现代密码学

第二十一讲 DES的轮函数及密钥编排

信息与软件工程学院

第二十一讲 DES的轮函数及密钥编排

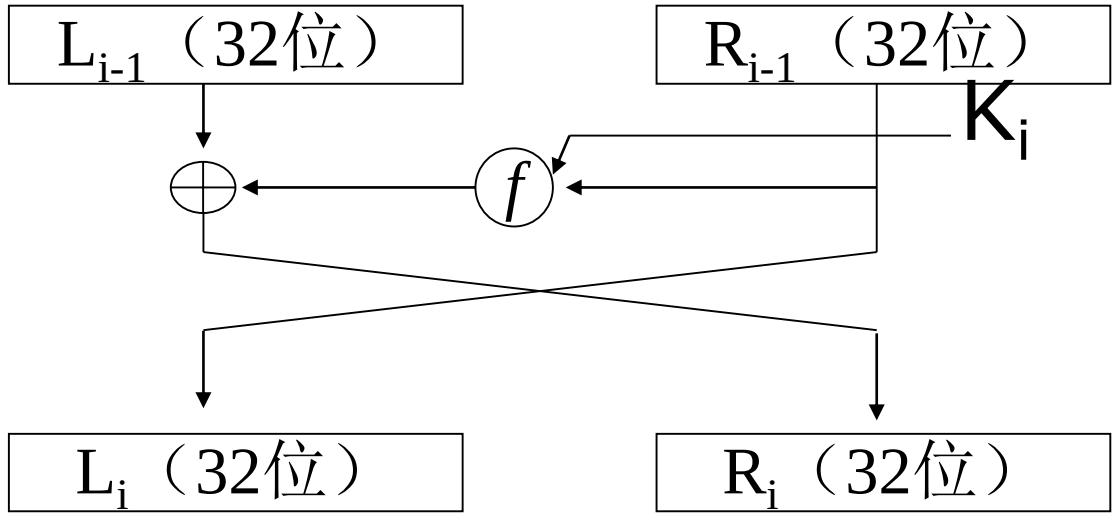
- DES的轮函数
- DES的密钥编排

DES的轮函数的结构

设输入为（x, y）

则DES的轮函数输出为：

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



它等价于两个对合变换的复合：

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

