based on the these weaknesses, we find 16 different 2-round iterative characteristics and construct several 15-round differentials. Finally, we attack 18 rounds of PRIDE with 2^{60} chosen plaintexts, 2^{66} encryptions and 2^{64} bytes, respectively.

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 the differential characteristics of PRIDE and we describe differential attack on 18-round PRIDE in Section 5. Section 6 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 the key addition layer of the r-th round
Y_r	the state after the S-box layer of the r-th round input
Z_r	the state after the $\mathcal{P}$ permutation layer of the r-th round
W_r	the state after the matrix layer of the r-th round
O_r	the output of the r-th round
C	the ciphertext of block cipher PRIDE
ΔX	the XOR difference of X and X'
$\oplus$	bitwise exclusive OR (XOR)
$x\|\|y$	bit string concatenation of x and y
$X[n_1, n_2, ...]$	the n_1, n_2,...-th nibbles of state X, $1 \leq n_1 < n_2 < ... \leq 16$
$X\{b_1, b_2, ...\}$	the b_1, b_2,...-th bits of state X, $1 \leq b_1 < b_2 < ... \leq 64$, numbered from the left to right

3 Description of PRIDE

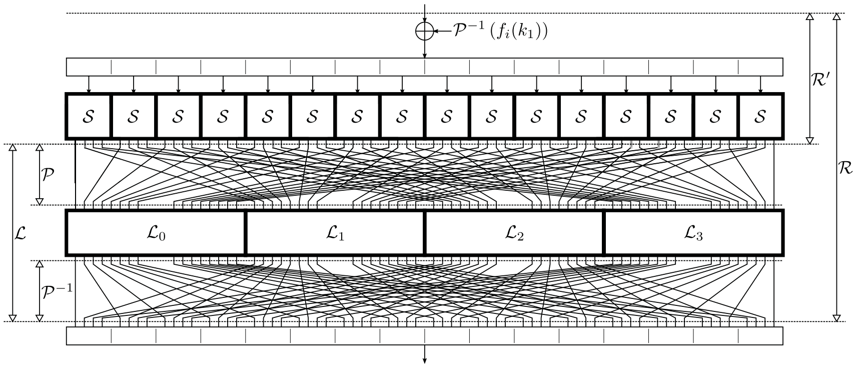
PRIDE designed by Albrecht et al. is a SPN structure block cipher with 64-bit block and 128-bit key. The 64-bit input of the round function is splitted into 16 4-bit nibbles, XORed with the round key, and fed into 16 parallel 4-bit Sboxes and then permuted and processed by the linear layer, see Fig. 3. The cipher has 20 rounds, the first 19 rounds of which are identical, and the linear layer of the last round is omitted, see Fig. 2.

3.1 S-box of Block Cipher PRIDE

The PRIDE S-box is given in Table 1:

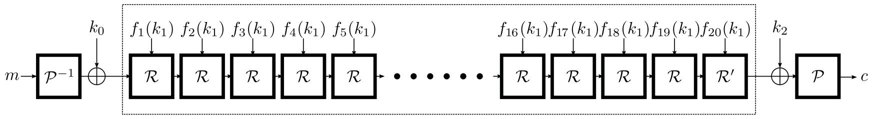
3.2 The Linear Layer of Block Cipher PRIDE

The linear layer $\mathcal{L}$ of block cipher PRIDE can be divided into three sub-layers, a permutation layer $\mathcal{P}$, a matrix layer $\mathcal{M}$ and another permutation layer $\mathcal{P}^{-1}$



$\mathcal{P}^{-1}(f_i(k_1))$
$\mathcal{R}'$
$\mathcal{R}$
$\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$ $\mathcal{S}$
$\mathcal{P}$
$\mathcal{L}$
$\mathcal{L}_0$
$\mathcal{L}_1$
$\mathcal{L}_2$
$\mathcal{L}_3$
$\mathcal{P}^{-1}$

