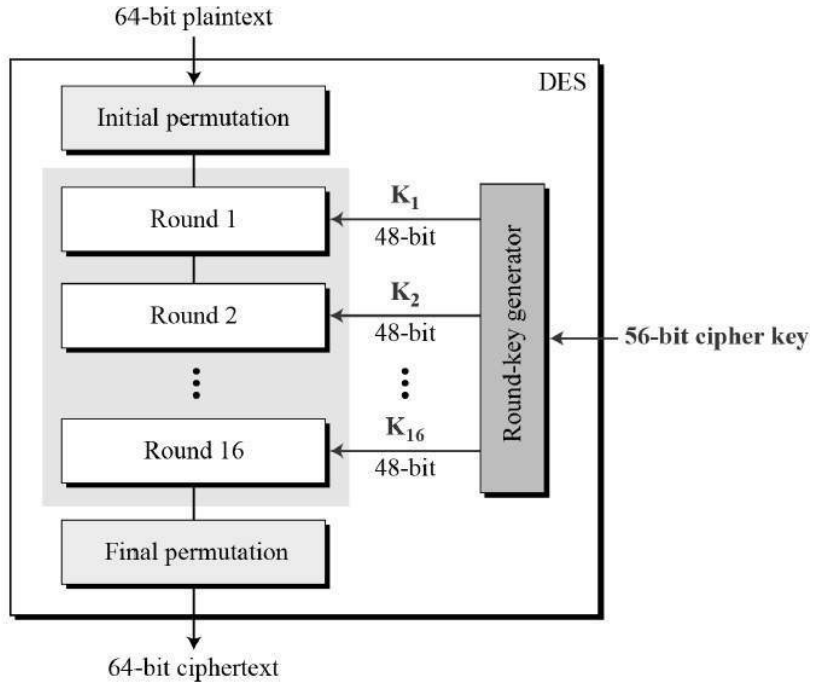
DES algorithm & 양자회로 구현

https://youtu.be/M8YRDcw7C8A

정보컴퓨터공학과 송경주

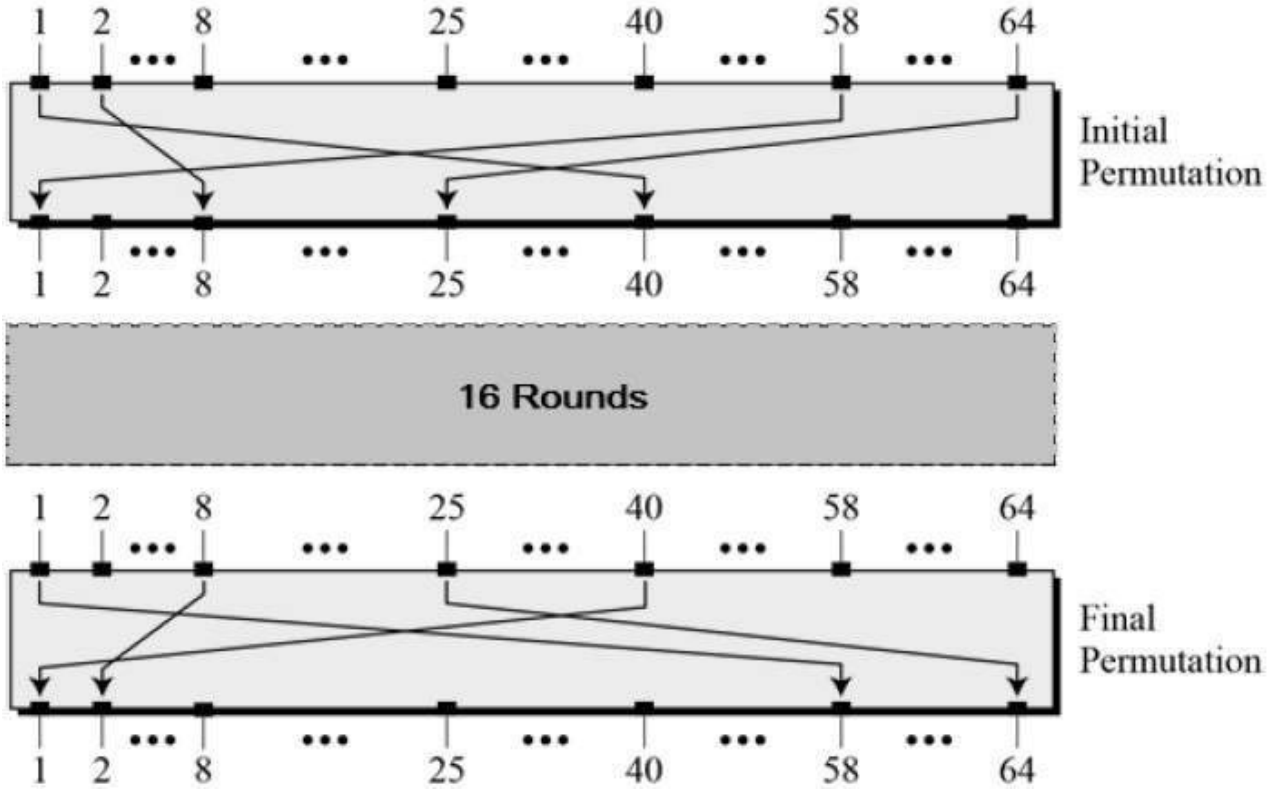
DES

- NIST(National Institute of Standards and Technology)가 발표한 대칭 키 블록암호
- 16 라운드의 Feistel 암호
- Block size : 64bit
- Key length : 56bit
- Initial/Final Permutation, Round function, Round-key generator 로 구성