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

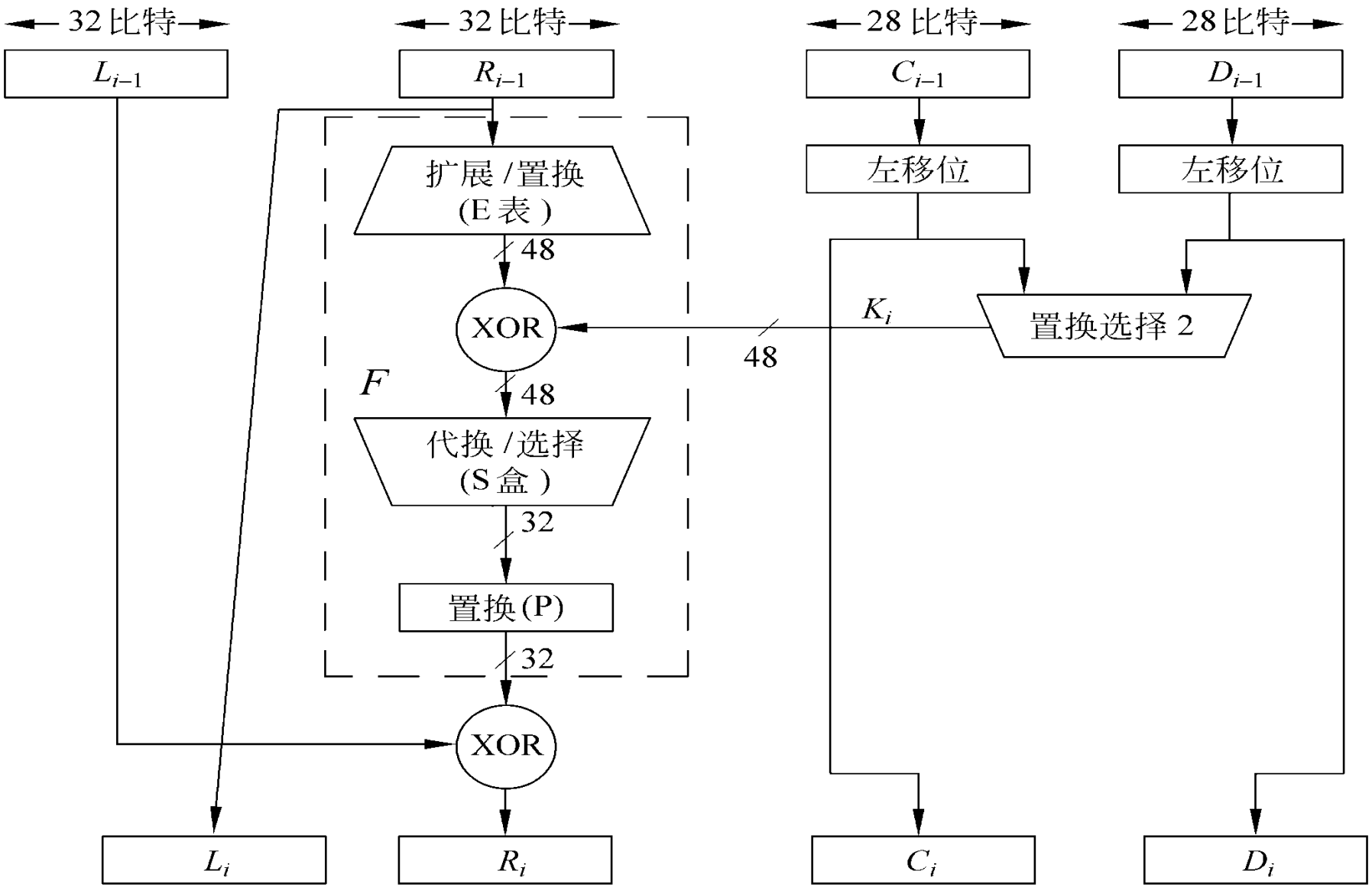
注意

- 无论f函数如何选取，DES的轮函数是一个对合变换。

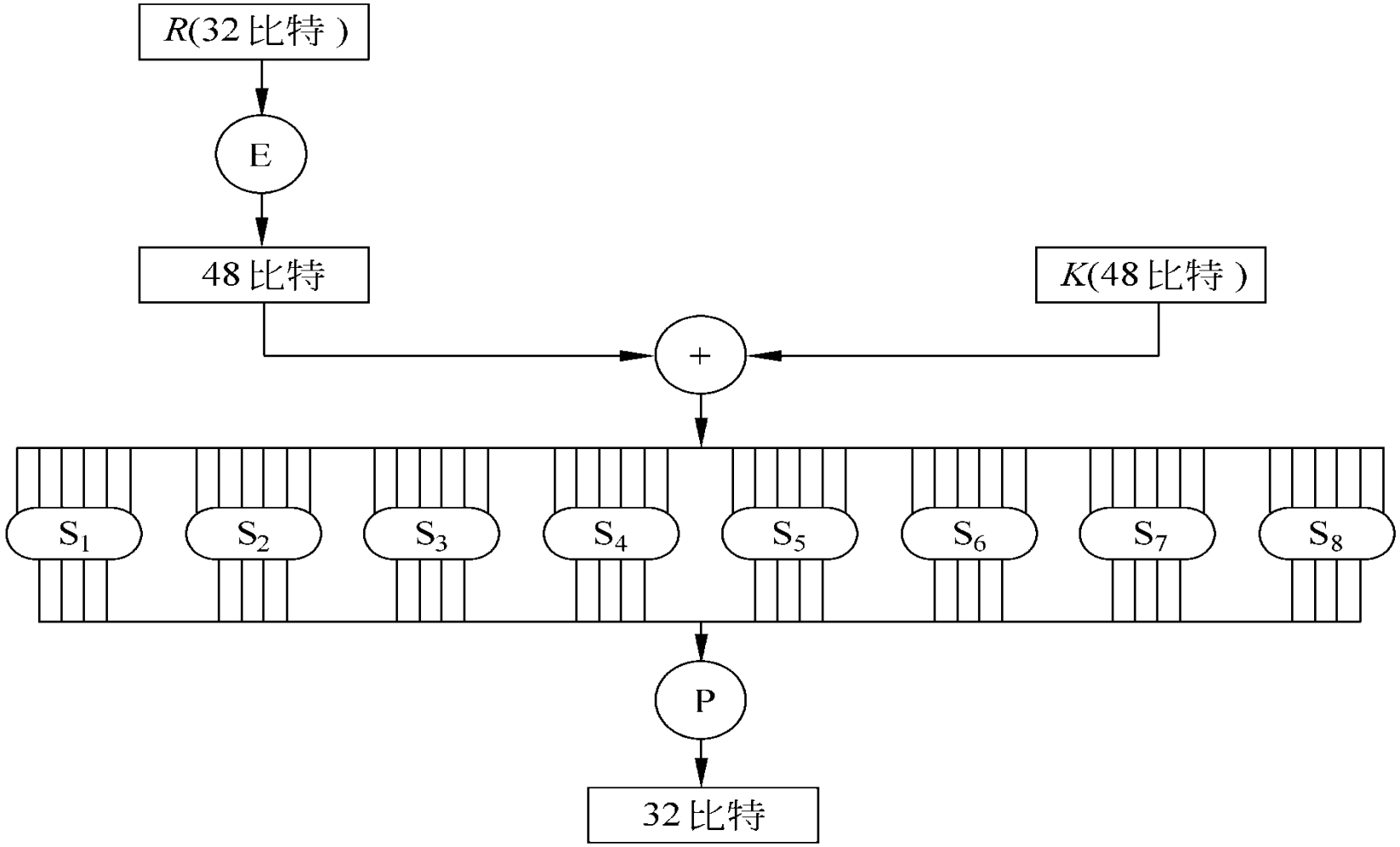
$$F(x,y)=(x\oplus f(k,y),y)$$

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

DES算法轮结构


32 比特
32 比特
28 比特
28 比特
L_{i-1}
