密 码 学

第三讲

（*数据加密标准DES*）

张焕国

武汉大学计算机学院

目　录

目　录

一、DES的概况

1、重要时间：

- *1973年美国国家标准局（NBS）向社会公开征集加密算法，以制定加密算法标准；*
- *1974年第二次征集；*
- *1975年选中IBM的算法，公布征求意见；*
- *1977年1月15日正式颁布；*
- *1998年底以后停用。*
- *1999年颁布3DES为新标准。*

一、DES的概况

2、标准加密算法的目标

①*用于加密保护政府机构和商业部门的非机密的敏感数据。*

②*用于加密保护静态存储和传输信道中的数据。*

③*安全使用**10~15年**。*

一、DES的概况

3、整体特点

①分组密码:明文、密文和密钥的分组长度都是64位。

②面向二进制的密码算法:因而能够加解密任何形式的计算机数据。

③对合运算:因而加密和解密共用同一算法，使工程实现的工作量减半。

④综合运用了置换、代替、代数等多种密码技术。

一、DES的概况

4、应用

①*许多国际组织采用为标准。*

②*在全世界范围得到广泛应用。*

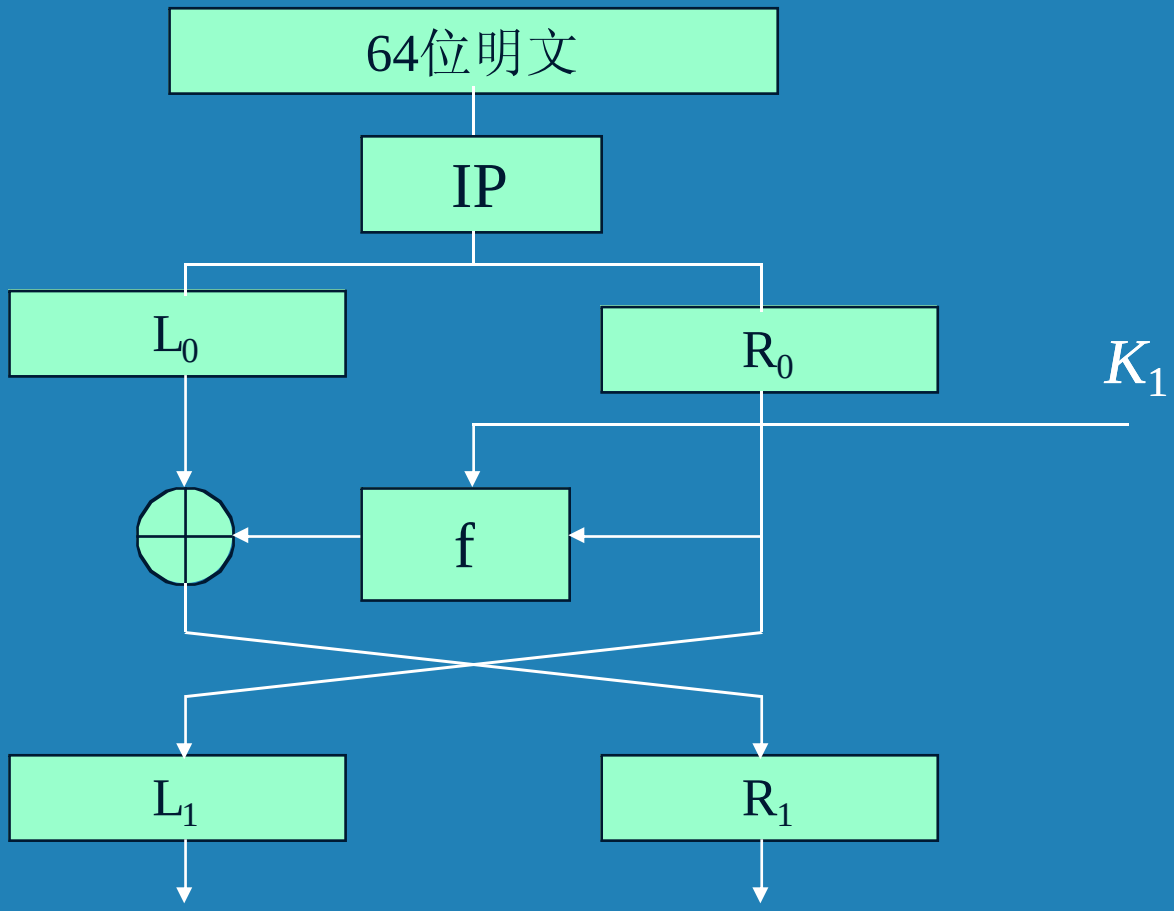
③*产品形式：软件（嵌入式，应用软件）*

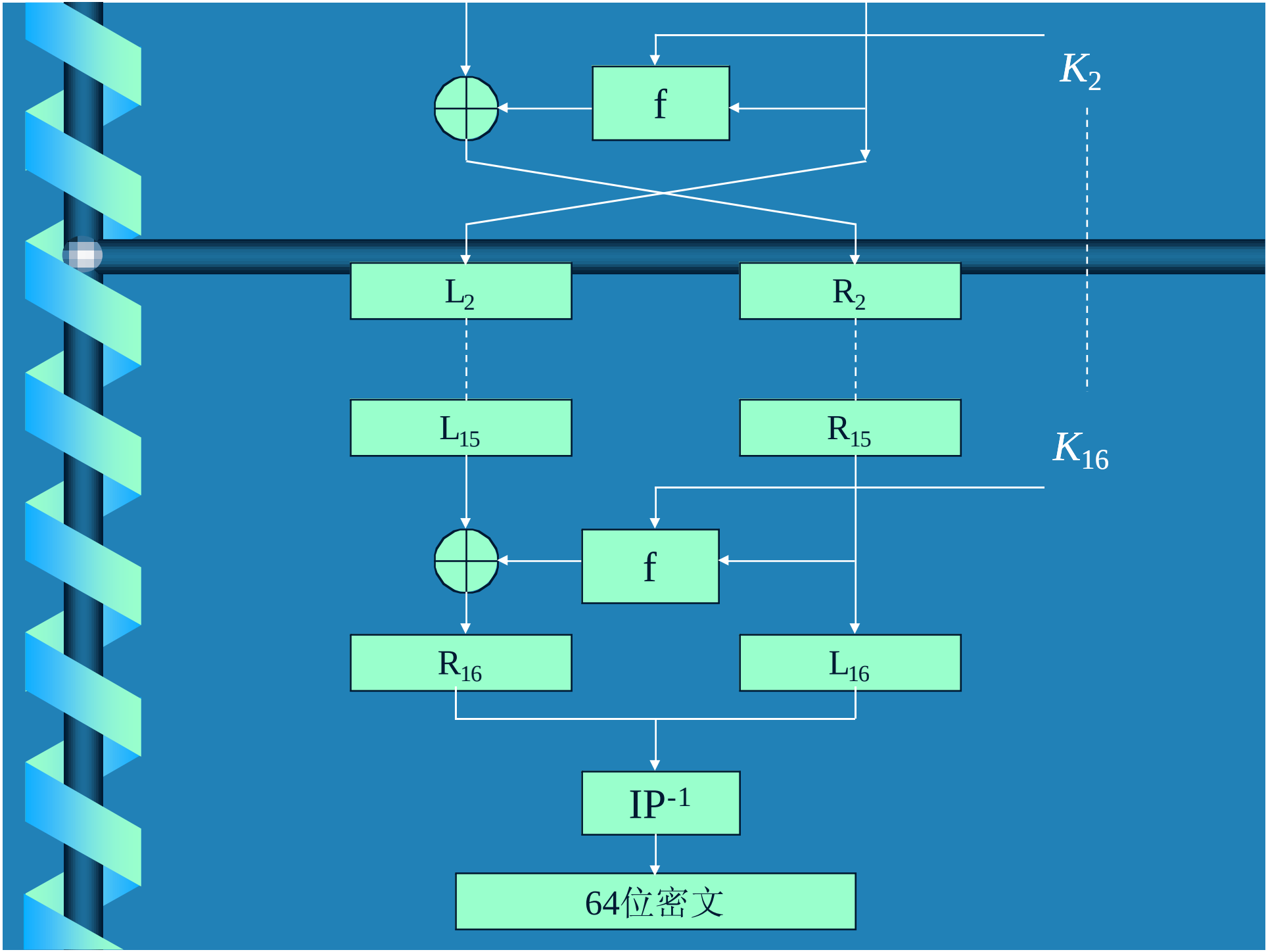
硬件（芯片，插卡）

5、结论