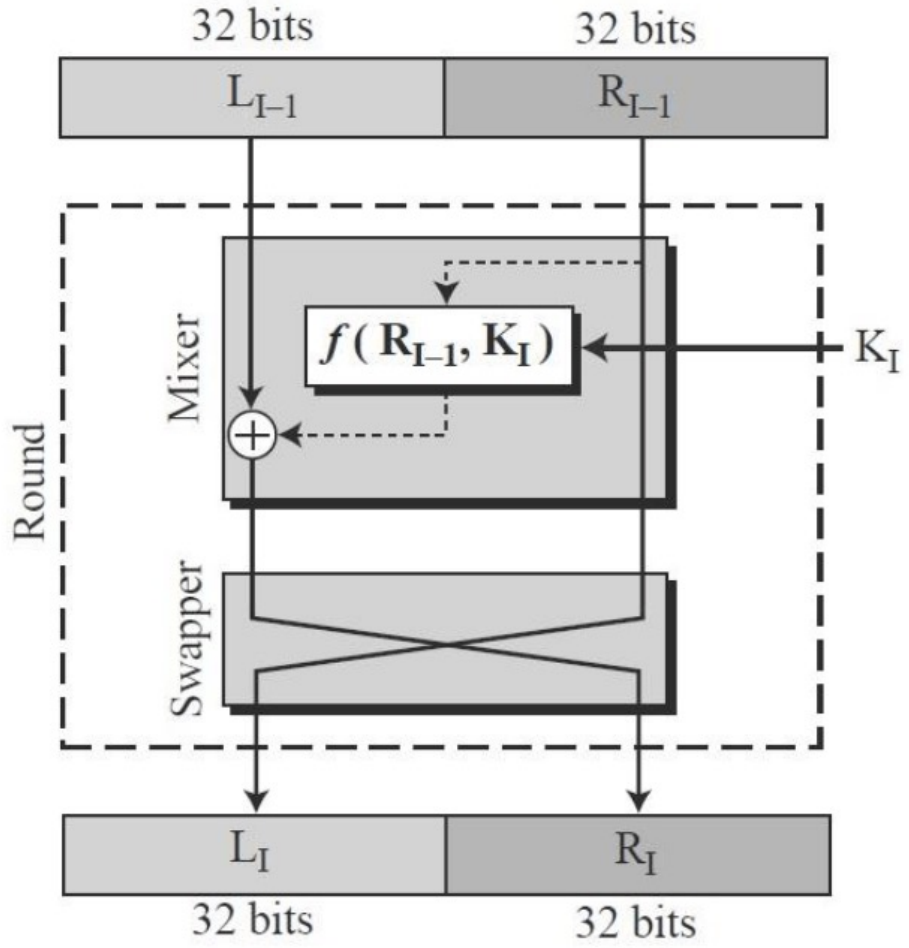
DES

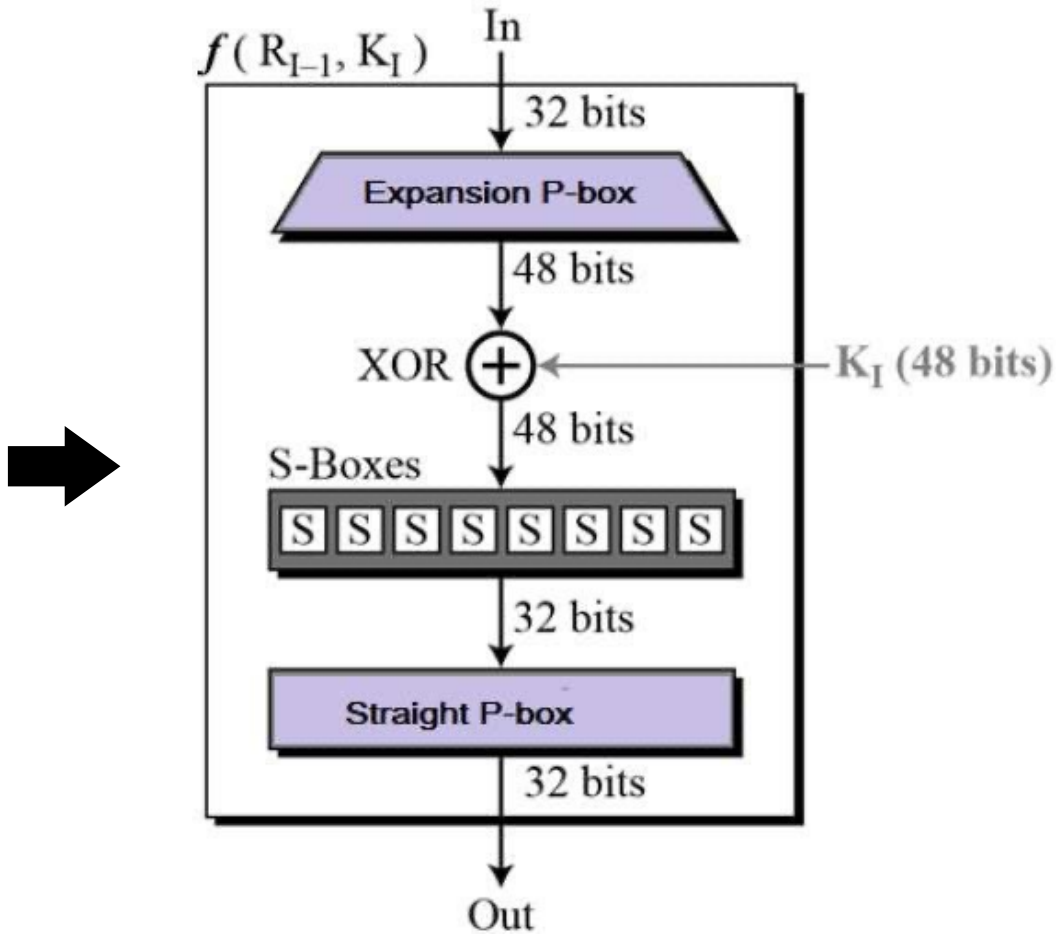
- Permutation : Initial, Final