Fig. 1. The Round Function $\mathcal{R}$ of PRIDE



m
$\mathcal{P}^{-1}$
k_0
$f_1(k_1)$ $f_2(k_1)$ $f_3(k_1)$ $f_4(k_1)$ $f_5(k_1)$
$\mathcal{R}$ $\mathcal{R}$ $\mathcal{R}$ $\mathcal{R}$ $\mathcal{R}$
$f_{16}(k_1)$ $f_{17}(k_1)$ $f_{18}(k_1)$ $f_{19}(k_1)$ $f_{20}(k_1)$
$\mathcal{R}$ $\mathcal{R}$ $\mathcal{R}$ $\mathcal{R}$ $\mathcal{R}'$
k_2
$\mathcal{P}$
c

Fig. 2. Overall Structure of the PRIDE

which is the inverse of $\mathcal{P}$:

$$\mathcal{M} : \mathcal{L}_0 \times \mathcal{L}_1 \times \mathcal{L}_2 \times \mathcal{L}_3$$

$$\mathcal{L} : \mathcal{P}^{-1} \circ \mathcal{M} \circ \mathcal{P}$$

The detailed definitions of $\mathcal{P}$, $\mathcal{P}^{-1}$, $\mathcal{L}_i (i = 0, 1, 2, 3)$ are in Appendix.

3.3 Key Schedule of Block Cipher PRIDE

The 128-bit master key for block cipher PRIDE is $(k_0||k_1)$, the sizes of $k_i (i = 0, 1)$ are 64. k_0 is used for pre-whitening and post-whitening, while k_1 is used to produce the subkey $f_r(k_1)$ for round r.

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

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.

Table 1. 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

3.4 Discussion on PRIDE

Since pre-whitening and post-whitening only use 64 bits key and the other 64 bits are used as round keys. Without security claim as PRINCE, we can attack 20 rounds of PRIDE by Meet-in-the-Middle method with 2^{32} known plaintexts, 2^{96} table look-up and 2^{41} bytes, respectively.

The Meet-in-the-Middle attack presented by Diffie and Hellman[7] have been successfully used against several block ciphers. It devotes to splitting the whole cipher E_k into $E_k{=}E^2{}_{k_2} \cdot E^1_{k_1}$, and guessing k_1 and k_2 respectively to compute and check whether $E^1_{k_1}(m)$ equal to ${E^2}^{-1}_{k_2}(c)$ or not. If $E^1_{k_1}(m){=}{E^2}^{-1}_{k_2}(c)$, the key guessed is the right one. Meet-in-the-Middle attack is also very effective when applied to PRIDE.

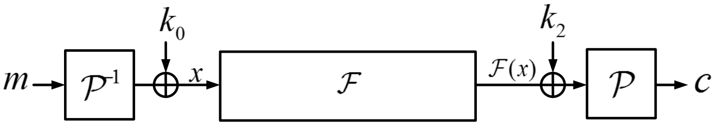


Fig. 3. Abstract Structure of PRIDE

1. Collect 2^{32} pairs of (m, c)
2. For each of 2^{64} possible values of k_1:
   (a) Randomly choose 2^{32} values of x, calculate the corresponding $\mathcal{F}(x)$, store $(x, \mathcal{F}(x), x \oplus \mathcal{F}(x))$ in a hash table $\mathcal{H}$ indexed by $x \oplus \mathcal{F}(x)$,
   (b) For each (m, c) pair, calculate $\mathcal{P}^{-1}(m \oplus c)$ and choose the item in $\mathcal{H}$ where $x \oplus \mathcal{F}(x) = \mathcal{P}^{-1}(m \oplus c)$, calculate $k_0 = \mathcal{P}^{-1}(m) \oplus x$,
   (c) Encrypt a plaintext m using (k_0, k_1). If we get the right ciphertext c, (k_0, k_1) is the right key.

The data complexity of this process is 2^{32}, the time complexity is 2^{96} table look-up, and the memory complexity is 2^{41} bytes. Since the size of key is 128 bits, and this structure can not reach the security level expected. We propose the designer use k_0 and k_1 as round keys iteratively.

