



# 现代密码学

## 第二十一讲 DES的轮函数及密钥编排

16轮 Feistel结构

信息与软件工程学院

A decorative graphic consisting of ten horizontal blue lines of varying lengths, stacked vertically, is positioned on the left side of the slide.

## 第二十一讲 DES的轮函数及密钥编排

---

A diagram illustrating the components of the DES algorithm. It features two white circles connected by a vertical line. The top circle is connected to a blue horizontal bar containing the text 'DES的轮函数'. The bottom circle is connected to another blue horizontal bar containing the text 'DES的密钥编排'. Both circles have short lines extending from their top and bottom, suggesting they are part of a larger flow or structure.

DES的轮函数

DES的密钥编排

---

# DES的轮函数的结构

设输入为  $(x, y)$

则DES的轮函数输出为:

$$(y, x \oplus f_k(y))$$

连续变换2次后将回到原来用值

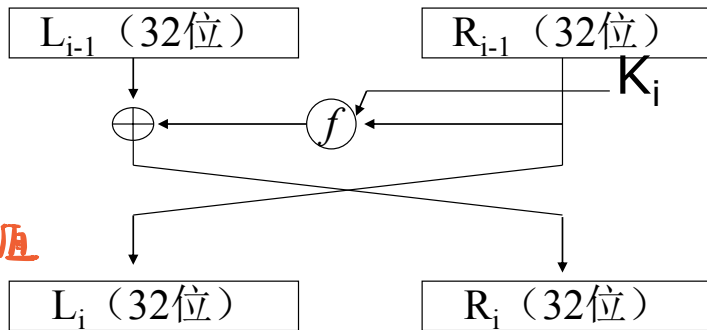
它等价于两个对合变换的复合:

$$(x, y) \mapsto (x \oplus f(k, y), y) \mapsto (y, x \oplus f(k, y))$$

映射

$$(a, b) \mapsto (b, a)$$

采用2次变换出数,也是对合变换



## 注意

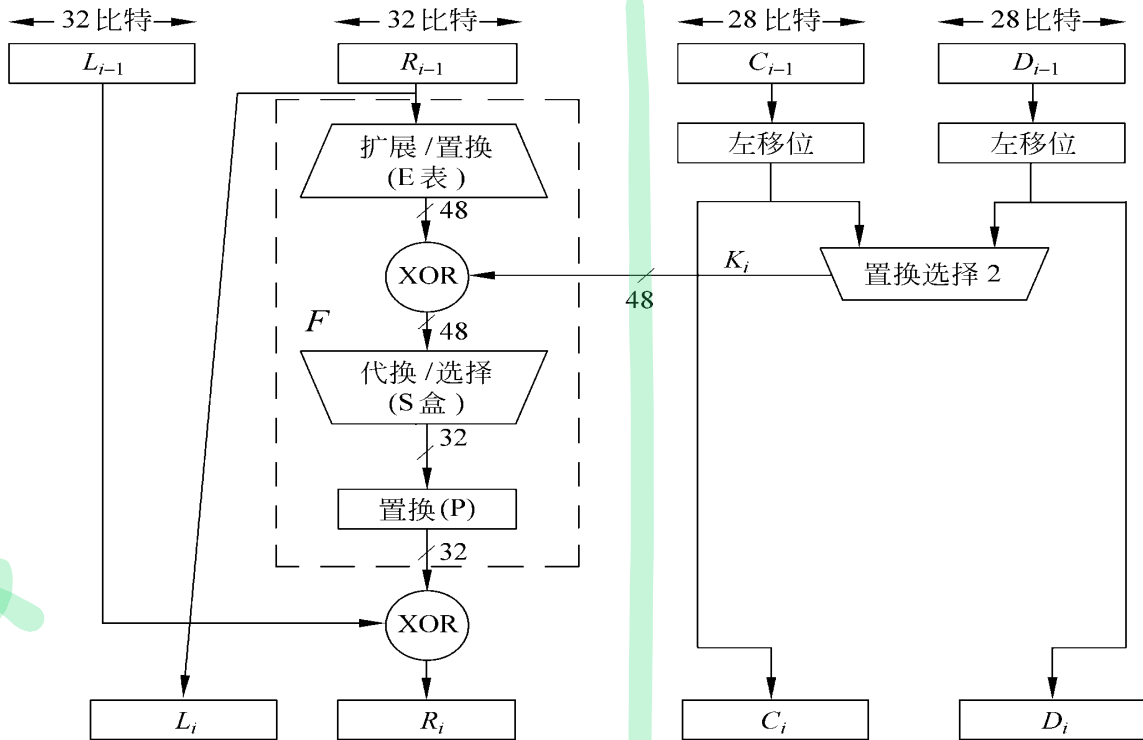
- 无论f函数如何选取，DES的轮函数是一个对合变换。(证明)