R_{i-1}
C_{i-1}
D_{i-1}
扩展 /置换
(E 表)
左移位
左移位
48
XOR
K_i
48
置换选择 2
F
48
代换 /选择
(S 盒)
32
置换(P)
32
XOR
L_i
R_i
C_i
D_i

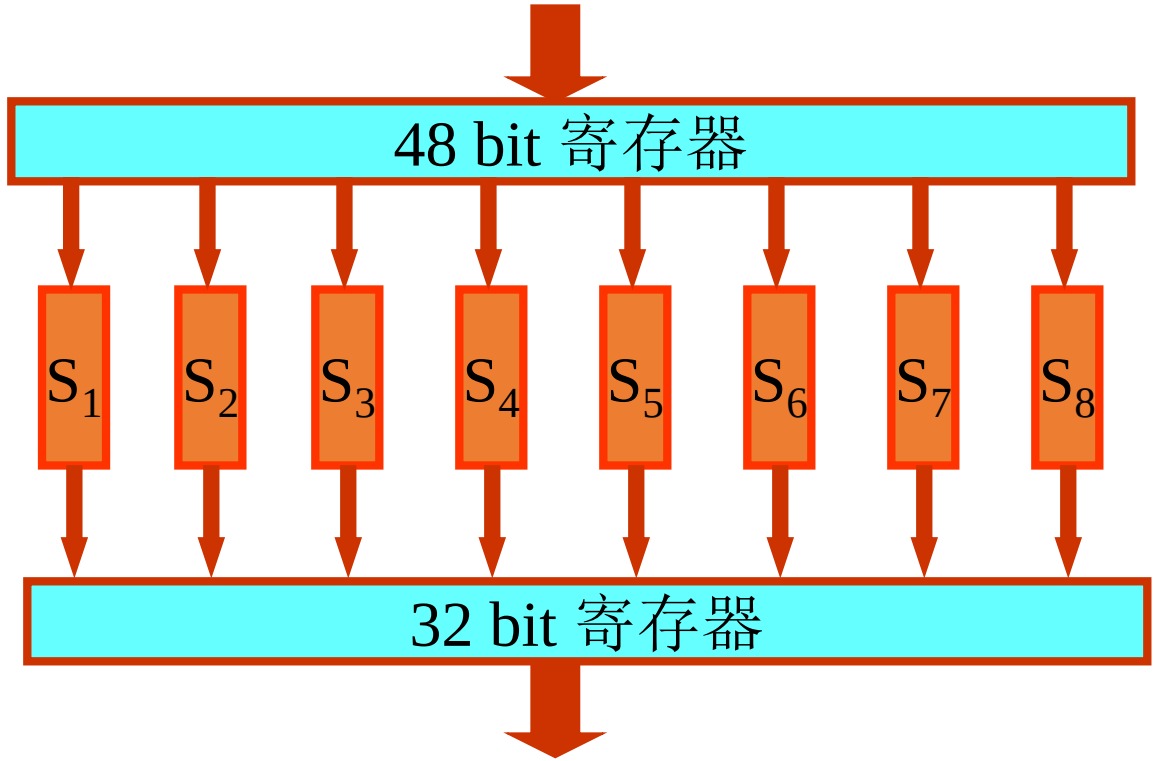
函数f(R,K)的计算过程



选择扩展运算E

32	1	2	3	4	**5**
4	5	6	7	8	**9**
8	9	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	30	31	32	**1**