DES

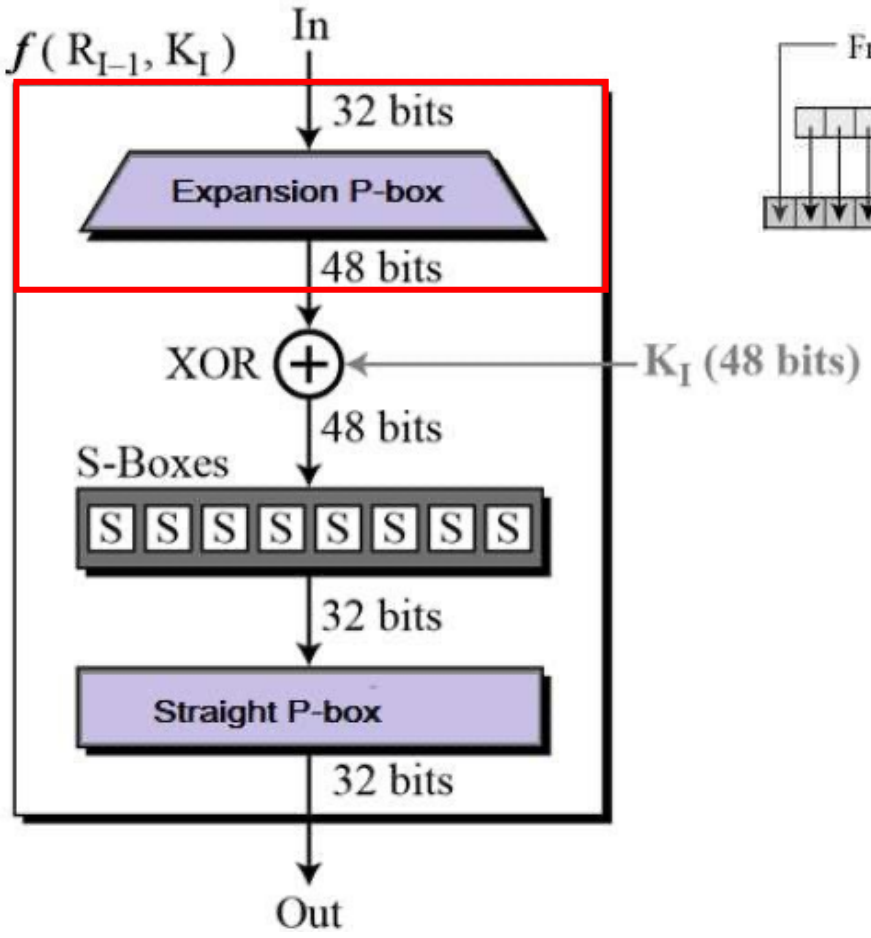
- Round function

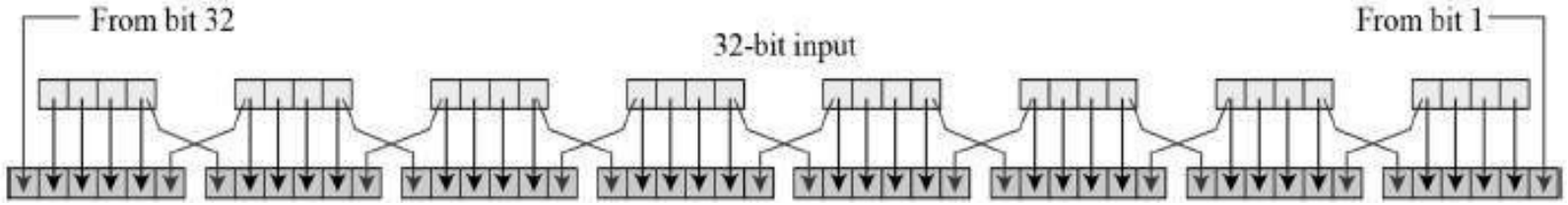