4 Differential Characteristic of Block Cipher PRIDE

In this section, we first present the XOR difference distribution of S-box in Table 2, from which we can see that there are several difference propagations from 1-

bit to 1-bit. Mounting 2-round iterative differential characteristics in Table 3, we find the 15-round differential characteristic in Table 5.

Table 2. XOR Difference Distribution Table for PRIDE S-box

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0x1	0	0	0	0	4	4	4	4	0	0	0	0	0	0	0	0
0x2	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x3	0	0	0	0	0	0	0	0	4	0	0	4	2	2	2	2
0x4	0	4	0	0	0	0	4	0	0	2	2	0	2	0	0	2
0x5	0	4	0	0	0	4	0	0	0	2	2	0	2	0	0	2
0x6	0	4	0	0	4	0	0	0	0	2	2	0	0	2	2	0
0x7	0	4	0	0	0	0	0	4	0	2	2	0	0	2	2	0
0x8	0	0	4	4	0	0	0	0	4	0	4	0	0	0	0	0
0x9	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
0xa	0	0	0	0	2	2	2	2	4	0	4	0	0	0	0	0
0xb	0	0	4	4	0	0	0	0	0	0	0	0	2	2	2	2
0xc	0	0	2	2	2	2	0	0	0	2	0	2	2	0	2	0
0xd	0	0	2	2	0	0	2	2	0	2	0	2	0	2	0	2
0xe	0	0	2	2	0	0	2	2	0	2	0	2	2	0	2	0
0xf	0	0	2	2	2	2	0	0	0	2	0	2	0	2	0	2

Observation 1 *If the input difference of S-box is* $0x8$*, the output difference is* $0x8$ *with probability* $\frac{1}{4}$*. We can obtain 2-round iterative differential characteristic holding with probability* 2^{-8} *as in Table 3:*

Table 3. 2-Round Differential Characteristic for PRIDE

ΔI_r	0x0	0x8	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔX_r	0x0	0x8	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔY_r	0x0	0x8	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔZ_r	0x4	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔW_r	0x0	0x4	0x4	0x4	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔI_{r+1}	0x0	0x0	0x0	0x0	0x0	0x8	0x0	0x0	0x0	0x8	0x0	0x0	0x0	0x8	0x0	0x0
ΔX_{r+1}	0x0	0x0	0x0	0x0	0x0	0x8	0x0	0x0	0x0	0x8	0x0	0x0	0x0	0x8	0x0	0x0
ΔY_{r+1}	0x0	0x0	0x0	0x0	0x0	0x8	0x0	0x0	0x0	0x8	0x0	0x0	0x0	0x8	0x0	0x0
ΔZ_{r+1}	0x0	0x4	0x4	0x4	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔW_{r+1}	0x4	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔI_{r+2}	0x0	0x8	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0

There are totally 16 2-round iterative differential characteristics listed in Table 4:

Table 4. 16 2-Round Differential Characteristics

$$(8000000000000000)\xrightarrow{1\text{r}}(0000800080008000)\xrightarrow{1\text{r}}(8000000000000000)$$

$$(0800000000000000)\xrightarrow{1\text{r}}(0000080008000800)\xrightarrow{1\text{r}}(0800000000000000)$$

$$(0080000000000000)\xrightarrow{1\text{r}}(0000800000800080)\xrightarrow{1\text{r}}(0080000000000000)$$

$$\vdots$$

$$(0000000000000800)\xrightarrow{1\text{r}}(0800080008000000)\xrightarrow{1\text{r}}(0000000000000800)$$

$$(0000000000000080)\xrightarrow{1\text{r}}(0080008000800000)\xrightarrow{1\text{r}}(8000000000000080)$$

$$(0000000000000008)\xrightarrow{1\text{r}}(0008000800080000)\xrightarrow{1\text{r}}(0000000000000008)$$

Based on Observation 1, we iterative the 2-Round differential characteristic in Table 3 for 7 times and then attach anther one round behind them, we can obtain 15 rounds differential characteristic with probability $p = \frac{1}{2^{58}}$. The starting and the ending points are listed in Table 5.