选择压缩运算S



DES的S盒

	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	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S_1
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	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S_2
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	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	S_3
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

x_5 x_0

1 0

x_5 x_4 x_3 x_2 x_1 x_0

1 0 1 1 0 0

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

行号 \ 列号	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
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

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。

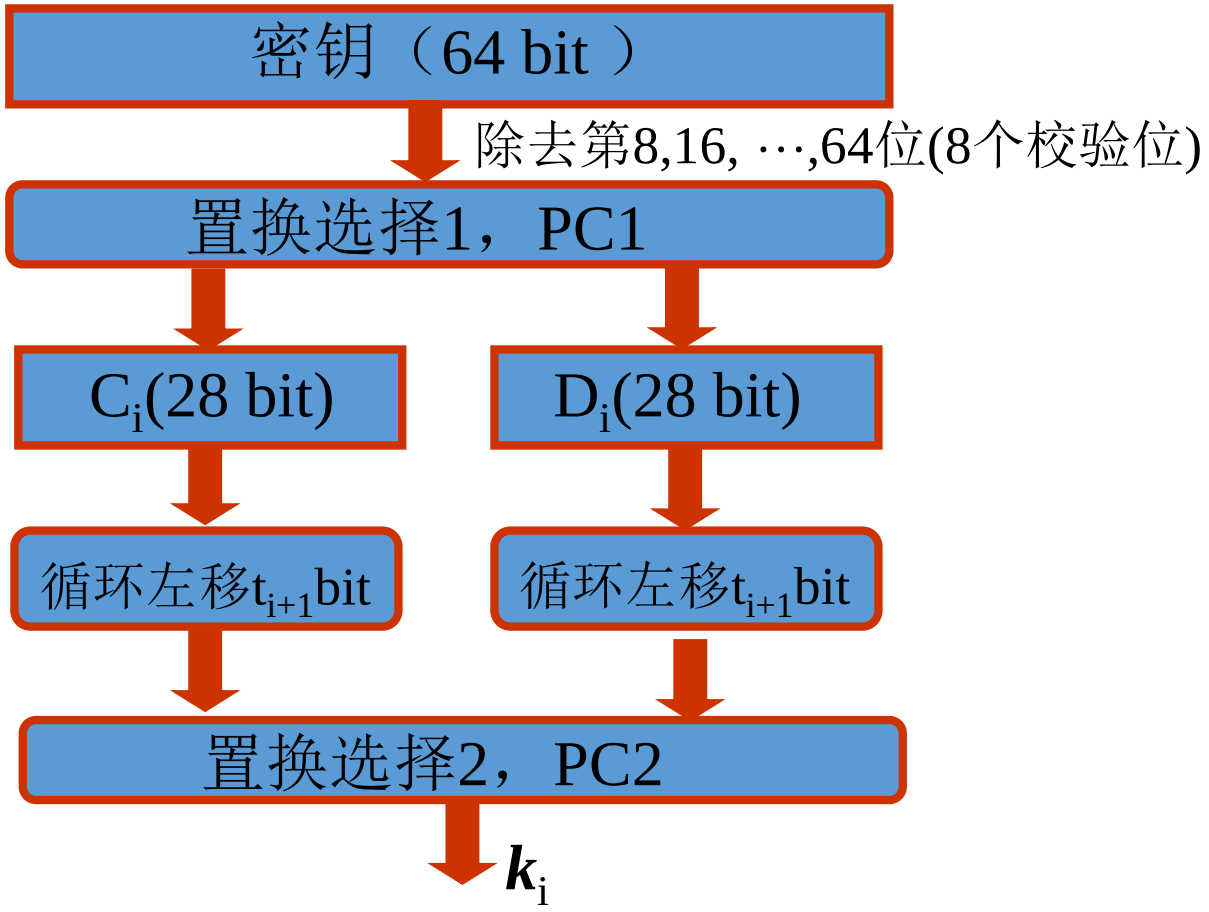
P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