$$F(x, y) = (x \oplus f(k, y), y)$$

$$F(F(x, y)) = F(x \oplus f(k, y), y) = ((x \oplus f(k, y)) \oplus f(k, y), y) = (x, y)$$

抵消?

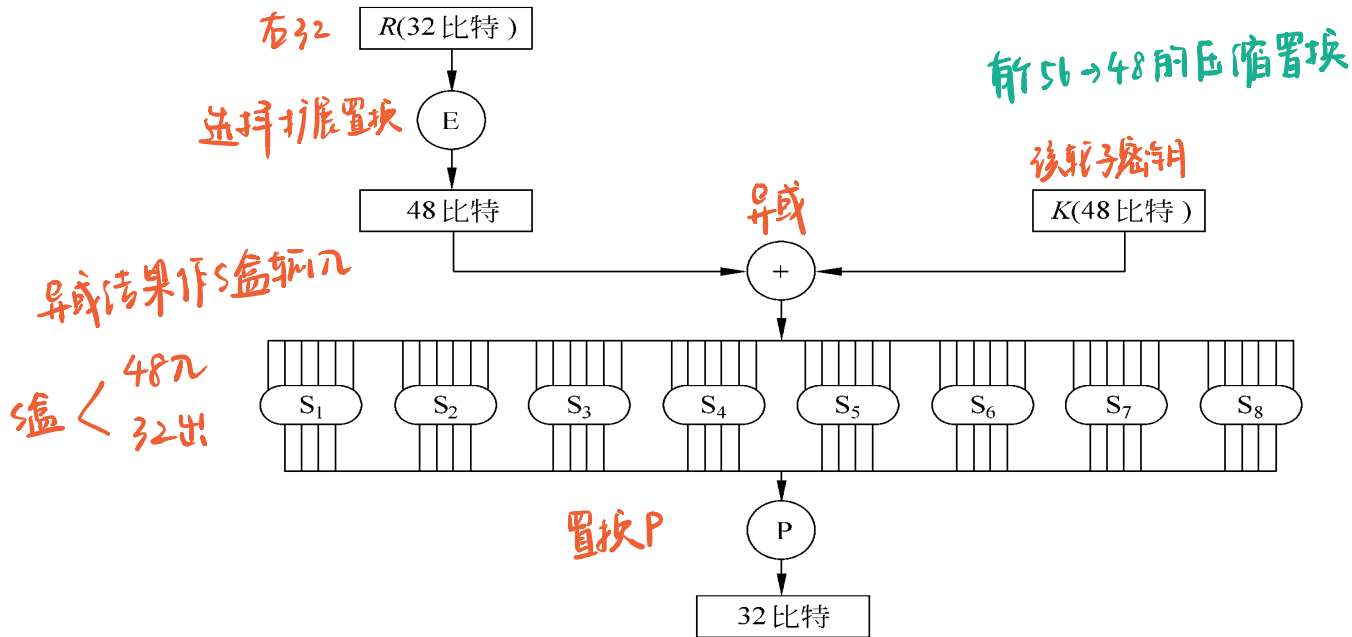
# DES算法轮结构 每轮展开的结构



轮函数

密钥编排

# 函数 $f(R, K)$ 的计算过程



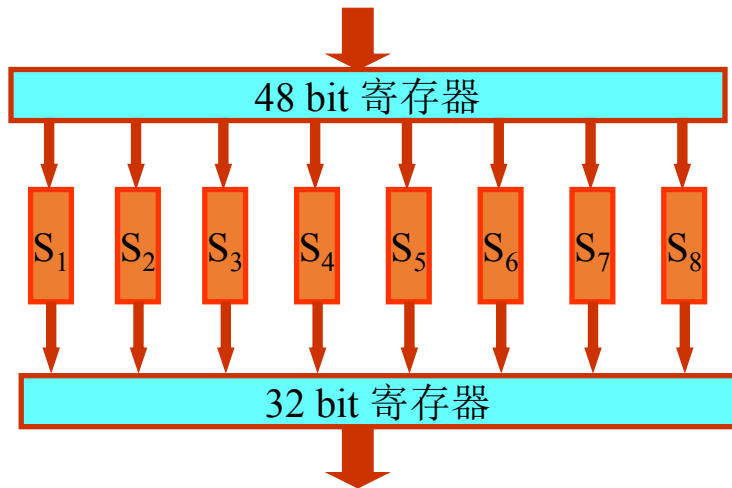
# 选择扩展运算E

<b>32</b>	1	2	3	4	<b>5</b>
<b>4</b>	5	6	7	8	<b>9</b>
<b>8</b>	9	10	11	12	<b>13</b>
<b>12</b>	13	14	15	16	<b>17</b>
<b>16</b>	17	18	19	20	<b>21</b>
<b>20</b>	21	22	23	24	<b>25</b>
<b>24</b>	25	26	27	28	<b>29</b>
<b>28</b>	29	30	31	32	<b>1</b>

原矩阵最左-1

原矩阵最右+1

## 选择压缩运算 $S$





# DES的S盒 例子(4×16矩阵)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S <sub>1</sub>
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	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S <sub>2</sub>
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S <sub>3</sub>
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	

# DES的S-盒的输入和输出关系

2. 高+低构成数

$x_5 x_0$

1 0

3. 行号

1. 输入6bit为: 101100

$x_5 x_4 x_3 x_2 x_1 x_0$

1 0 1 1 0 0

3. 列号

4. 拆为二进制

$(y_3, y_2, y_1, y_0) = (0, 0, 1, 0)$