- *用于其设计目标是安全的。*
- *设计精巧、实现容易、使用方便，堪称典范。*

二、算法总框图




f
K_2
L_2
R_2
L_{15}
R_{15}
K_{16}
f
R_{16}
L_{16}
IP^{-1}
64位密文

三、加密过程

1、64位密钥经子密钥产生算法产生出16个子密钥：K_1，K_2，...，K_{16}，分别供第一次，第二次，...，第十六次加密迭代使用。

2、64位明文经初始置换IP，将数据打乱重排并分成左右两半。左边为L_0，右边为R_0。

3、第一次加密迭代：

在子密钥K_1的控制下，由加密函数f对R_0加密：

$$L_0 \oplus f(R_0, K_1)$$

以此作为第二次加密迭代的R_1，以R_0作为第二次加密迭代的L_1。

三、加密过程

4、第二次加密迭代至第十六次加密迭代分别用子密钥K_2，...，K_{16}进行，其过程与第一次加密迭代相同。

5、第十六次加密迭代结束后，产生一个64位的数据组。以其左边32位作为R_{16}，以其右边32位作为L_{16}。

6、 L_{16}与R_{16}合并，再经过逆初始置换IP^{-1}，将数据重新排列，便得到64位密文。

7、DES加密过程的数学描述：

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \\ i = 1,2,3,\ldots 16 \end{cases}$$