DES

- Round function : Expansion P-box

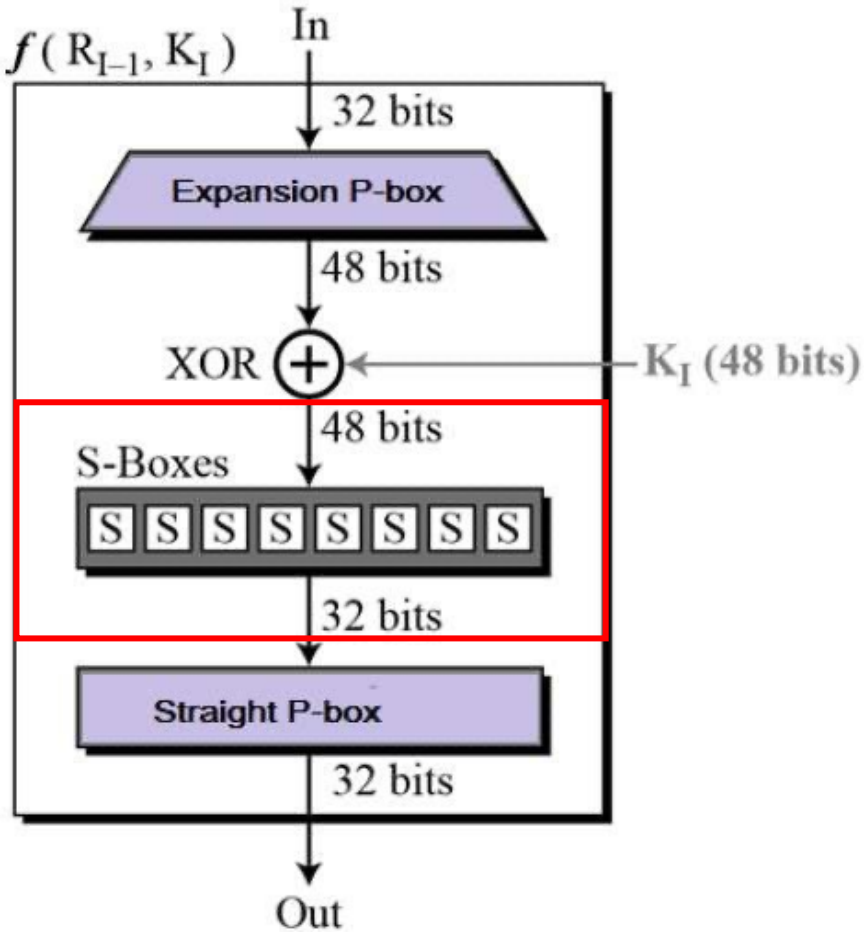


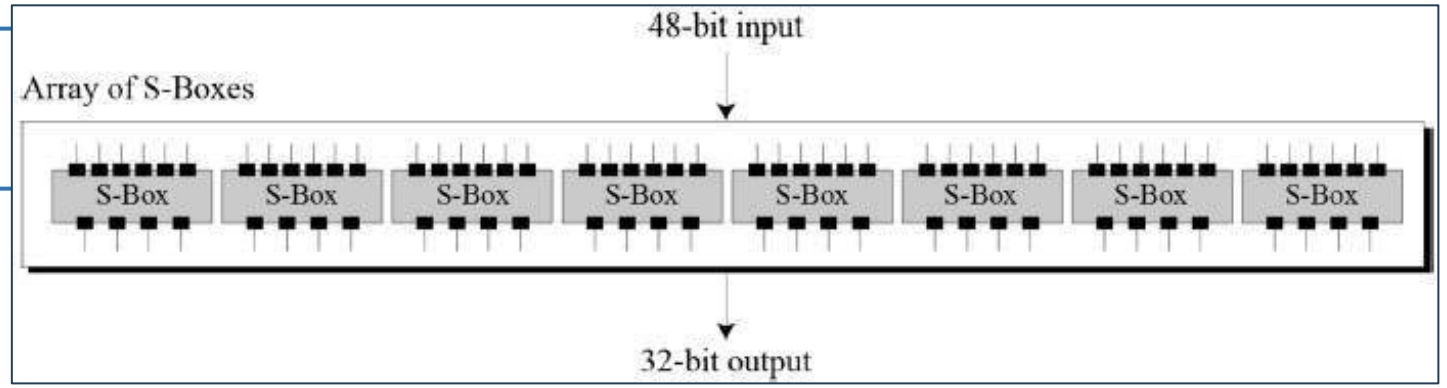