列号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
行号																
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	2	14	10	0	6	13



## P盒置换

无太多规律

将S-盒变换后的32比特数据再进行P盒置换，置换后得到的32比特即为 $f$ 函数的输出。

### • 基本特点:

- (1) P盒的各输出块的4个比特都来自不同的输入块;
- (2) P盒的各输入块的4个比特都分配到不同的输出块之中;
- (3) P盒的第 $t$ 输出块的4个比特都不来自第 $t$ 输入块。

$P$			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

含义:P盒输出的第1个元是输入的第16个元。

A decorative graphic consisting of ten horizontal blue lines of varying lengths, stacked vertically, is positioned in the top left corner.

## 第二十一讲 DES的轮函数及密钥编排

---

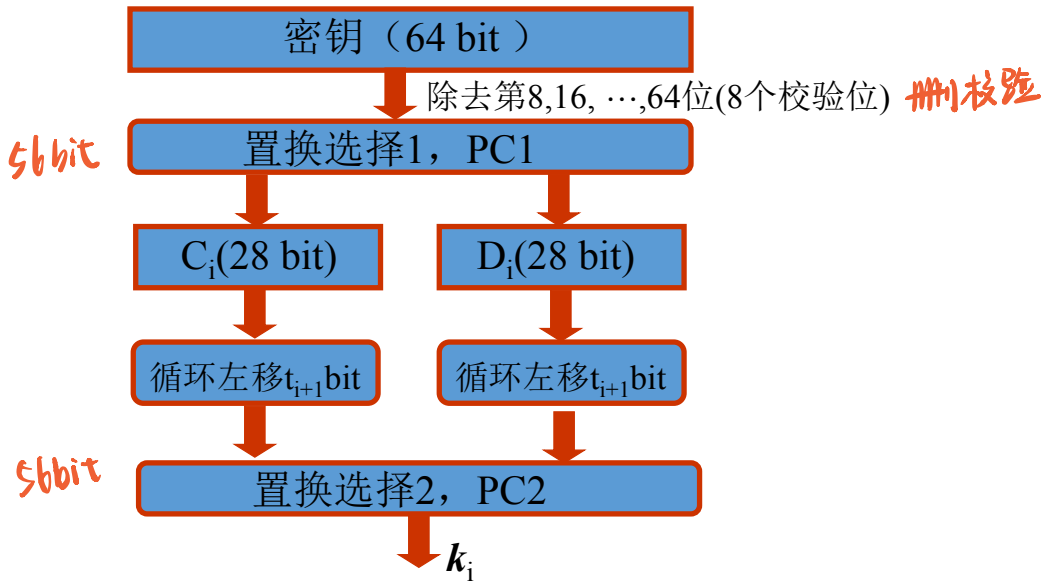
A diagram illustrating the components of the DES algorithm. It features two white circles connected by a vertical line. The top circle is connected to a blue horizontal bar containing the text 'DES的轮函数'. The bottom circle is connected to another blue horizontal bar containing the text 'DES的密钥编排'. Both circles have short lines extending from their top and bottom, suggesting they are part of a larger flow or structure.