Table 5. 15-Round Differential Characteristic for PRIDE

ΔI_r	0x0	0x8	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0	0x0
ΔX_{r+15}	0x0	0x0	0x0	0x0	0x0	0x8	0x0	0x0	0x0	0x8	0x0	0x0	0x8	0x0	0x0	0x0

Observation 2 *If the input difference of $\mathcal{L}_0^{-1}$ is ΔW_r[1, 2,..., 16]=(0?00 0?00 0?00 0?00), the output difference is ΔZ_r[1, 2,..., 16]=(0000 0?00 0?00 0?00) with probability $\frac{1}{2}$; If the input difference of $\mathcal{L}_3^{-1}$ is ΔW_r[49, 50,..., 64]=(0?00 0?00 0?00 0?00), the output difference is ΔZ_r[49, 50,..., 64]=(0000 0?00 0?00 0?00) with probability $\frac{1}{2}$. ("?" is the undermined value)*

Since ΔZ_r[1, 2,..., 16]=$\mathcal{L}_0^{-1} \times \Delta W_r$[1, 2,..., 16]=$\mathcal{L}_0^{-1}\times$ (0?00 0?00 0?00 0?00)=(0?00 0?00 0?00 0?00), and (0?00 0?00 0?00 0?00)=(0000 0?00 0?00 0?00) with probability $\frac{1}{2}$; $\mathcal{L}_3^{-1}$ situation is the same as $\mathcal{L}_0^{-1}$.

Observation 3 *If the input difference of $\mathcal{L}_1^{-1}$ is ΔW_r[17, 18,..., 32]=(00?0 ???0 0??0 0??0), the output difference is ΔZ_r[17, 18,..., 32]=(0000 0?00 0?00 0?00) with probability $\frac{1}{2^5}$; If the input difference of $\mathcal{L}_2^{-1}$ is ΔW_r[33, 34,..., 48]=(???0 00?0 0??0 0??0), the output difference is ΔZ_r[33, 34,..., 48]=(0000 0?00 0?00 0?00) with probability $\frac{1}{2^5}$.*

Proof. Since $\Delta Z_r[17, 18, \ldots, 32]^T$=$\mathcal{L}_1^{-1} \times \Delta W_r[17, 18, \ldots, 32]^T$, the input difference (00?0 ???0 0??0 0??0) and the output difference (???0 00?0 0??0 0??0)

Table 6. Differential Analysis on 18-round PRIDE

ΔI_1	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
ΔY_1	0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000
ΔZ_1	0000 0100 0100 0100 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔW_1	0100 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔI_2	0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔX_{17}	0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000
ΔY_{17}	0000 0000 0000 0000 0000 ???? 0000 0000 0000 ???? 0000 0000 0000 ???? 0000 0000
ΔZ_{17}	0000 0?00 0?00 0?00 0000 0?00 0?00 0?00 0000 0?00 0?00 0?00 0000 0?00 0?00 0?00
ΔW_{17}	0?00 0?00 0?00 0?00 00?0 ???0 0??0 0??0 ???0 00?0 0??0 0??0 0?00 0?00 0?00 0?00
ΔI_{18}	00?0 ?0?? 0??0 0000 0?00 ??0? 0??0 0000 0000 ???? 0??? 0000 0000 ???? 0?00 0000
ΔX_{18}	00?0 ?0?? 0??0 0000 0?00 ??0? 0??0 0000 0000 ???? 0??? 0000 0000 ???? 0?00 0000
ΔY_{18}	???? ???? ???? 0000 ???? ???? ???? 0000 0000 ???? ???? 0000 0000 ???? ???? 0000
ΔO_{18}	???? ???? ???? 0000 ???? ???? ???? 0000 0000 ???? ???? 0000 0000 ???? ???? 0000

construct a linear equation set as follows:

$$\begin{cases} \Delta W_r[23] \oplus \Delta W_r[31] = 0 \\ \Delta W_r[19] \oplus \Delta W_r[26] = 0 \\ \Delta W_r[19] \oplus \Delta W_r[27] = 0 \\ \Delta W_r[21] \oplus \Delta W_r[22] = 0 \\ \Delta W_r[22] \oplus \Delta W_r[23] \oplus \Delta W_r[30] = 0 \\ \Delta W_r[22] \oplus \Delta W_r[30] \oplus \Delta W_r[31] = 0 \\ \Delta W_r[23] \oplus \Delta W_r[31] = 0 \\ \Delta W_r[26] \oplus \Delta W_r[27] = 0 \\ \Delta W_r[19] \oplus \Delta W_r[27] = 0 \end{cases}$$