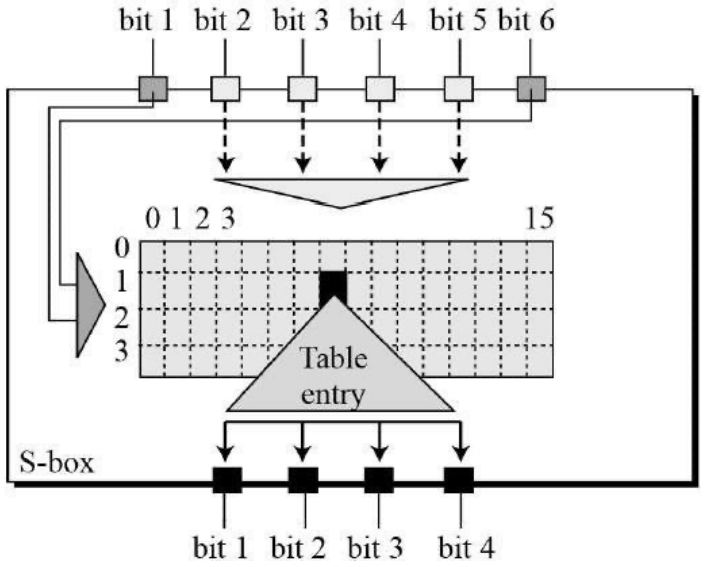
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