含义:P盒输出的第1个元是输入的第16个元。

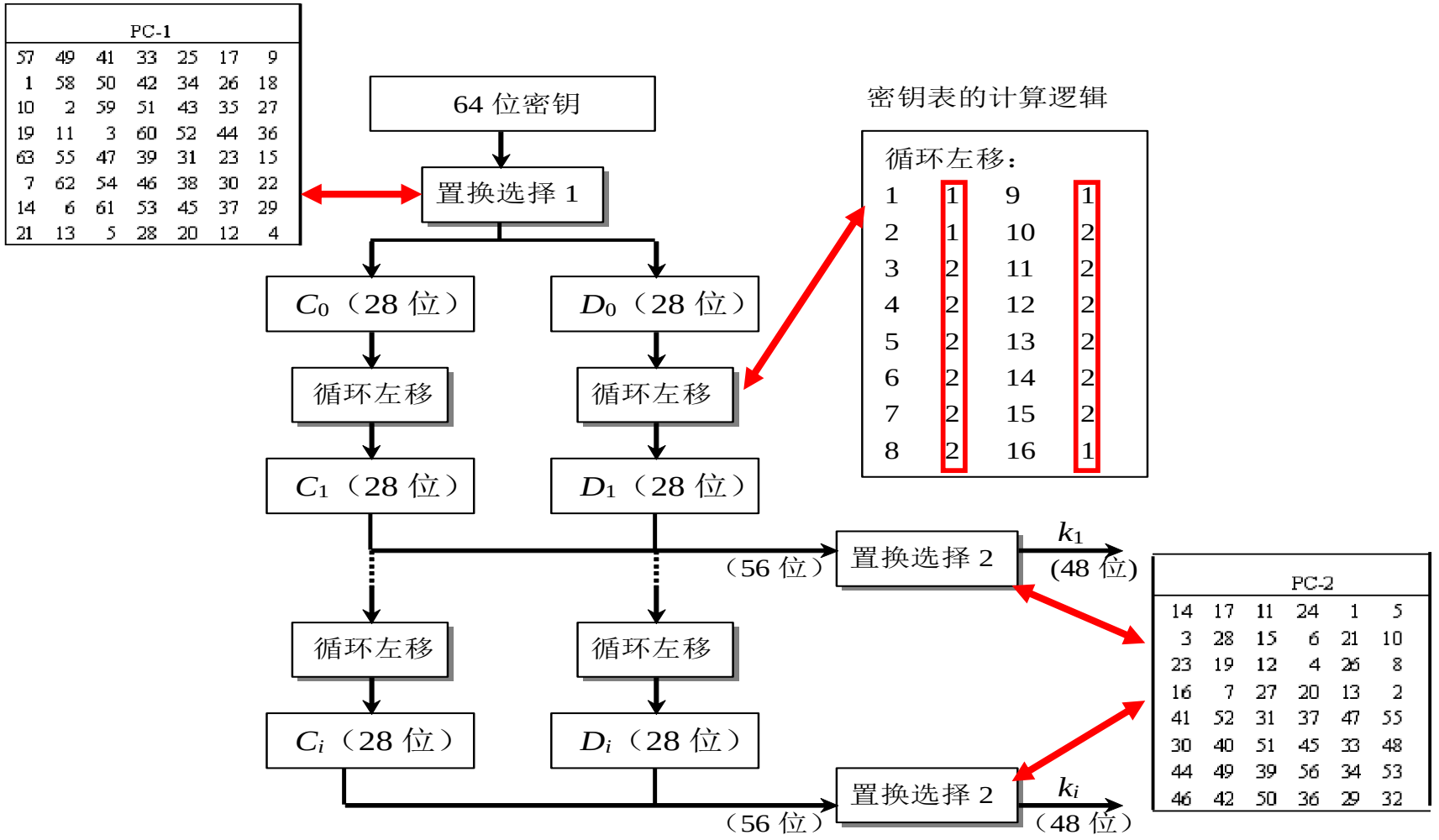
第二十一讲 DES的轮函数及密钥编排

- DES的轮函数
- DES的密钥编排

DES密钥编排


密钥（64 bit）
除去第8,16, …,64位(8个校验位)
置换选择1，PC1
C_i(28 bit)
D_i(28 bit)
循环左移t_{i+1}bit
循环左移t_{i+1}bit
置换选择2，PC2
k_i

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

移位次数表

第*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