四、子密钥的产生

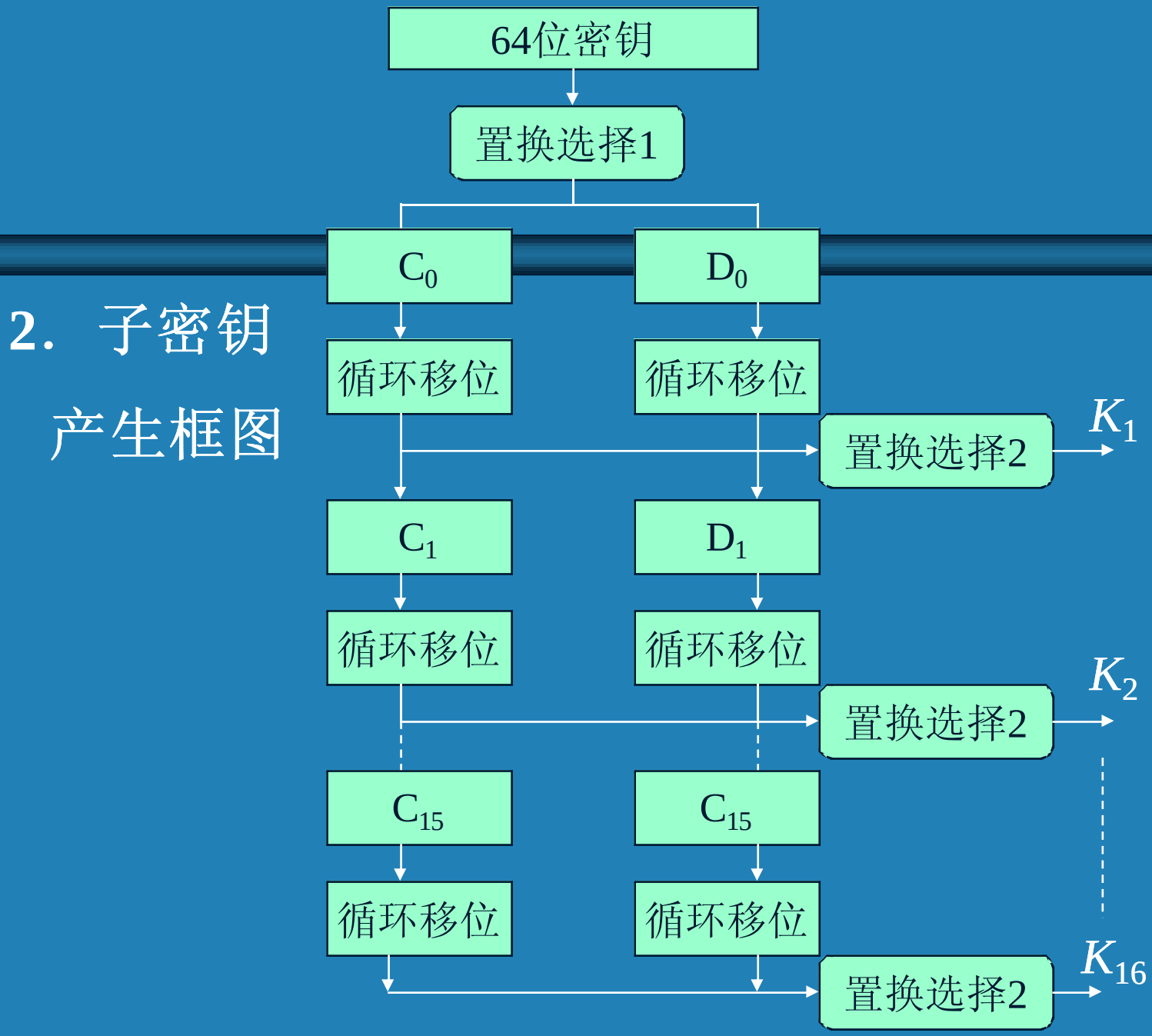
1、功能：

64位密钥经过置换选择1、循环左移、置换选择2等变换，产生16个子密钥

K_1，K_2，…K_{16}，

分别供各次加密迭代使用。

2. 子密钥产生框图


64位密钥
置换选择1
C_0
D_0
循环移位
循环移位
置换选择2
K_1
C_1
D_1
循环移位
循环移位
置换选择2
K_2
C_{15}
C_{15}
循环移位
循环移位
置换选择2
K_{16}

3、置换选择1：

①、*作用*

- *去掉密钥中的8个奇偶校验位。*
- *打乱重排，形成C_0（左28位），D_0（右28位）。*

②、*矩阵* C_0 D_0

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

4、循环移位：

①、*作用*

- *对C_0，D_0分别循环移位。*

②、*循环移位表*

迭代次数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
移位次数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

