Improved Differential Analysis of Block Cipher PRIDE

Qianqian Yang[1,2,3], Lei Hu[1,2], Siwei Sun[1,2], Kexin Qiao[1,2], Ling Song[1,2], Jinyong Shan[1,2], Xiaoshuang Ma[1,2]

[1]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
[3]University of Chinese Academy of Sciences, Beijing 100049, China
yangqianqian521@126.com

November 25, 2014

Abstract. In CRYPTO 2014 Albrecht *et al.* brought in a 20-round iterative lightweight block cipher PRIDE which is based on a good linear layer for achieving a tradeoff between security and efficiency. A recent analysis is presented by Zhao *et al.*. Inspired by their work, we use an automatic search method to find out 56 iterative differential characteristics of PRIDE, containing 24 1-round iterative characteristics, based on three of them we construct a 15-round differential and perform a differential attack on the 19-round PRIDE, with data, time and memory complexity of 2^{62}, 2^{63} and 2^{71} respectively.

Keywords: Block Cipher, PRIDE, Differential attack, Active S-box, Automatic Method

1 Introduction

PRIDE [1] is a 20-round iterative lightweight block cipher designed by Albrecht *et al.* in CRYPTO 2014, which is based on a good linear layer for achieving a tradeoff between security and efficiency and going to both software-friendly and hardware-friendly. A recent analysis is presented by Zhao *et al.* [4]. They utilized the weaknesses of the S-box and the linear layer to find out 16 different 2-round iterative differential characteristics and construct several 15-round differentials, and based on one of the differential characteristics, they launched a differential attack on the 18-round PRIDE with data, time and memory complexity of $2^{60}, 2^{66}$ and 2^{64}, respectively.

In this paper, using the automatic methods presented in [2, 3], we find out 24 1-round iterative differential characteristics and 32 2-round iterative characteristics, including the same 16 characteristics presented in [4]. With one of the 1-round iterative differential characteristics and inspired by the analysis of Zhao *et al.* [4] we construct a 15-round differential path of differential probability 2^{-60}, and based on which we perform an improved differential attack on the 19-round PRIDE, with data, time and memory complexity of 2^{62}, 2^{63} and 2^{71} respectively.

2 Description of Block Cipher PRIDE

2.1 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 Sbox layer of the r-th round input
Z_r	the state after the 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
?	a bit with uncertain value
$X[n_1, n_2, ...]$	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

2.2 Description of PRIDE

PRIDE is an FX-structure block cipher with 64-bit blocks and 128-bit keys. The 128-bit master key is composed of the subkey k_1 and the pre-whitening key k_0 which is equal to the post-whitening k_2, i.e.,

$$k = k_0||k_1 \; with \; k_2 = k_0.$$

The cipher has an iterations of 20 rounds, of which the first 19 are identical. The structure of the cipher is depicted in Fig.1, which is redrawn from [1].

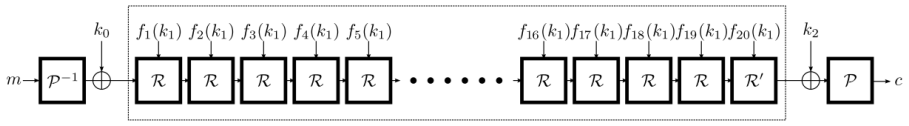

Fig. 1: Overall Structure of the PRIDE

The round function R of PRIDE is an SPN structure: The state is XORed with the round key, fed into 16 parallel 4-bit S-boxes and then permuted and processed by the linear layer, see Fig.2, which is also redrawn from [1].

The S-box of PRIDE is given in Table 1, and the linear layer is defined as

$$M := L_0 \times L_1 \times L_2 \times L_3$$

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

where detailed definitions of $L_i, i \in \{0, 1, 2, 3\}$ are given in Appendix A. The linear layer of the last round is omitted.