DES的轮函数

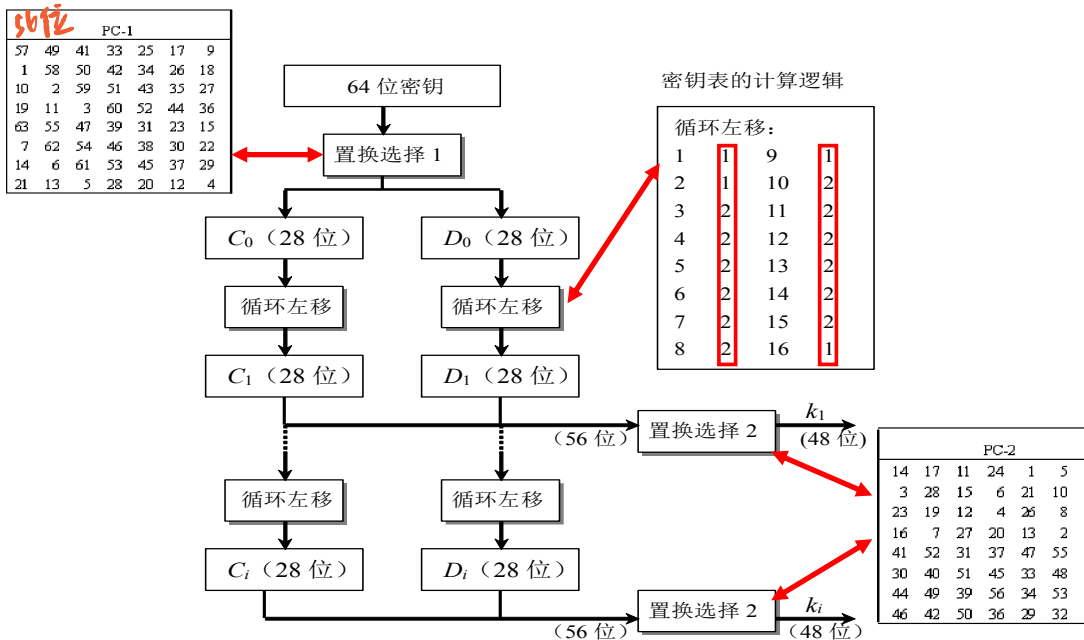
DES的密钥编排

---

# DES密钥编排



# DES中的子密钥的生成



# DES算法密钥编排中使用的表

PC-1							
57	49	41	33	25	17	9	
1	58	50	42	34	26	18	
10	2	59	51	43	35	27	
19	11	3	60	52	44	36	
63	55	47	39	31	23	15	
7	62	54	46	38	30	22	
14	6	61	53	45	37	29	
21	13	5	28	20	12	4	

PC-2						
14	17	11	24	1	5	
3	28	15	6	21	10	
23	19	12	4	26	8	
16	7	27	20	13	2	
41	52	31	37	47	55	
30	40	51	45	33	48	
44	49	39	56	34	53	
46	42	50	36	29	32	

△ 每轮移位次数  
并不完全一样

移位次数表																
第 <i>i</i> 次迭代	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
循环左移次数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1



感谢聆听!

xynie@uestc.edu.cn