5、置换选择2：

①、*作用*

- *从C_i和D_i（56位）中选择出一个48位的子密钥K_i。*

②、*矩阵*

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

五、初始置换IP

①、作用

- 把64位明文打乱重排。
- 左一半为L_0（左32位），右一半为R_0（右32位）。
- 例：把输入的第1位置换到第40位，把输入的第58位置换到第1位。

五、初始置换IP

②、*矩阵*

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

六、逆初始置换IP^{-1}

①、*作用*

- *把64位中间密文打乱重排。*
- *形成最终的64位密文。*

②、*相逆性*

- *IP与IP^{-1}互逆。*
- *例：在IP中把输入的第1位置换到第40位，而在IP^{-1}中把输入的第40位置换到第1位。*

六、逆初始置换IP^{-1}

③、*矩阵*

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

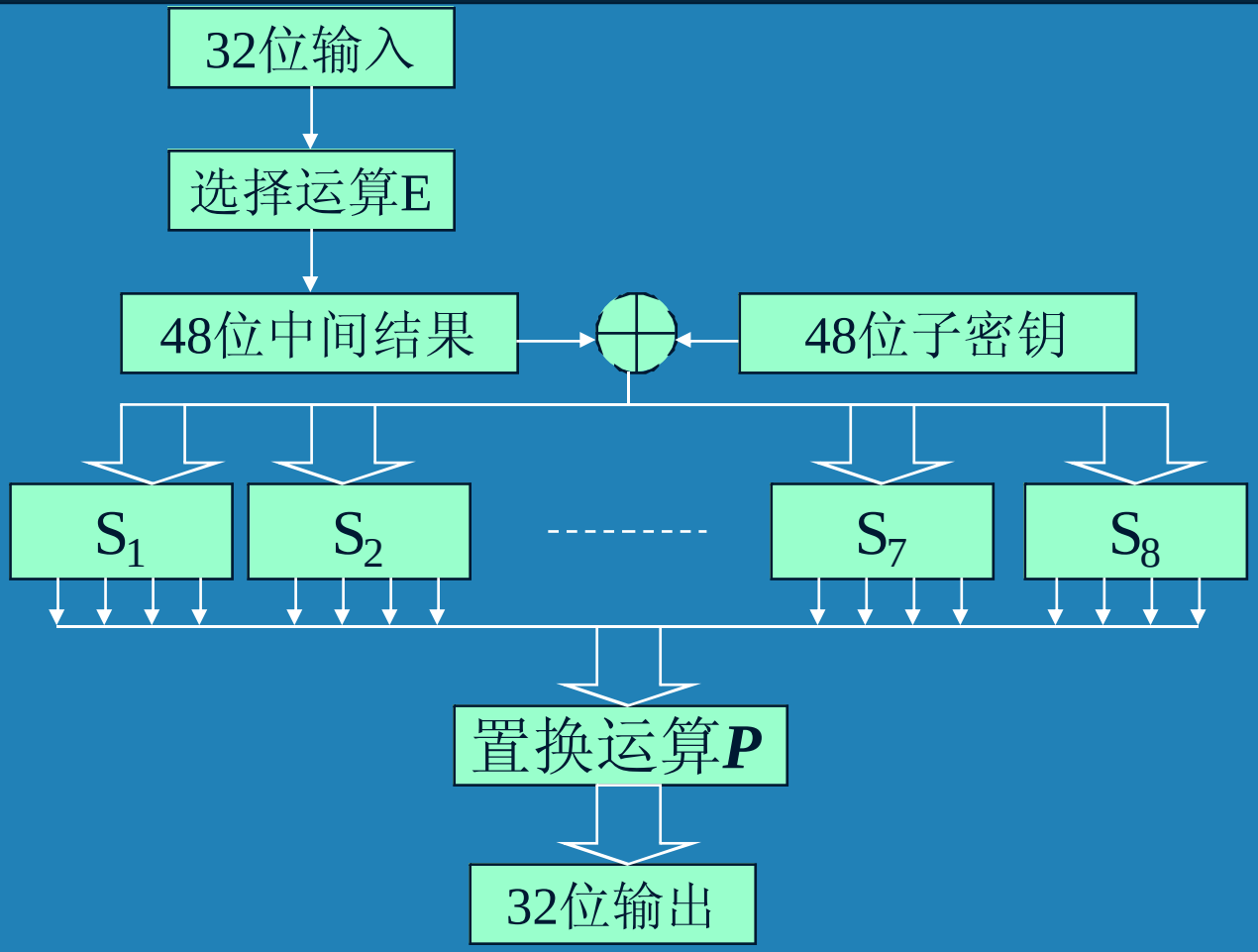
七、加密函数f

①作用

- *DES的核心。*
- *加密数据。*
- *数据处理宽度32位。*

七、加密函数f

②框图



七、加密函数f

③选择运算E

- *把32位输入扩充为48位中间数据；*
- *重复使用数据实现扩充。*