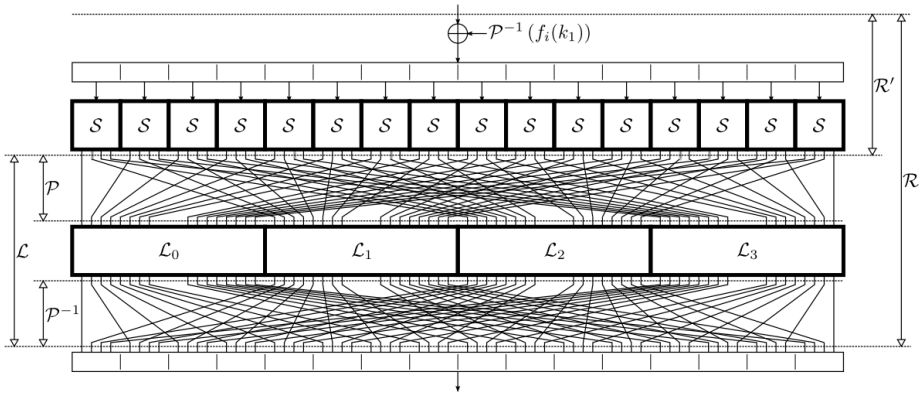

Fig. 2: Round Function R of PRIDE

Table 1: S-box of 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 Differential Attack on 19-Round PRIDE

In this section, we describe our differential attack on the 19-round PRIDE. We first give 24 1-round iterative characteristics, and then construct a 15-round distinguisher by concatenation. Finally we perform a key recovery procedure on the 19-round PRIDE.

3.1 Differential Characteristic of Block Cipher PRIDE

The XOR difference distribution table of the S-box in PRIDE is listed in Table 2. Our attack utilize a table look-up method to recover nibbles of key, thus a concrete difference distribution table with its entries being the specific pairs of input-output values is preferred.

We apply sun *et al*'s automatic search methods [2, 3] to the block cipher PRIDE and find out 56 iterative differential characteristics, which includes 24 1-round characteristics with input(output) hamming weight 2, 16 2-round characteristics with input(output) hamming weight 3 and 16 same 2-round characteristics with input(output) hamming weight 1 as ones described in [4]. We only show the 24 1-round iterative characteristics in Table 3.

We choose the 4th differential characteristic in Table 3 to construct a 15-round differential characteristic with probability 2^{-60} to launch the differential attack on the 19-round PRIDE.

Table 2: XOR Difference Distribution Table for the S-box of PRIDE

	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

3.2 Differential Analysis on Block Cipher PRIDE

In this subsection, we put our 15-round differential characteristic from the 3rd to the 17th round of PRIDE, extending 2 rounds backward and forward respectively. The description is given in Table 4. We find that the hamming weight of ΔY_2 is one less than that of ΔY_1 in [4] and the hamming weight of ΔX_{18} is one less than that of ΔX_{17} in [4]. Additionally, we notice that when the input difference of the S-box is 1000, the output difference must be ?0??, and when the output difference is 1000, the input difference must be ?0??(the authors of [4] seemed to miss this point). Due to the above two rules, we can extend 2 rounds backward and forward respectively to achieve the differential attack on the 19-round PRIDE. Consequently the 1-round iterative characteristics is more appropriate than the 2-round iterative characteristics in [4].

-Data Collection Phase. Choose $2^{25.65}$ structures, in each of which, plaintexts fix in nibbles 4, 6, 8, 11, 12, 15, 16 and traverse in nibbles 1, 2, 3, 5, 7, 9, 10, 13, 14. There are 2^{36} plaintexts and their corresponding ciphertexts which consist of 2^{71} pairs. There are 16 possible values for ΔX_2 since only 4 different input differences of S-box can result in output difference 1000 and the probability is 2^{-2}. Thus, the probability that a pair of plaintexts in a structure can result in the expected input difference of the distinguisher is $16/2^{36} \times 2^{-4} = 2^{-36}$.