DES

- Round function : S-box





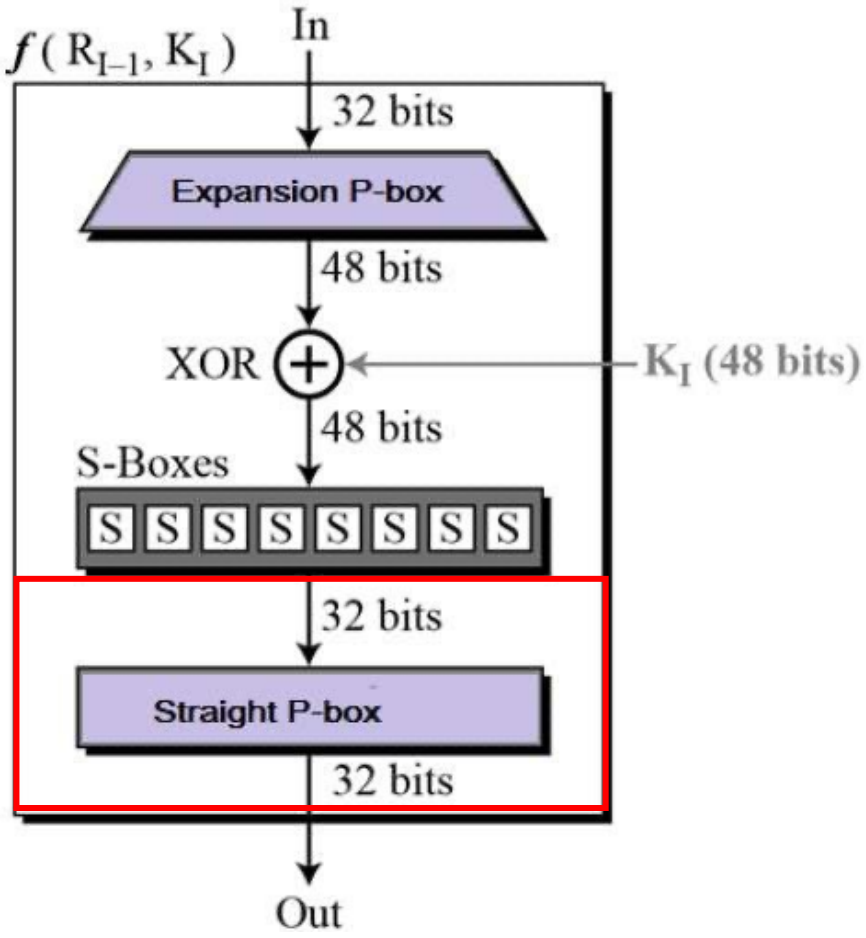


Row #	S_1	1	2	3	...	7	...	15	Column #
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S(i, j) <16, can be represented with 4 bits

DES

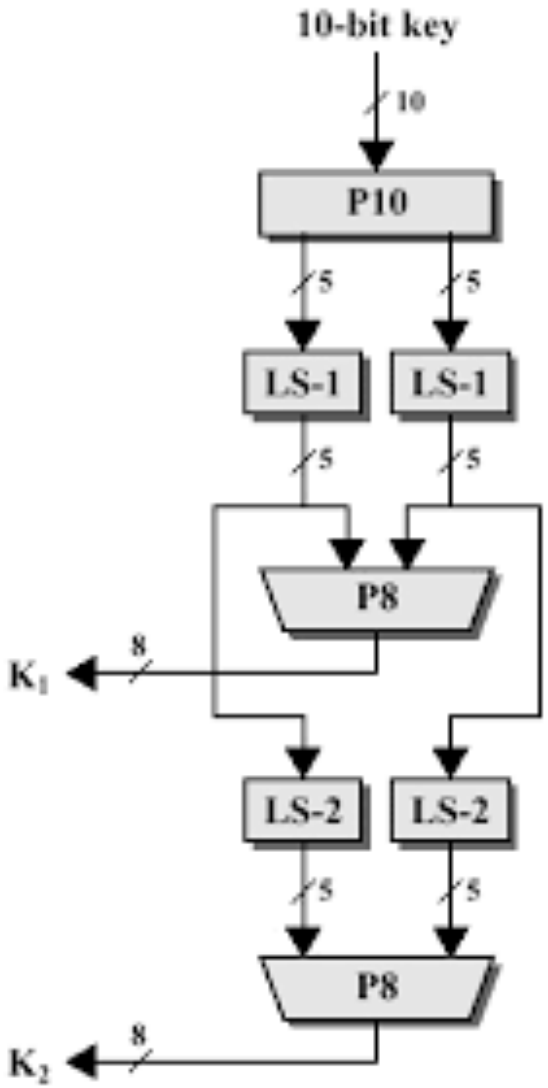
- Round function : Straight P-box



16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

DES

- Key Generation



DES 양자회로

- S-Box1 (Version 1)

```
static void
s1 (
        unsigned long   a1,
        unsigned long   a2,
        unsigned long   a3,
        unsigned long   a4,
        unsigned long   a5,
        unsigned long   a6,
        unsigned long   *out1,
        unsigned long   *out2,
        unsigned long   *out3,
        unsigned long   *out4
) {
        unsigned long   x1, x2, x3, x4, x5, x6, x7, x8;
        unsigned long   x9, x10, x11, x12, x13, x14, x15, x16;
        unsigned long   x17, x18, x19, x20, x21, x22, x23, x24;
        unsigned long   x25, x26, x27, x28, x29, x30, x31, x32;
        unsigned long   x33, x34, x35, x36, x37, x38, x39, x40;
        unsigned long   x41, x42, x43, x44, x45, x46, x47, x48;
        unsigned long   x49, x50, x51, x52, x53, x54, x55, x56;
        unsigned long   x57, x58, x59, x60, x61, x62, x63;
```

input qubit (6)

output qubit (4)

anclia qubit (63)