Considering the rank this equation set can be simplified as follows:

$$\begin{cases} \Delta W_r[19] \oplus \Delta W_r[26] = 0 \\ \Delta W_r[21] \oplus \Delta W_r[22] = 0 \\ \Delta W_r[22] \oplus \Delta W_r[23] \oplus \Delta W_r[30] = 0 \\ \Delta W_r[22] \oplus \Delta W_r[30] \oplus \Delta W_r[31] = 0 \\ \Delta W_r[19] \oplus \Delta W_r[27] = 0 \end{cases}$$

We can get the output difference ΔZ_r[17, 18,..., 32]=(0000 0?00 0?00 0?00) if the 5 equations are satisfied. The probability is 2^{-5}.

Since the proof of $\mathcal{L}_2^{-1}$ is similar, we omitted it here. □

5 Differential Attack on 18-Round PRIDE

In this section, we put our 15-round differential characteristic from the second round to the 16 round, extending 1 round backward and 2 rounds forward, and analyze 18-th block cipher PRIDE.

- **Data Collection Phase**. Choose 2^n structures, in each of which, plaintexts fix in nibbles 1, 2, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16 and traverse in nibbles 6, 10, 14. There are 2^{12} plaintexts and their corresponding ciphertexts which consist of 2^{23} pairs. After 18-round encryption, the ciphertext difference should satisfy $\Delta C[4, 8, 9, 12, 13, 16] = 0$, which makes only 2^{-1} pairs left.

– **Key Recovery Phase**. 2^{64} key bits corresponding to $(k_0 \oplus \mathcal{P}^{-1}(f_1(k_1)))[6]$, $(k_0 \oplus \mathcal{P}^{-1}(f_1(k_1)))[10]$, $(k_0 \oplus \mathcal{P}^{-1}(f_1(k_1)))[14]$ in the 1st round, $k_0[1,2,3]$, $k_0[5,6,7]$, $k_0[10,11]$ and $k_0[14,15]$ of the post-whitening, and 12 bits equivalent key $(\mathcal{M} \circ \mathcal{P})^{-1}(f_r(k_1))[6]$, $(\mathcal{M} \circ \mathcal{P})^{-1}(f_r(k_1))[10]$, $(\mathcal{M} \circ \mathcal{P})^{-1}(f_r(k_1))[14]$ are guessed in this phase, we build 2^{64} counters for each of them.
  - Step 1. Guess $(k_0 \oplus \mathcal{P}^{-1}(f_1(k_1)))[6]$, encrypt the 6-th nibble of plaintexts partially, and sieve 2^4 pairs whose S-box output difference $\Delta Y_1[6] = 0x8$, which makes 2^{-5} pairs remain.
  - Step 2. Guess $(k_0 \oplus \mathcal{P}^{-1}(f_1(k_1)))[10]$, encrypt the 10-th nibble of plaintexts partially, and sieve 2^4 pairs whose S-box output difference $\Delta Y_1[10] = 0x8$, and 2^{-9} pairs left.
  - Step 3. Guess $(k_0 \oplus \mathcal{P}^{-1}(f_1(k_1)))[14]$ encrypt the 14th nibble of plaintexts partially, and sieve anther 2^4 pairs whose S-box output difference $\Delta Y_1[14] = 0x8$, 2^{-13} pairs fulfil our condition.
  - Step 4. Guess $k_0[i](i = 1,2,3,5,6,7,15,11,10,14)$ one by one, decrypt the corresponding nibbles of ciphertexts partially, and sieve pairs by factors 2^{-3}, 2^{-1}, 2^{-2}, 2^{-3}, 2^{-1}, 2^{-2}, 2^{-1}, 2^{-3}, 1 and 1, respectively, 2^{-29} pairs left.
  - Step 5. According to Observation 2 and 3, decrypt the remaining pairs and sieve them by 2^{12} factor without guessing any key bits and 2^{-41} pairs left after this process.
  - Step 6. For each pairs left, guess $(\mathcal{M} \circ \mathcal{P})^{-1}(f_r(k_1))[6]$, decrypt the 6-th nibble of $\Delta Y_{17}[6]$ partially, and sieve pairs by factor 2^4 whose S-box input difference $\Delta X_{17}[6] = 0x8$, on average 2^{-45} right pairs remain.
  - Step 7. For each pairs left, guess $(\mathcal{M} \circ \mathcal{P})^{-1}(f_r(k_1))[10]$, decrypt the 10-th nibble of $\Delta Y_{17}[10]$ partially, and sieve pairs by factor 2^4 whose S-box input difference $\Delta X_{17}[10] = 0x8$, on average 2^{-49} right pairs remain.
  - Step 8. For each pairs left, guess $(\mathcal{M} \circ \mathcal{P})^{-1}(f_r(k_1))[6]$, decrypt the 14-th nibble of $\Delta Y_{17}[14]$ partially, and sieve pairs by factor 2^4 whose S-box input difference $\Delta X_{17}[14] = 0x8$, on average 2^{-53} right pairs remain. If any pairs left for some key value, increment the corresponding counter.