Observing from Table 2, we know that the output difference 1000 only has four different input differences. Thus, extending 2 rounds backward has 16 different cases. Similar to backward extending, the extending 2 rounds forward also has 16 different situations. In order to guarantee the bits of exhaustively searching less than 60, we choose the situations which the active S-boxes are

Table 3: 1-round iterative characteristics of PRIDE

1	1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
2	1000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
3	1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000
4	0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
5	0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000
6	0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000
7	0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
8	0000 1000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000
9	0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000
10	0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000
11	0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000
12	0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000
13	0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000
14	0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000
15	0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000
16	0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000
17	0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 1000 0000
18	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000
19	0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000
20	0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000
21	0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000
22	0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000
23	0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000 1000
24	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1000 0000 0000 0000 1000

more than 17 except for 21. There are 109 situations totally. Because of the 5th and the 6th differentials in Table 3 forming the same structures, we use the three differentials to recovery the information about the key. The expected number of right pairs is $2^{25.65+71} \times 2^{-36} \times 2^{-60} \times \frac{109}{16^2} \times 3 = 2$. The data complexity is $2^{25.65} \times 2^{36} \approx 2^{61.65}$.

After 19-round encryption, the ciphertext difference should satisfy $\Delta C[3, 4, 6, 7, 11, 12, 14, 15, 16] = 0$, which makes only $2^{60.65}$ pairs left.

-Key Recovery Phase. ^{65}

Table 4: Differential Analysis on 19-round PRIDE

ΔI_1	???? ???? ???? 0000 ???? 0000 ???? 0000 ???? ???? 0000 0000 ???? ???? 0000 0000
ΔX_1	???? ???? ???? 0000 ???? 0000 ???? 0000 ???? ???? 0000 0000 ???? ???? 0000 0000
ΔY_1	?00? 00?0 00?0 0000 ?00? 0000 00?0 0000 ?0?? 00?0 0000 0000 ?00? 00?0 0000 0000
ΔZ_1	?000 ?000 ?000 ?000 0000 0000 0000 0000 0??0 00?0 ??00 0?00 ?000 ?000 ?000 ?000
ΔW_1	0000 ?000 ?000 0000 0000 0000 0000 0000 0000 ?000 ?000 0000 0000 ?000 ?000 0000
ΔI_2	0000 0000 0000 0000 ?0?? 0000 0000 0000 ?0?? 0000 0000 0000 0000 0000 0000 0000
ΔX_2	0000 0000 0000 0000 ?0?? 0000 0000 0000 ?0?? 0000 0000 0000 0000 0000 0000 0000
ΔY_2	0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔZ_2	0000 1000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔW_2	0000 1000 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
ΔI_3	0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔX_{18}	0000 0000 0000 0000 1000 0000 0000 0000 1000 0000 0000 0000 0000 0000 0000 0000
ΔY_{18}	0000 0000 0000 0000 ?0?? 0000 0000 0000 ?0?? 0000 0000 0000 0000 0000 0000 0000
ΔZ_{18}	0000 ?000 ?000 0000 0000 0000 0000 0000 0000 ?000 ?000 0000 0000 ?000 ?000 0000
ΔW_{18}	?000 ?000 ?000 ?000 0000 0000 0000 0000 ??00 000? ??00 0000 ?000 ?000 ?000 ?000
ΔI_{19}	?0?? 00?0 0000 0000 ?00? 0000 0000 00?0 ?0?? 00?0 0000 0000 ?00? 0000 0000 0000
ΔX_{19}	?0?? 00?0 0000 0000 ?00? 0000 0000 00?0 ?0?? 00?0 0000 0000 ?00? 0000 0000 0000
ΔY_{19}	???? ???? 0000 0000 ???? 0000 0000 ???? ???? ???? 0000 0000 ???? 0000 0000 0000
ΔO_{19}	???? ???? 0000 0000 ???? 0000 0000 ???? ???? ???? 0000 0000 ???? 0000 0000 0000

$2^{56.65} \times (4/16)^4 \times (6/16)^{10} \times 8/16 \approx 2^{33.50}$ pairs left. Next we use the method of table look-up to recovery these bits of key.