DES 양자회로

- S-Box1 (Version 2)

```
static void
s1 (
        unsigned long   a1,
        unsigned long   a2,
        unsigned long   a3,
        unsigned long   a4,
        unsigned long   a5,
        unsigned long   a6,
        unsigned long   *out1,
        unsigned long   *out2,
        unsigned long   *out3,
        unsigned long   *out4
) {
        unsigned long   x1, x2, x3, x4, x5, x6, x7, x8;
        unsigned long   x9, x10, x11, x12, x13, x14, x15, x16;
        unsigned long   x17, x18, x19, x20, x21, x22, x23, x24;
        unsigned long   x25, x26, x27, x28, x29, x30, x31, x32;
        unsigned long   x33, x34, x35, x36, x37, x38, x39, x40;
        unsigned long   x41, x42, x43, x44, x45, x46, x47, x48;
        unsigned long   x49, x50, x51, x52, x53, x54, x55, x56;
```

input qubit (6)

output qubit (4)

anclia qubit (56)

DES 양자회로

- S-box (version 1)

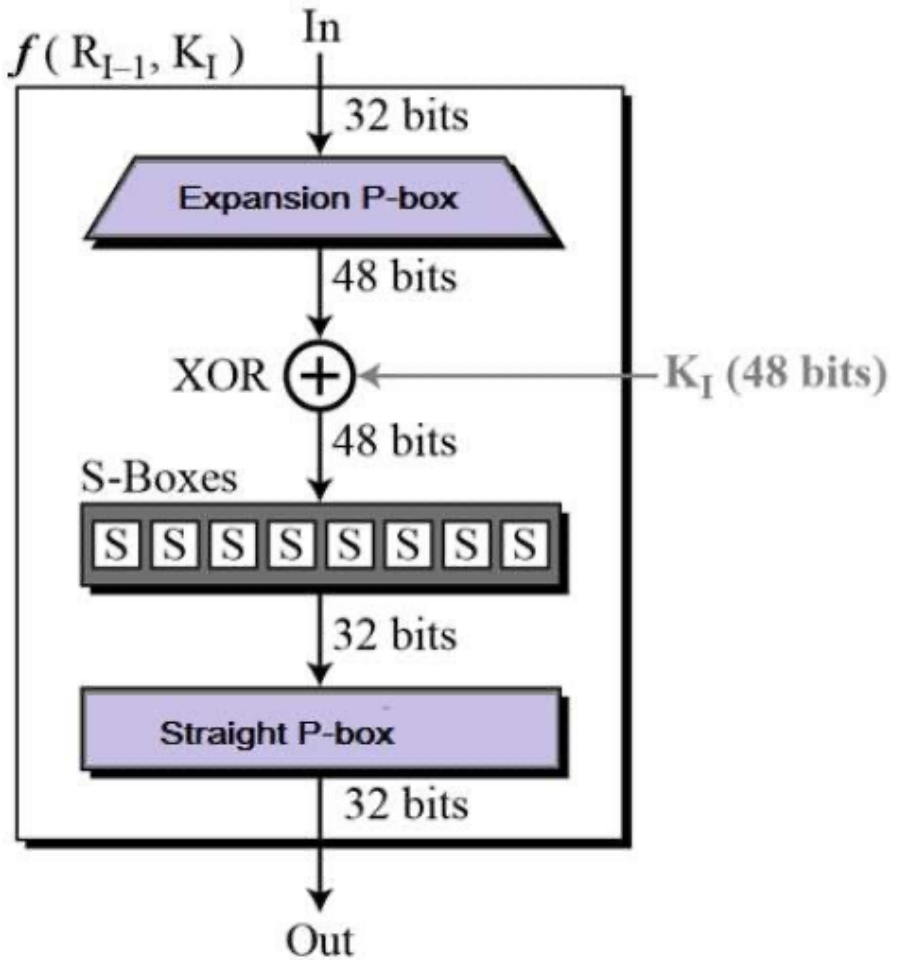
Qubit	Toffoli	CNOT	X	Depth
496	214	652	449	67

- S-box (version 2)