    In order to distinguish the right key from the wrong ones, we expect two pairs satisfy our differential path which require n to be 48 since the probability of our differential path is 2^{-58}. In this way, about 2^{-5} pairs expected to left for the wrong keys.

  - Step 9. Exhaustively search the rest 64 bits key which are not guessed in the former process.

– **Data/Time/Memory Complexity**
  - Data Complexity: 2^{60} chosen plaintexts.
  - Time Complexity: Data collection phase: 2^{60} encryptions/Key recovery phase: 2^{66} encryptions.
    - ∗ Step 1. For 2^4 possible key values, encrypt the 6-th nibble for each plaintexts of the left pairs, when considering our 18-round PRIDE, the time complexity is $2 \times 2^{47} \times 2^4 \times \frac{1}{16} \times \frac{1}{18} \approx 2^{43}$ encryptions .

        - Step 2. The time complexity of this step is similar with that of Step 1. $2 \times 2^{43} \times 2^4 \times 2^4 \times \frac{1}{16} \times \frac{1}{18} \approx 2^{43}$ encryptions.
        - Step 3. Similar with Step 1. the time complexity is about $2 \times 2^{39} \times 2^8 \times 2^4 \times \frac{1}{16} \times \frac{1}{18} \approx 2^{43}$ encryptions.
        - Step 4. The dominant time complexity of this step is the last nibble operation, since the sieved pairs is less than key bits guessed for the former nibbles operations, it is about $2 \times 2^{19} \times 2^{48} \times 2^4 \times \frac{1}{16} \times \frac{1}{18} \approx 2^{62}$ encryptions.
        - Step 5. For each key guessed in former steps decrypt each middle state of the left pairs from O_{17} to Y_{17}, the time complexity is about $2 \times 2^{19} \times 2^{52} \times \frac{1}{4} \times \frac{1}{18} \approx 2^{66}$ encryptions.
        - Step 6. Similar with Step 1. the time complexity is about $2 \times 2^7 \times 2^{52} \times 2^4 \times \frac{1}{16} \times \frac{1}{18} \approx 2^{55}$ encryptions.
        - Step 7. Similar with Step 1. the time complexity is about $2 \times 2^3 \times 2^{56} \times 2^4 \times \frac{1}{16} \times \frac{1}{18} \approx 2^{55}$ encryptions.
        - Step 8. Similar with Step 1. the time complexity is about $2 \times 2^{-1} \times 2^{60} \times 2^4 \times \frac{1}{16} \times \frac{1}{18} \approx 2^{55}$ encryptions.
        - Step 9. 2^{64} encryptions.
    - Memory Complexity: 2^{64} bytes.
- **Success Probability** According to [8], the success probability for differential analysis is

$$P_s = \int_{-\frac{\sqrt{\mu S/N}-\phi^{-1}(1-2^{-a})}{\sqrt{S/N+1}}}^{\infty} \phi(x)dx \approx 0.61$$

where a is the number of key bits guessed and μ is the number of right pairs.