- Step 1. Firstly, we recover the values of $(k_0 \oplus P^{-1}(f_1(k_1)))[1]$. For each remaining pair of plaintexts, look up the concrete difference distribution table by its input difference in the first nibble and output difference 1000, we get 4 candidates for $(k_0 \oplus P^{-1}(f_1(k_1)))[1]$ and then store the values in a table, say Table D. The time complexity is about $2^{33.50} \times \frac{1}{16} \times \frac{1}{19} \approx 2^{25.25}$.
- Step 2. For each pair of plaintexts associated with each of its corresponding candidates for $(k_0 \oplus P^{-1}(f_1(k_1)))[1]$, look up the concrete difference distribution table by its input difference in the 13th nibble and output difference 1001, we get 2 candidates for $(k_0 \oplus P^{-1}(f_1(k_1)))[13]$. Again we store the values in Table D. The time complexity is no more than $2^{33.50} \times 4 \times \frac{1}{16} \times \frac{1}{19} \approx 2^{27.25}$.
- Step 3. Similar to Step 2, for each pair of texts associated with each of its corresponding candidates for previously recovered key bits, look up the concrete difference table, we get the candidates for $(k_0 \oplus P^{-1}(f_1(k_1)))[2, 3, 5, 7, 9, 10, 14]$ and $k_0[1, 2, 8, 9, 10, 5]$ successively. The time complexity is about $2^{54.65} \times \frac{1}{16} \times \frac{1}{19} \approx 2^{46.40}$.
- Step 4. Because the value of ΔX_2 and ΔY_{18} are fixed, in order to get the information of $(M \circ P)^{-1}(f_{19}(k_1))[5, 9]$ and $P^{-1}(f_2(k_1))[5, 9]$ we only need to look up four times for all pairs associated with their corresponding candidates for $(k_0 \oplus P^{-1}(f_1(k_1)))[1, 2, 3, 5, 7, 9, 10, 13, 14]$ and $k_0[1, 2, 5, 8, 9, 10, 13]$.

- Step 5. Repeating the same process 109×3 times for different characteristics, we get Table D containing $2^{56.65} \times 2^8 \times 27 \times 3 \approx 2^{70.99}$ candidates for at least 68 bits of key. The most frequently appeared candidate serves as the right one and it cost $2^{56.65} \times 2^8 \times 27 \times 3 \times \frac{1}{16} \times \frac{1}{19} \approx 2^{62.74}$ to find it by common method.
- Step 6. For the rest of the no more than 60 bits, we perform an exhaustive search.

In summary, we achieve that the data, time and memory complexities are 2^{62}, 2^{63} and 2^{71}, respectively.

4 Conclusion

In this paper, we proposed an improved differential attack on the 19-round PRIDE by utilizing new 1-round iterative differential characteristics which is found by automatic search methods. The differential characteristics we used are suitable for extending 4 rounds to launch the differential attack. The data, time and memory complexities of our attack are 2^{62}, 2^{63} and 2^{71} respectively. Moreover, if more differentials can be used at the same time, it may be possible to lunch an attack on the full-round PRIDE.

References

1. Albrecht, M.R., Driessen, B., Kavun, E.B., Leander, G., Paar, C., Yalcin, T.: Block Ciphers - Focus On The Linear Layer (feat. PRIDE). Pre-proceeding of CRYPTO (2014)
2. Sun, S., Hu, L., Wang, M., Wang, P., Qiao, K., Ma, X., Shi, D., Song, L.: Automatic Enumeration of (Related-key) Differential and Linear Characteristics with Predefined Properties and Its Applications. Cryptology ePrint Archive (2014), `http://eprint.iacr.org/2014/747`
3. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-oriented Block Ciphers. In: Advances in Cryptology-ASIACRYPT 2014. pp. 158–178. Springer (2014)
4. Zhao, J., Wang, X., Wang, M., Dong, X.: Differential Analysis on Block Cipher PRIDE. Cryptology ePrint Archive (2014), `http://eprint.iacr.org/2014/525`

Appendix A

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

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

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