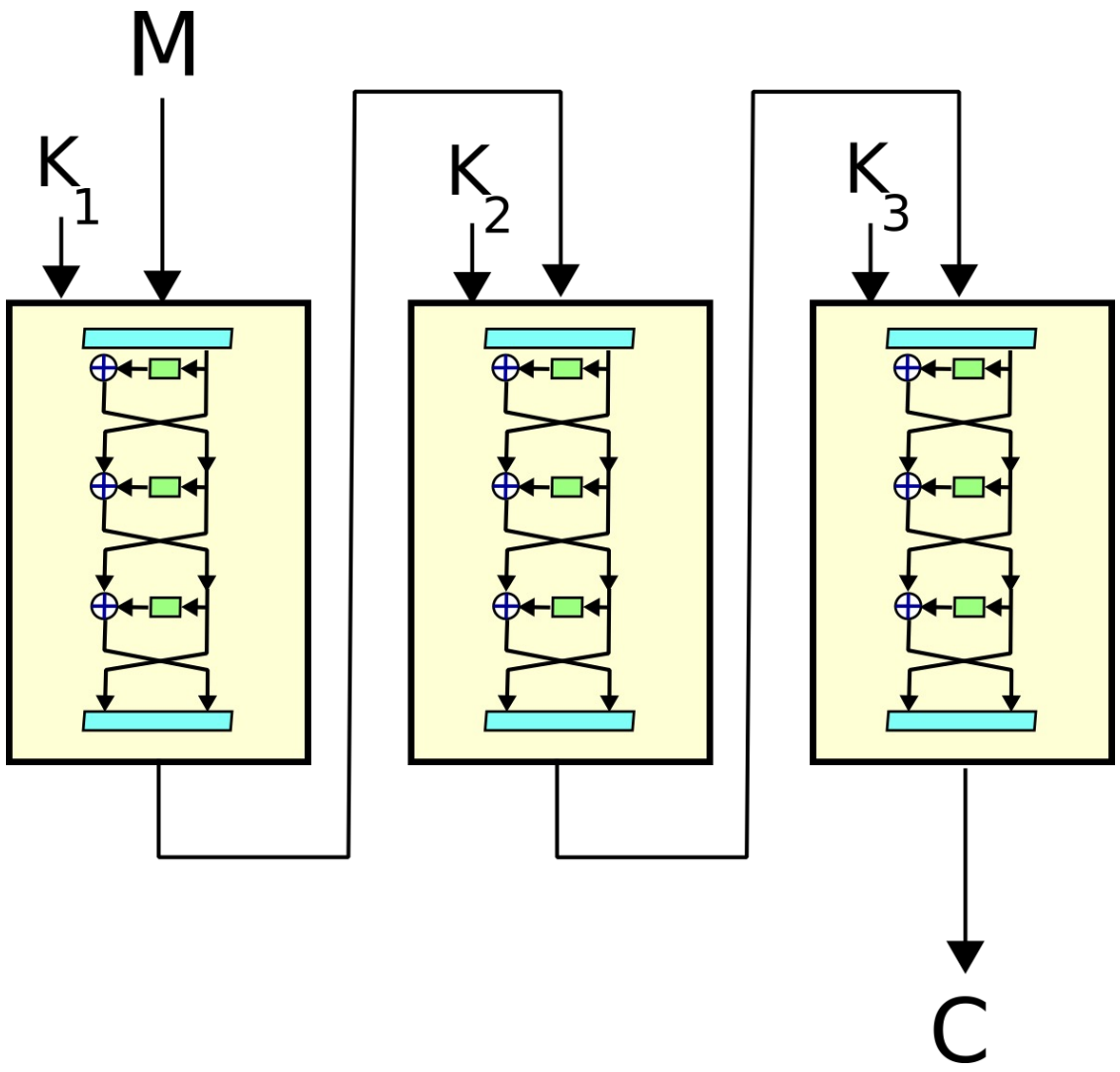
Qubit	Toffoli	CNOT	X	Depth
456	221	561	475	74

DES 양자회로

- Depth-optimized vs Qubit-optimized



Triple-DES (TDES)



DES 양자회로

- Depth-optimized (version 1)

Qubit	Toffoli	CNOT	X	Depth
7,536	3,424	12,992	7,184	1,044

- Depth-optimized (version 2)

Qubit	Toffoli	CNOT	X	Depth
6,896	3,536	11,536	7,600	1,012

DES 양자회로

- Qubit-optimized (version 1)

Qubit	Toffoli	CNOT	X	Depth
816	6,848	20,160	11,232	2,162

- Qubit-optimized (version 2)

Qubit	Toffoli	CNOT	X	Depth
776	7,072	17,856	11,104	2,354

DES 양자회로

- Qubit-optimized vs Depth-optimized

[Version 1]

- Qubit : Qubit-optimized 회로가 Depth-optimized 회로보다 약 89.17% 감소
- Depth : Depth-optimized 회로가 Qubit-optimized 회로보다 약 51.71% 감소

[Version 2]

- Qubit : Qubit-optimized 회로가 Depth-optimized 회로보다 약 88.75% 감소
- Depth : Depth-optimized 회로가 Qubit-optimized 회로보다 약 57% 감소

[All]

- Qubit : Qubit-optimized 회로가 Depth-optimized 회로보다 최대 약 89.7% 감소
- Depth : Depth-optimized 회로가 Qubit-optimized 회로보다 최대 약 57% 감소

Q & A