6 Conclusion

By observing properties of S-box and linear layer of PRIDE, we find 16 different 2-round iterative characteristics and construct several 15-round differentials for block cipher PRIDE. Based on one of the differentials, we attack 18-round PRIDE using 2^{60} chosen plaintexts 2^{66} encryptions and 2^{64} bytes. This is the first analysis result on PRIDE.

References

1. A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, C. Vikkelsoe: Present: An ultra-lightweight block cipher. In Proc. CHES 2007, LNCS 4727, pp. 450-466, Springer, 2007.
2. J. Guo, T. Peyrin, A. Poschmann, M. Robshaw: The LED Block Cipher. In Proc. CHES 2011, LNCS 6917, pp. 326-341, Springer, 2011.
3. 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, T. Yalçin: Prince - a low-latency block cipher for pervasive computing applications - extended abstract. In Proc. ASIACRYPT 2012, LNCS 7658, pp. 208-225, Springer, 2012.

4. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks and Louis Wingers: The SIMON and SPECK Families of Lightweight Block Ciphers. IACR Cryptology ePrint Archive, 2013:414, 2013.

5. Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, Tolga Yalcin: Block Ciphers - Focus On The Linear Layer (feat. PRIDE) . Pre-proceeding of CRYPTO 2014.

6. E. Biham and A. Shamir: Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, vol. 4, no.1, pp. 3-72, Springer, 1991.

7. W. Diffie, M.E. Hellman: Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer, vol. 10(6), pp. 74–84, IEEE Computer Society Press, 1977.

8. A.A. Selçuk, A. Biçak: On probability of success in linear and differential cryptanalysis. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 02: 3rd International Conference on Security in Communication Networks. LNCS 2576, pp. 174-185. Springer, 2002.

Appendix

$$\mathcal{L}_0 = \mathcal{L}_0^{-1} = \begin{pmatrix}
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1\\
1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1\\
1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1\\
1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0
\end{pmatrix}
\mathcal{L}_1 = \begin{pmatrix}
1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0\\
1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&1&0&0&0&0
\end{pmatrix}$$

$$\mathcal{L}_2 = \begin{pmatrix}
0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&1&0&0&0&0&0&0\\
1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&1&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&1&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1
\end{pmatrix}
\mathcal{L}_3 = \mathcal{L}_3^{-1} = \begin{pmatrix}
1&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
0&1&0&0&0&1&0&0&0&0&0&0&0&1&0&0\\
0&0&1&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&1&0&0&0&0&0&0&0&1\\
1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&1&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&1&0&0&0&1&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&1\\
1&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&0&1&0&0&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&1
\end{pmatrix}$$

$$\mathcal{L}_1^{-1} = \begin{pmatrix}
0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1\\
1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0
\end{pmatrix}
\mathcal{L}_2^{-1} = \begin{pmatrix}
0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1\\
1&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1\\
1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1
\end{pmatrix}$$

Table 7. Permutation $\mathcal{P}(x)$ of Block Cipher PRIDE

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathcal{P}(x)$	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
$\mathcal{P}(x)$	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
$\mathcal{P}(x)$	9	25	41	57	10	26	42	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
$\mathcal{P}(x)$	13	29	45	61	14	30	46	62	15	31	47	63	16	32	48	64

Table 8. Permutation $\mathcal{P}^{-1}$ of Block Cipher PRIDE

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathcal{P}^{-1}(x)$	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
$\mathcal{P}^{-1}(x)$	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
$\mathcal{P}^{-1}(x)$	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
$\mathcal{P}^{-1}(x)$	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64