- 矩阵：

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

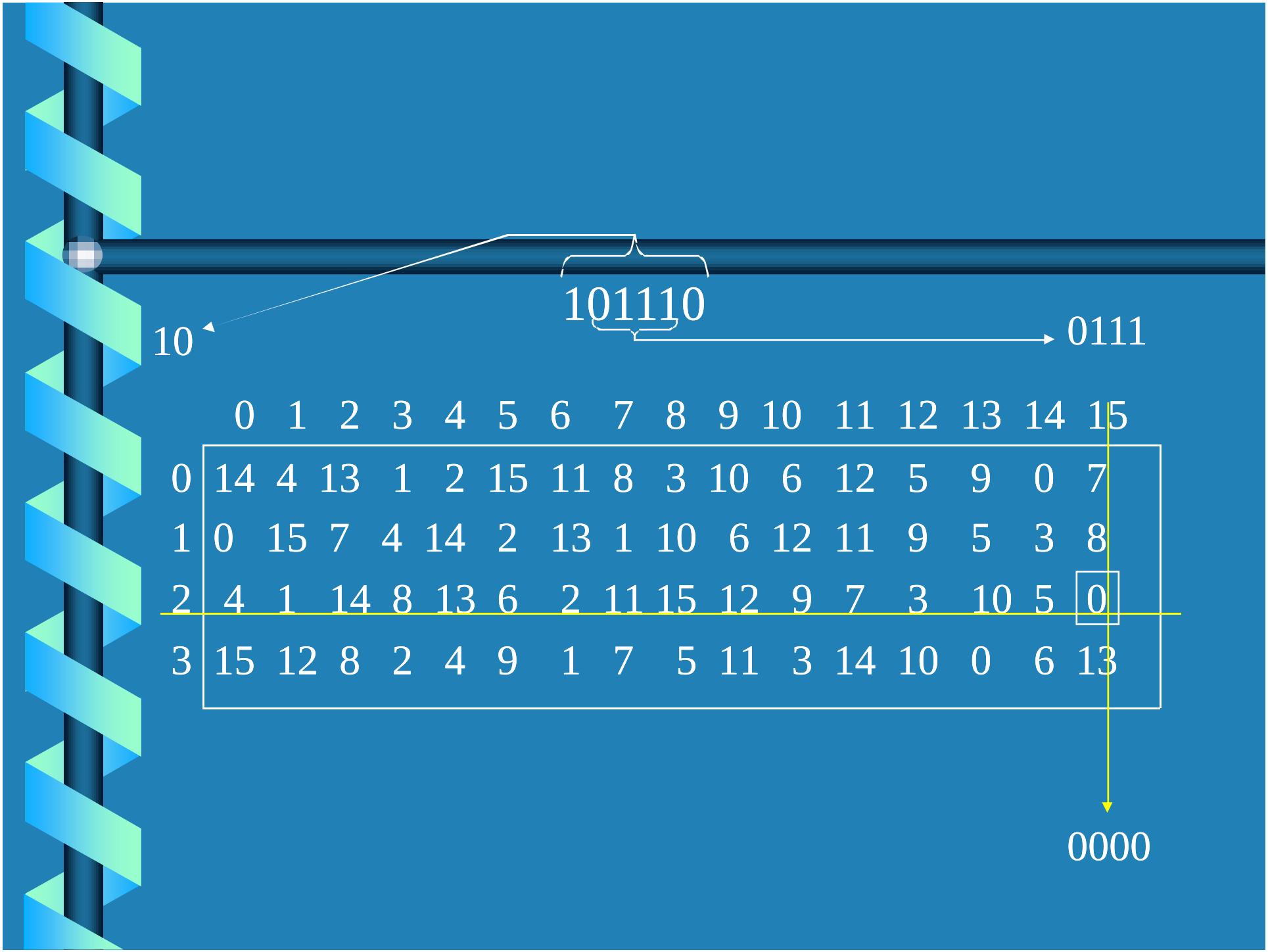
七、加密函数f

④选择替换S（S盒）

- *S盒是DES唯一的非线性变换。*
- *S盒是DES安全的关键。*
- *共有8个S盒。*
- *每个S盒有6个输入，4个输出，是一种非线性压缩变换。*
- *设输入为$b_1b_2b_3b_4b_5b_6$,则以b_1b_6组成的二进制数为行号，$b_2b_3b_4b_5$组成的二进制数为列号。行列交点处的数（二进制）为输出。*

S_1

	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	3	14	10	0	6	13


101110
10
0111
0000
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 3 14 10 0 6 13

七、加密函数f

⑤置换运算P

- *把数据打乱重排。*
- 矩阵：

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

八、DES的解密过程

- **DES**的运算是对和运算，解密和加密可共用同一个运算。
- 不同点：子密钥使用的顺序不同。
- 第一次解密迭代使用子密钥 K_{16}，第二次解密迭代使用子密钥 K_{15}，第十六次解密迭代使用子密钥K_1。

八、DES的解密过程

- ***DES解密过程的数学描述：***

$$\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus f(L_i, K_i) \\ i = 16,15,14, \ldots, 1 \end{cases}$$

九、DES的对和性证明

1、可逆性证明

①定义 T是把64位数据的左右两半交换位置：

$$T（L，R）＝（R，L）$$

- 因为，T^2 （L，R）＝（L，R）＝**I**，

其中**I**为恒等变换，于是，

$$T = T^{-1}，$$

所以 **T** 变换是对合运算。

九、DES的对和性证明

1、可逆性证明

②记DES第 i 轮中的主要运算为，即

$$F_i\ (L_{i-1},\ R_{i-1}) = (L_{i-1} \oplus f\ (R_{i-1}, K_i),\ R_{i-1})$$

- $$F_i^2 = F_i\ (L_{i-1} \oplus f\ (R_{i-1}, K_i),\ R_{i-1})$$

$$= (L_{i-1} \oplus f\ (R_{i-1}, K_i) \oplus f\ (R_{i-1}, K_i),\ R_{i-1})$$

$$= (L_{i-1},\ R_{i-1})$$

$$= I$$

所以，$F_i = F_i^{-1}$ 。

- 所以 $\mathbf{F_i}$变换也是对合运算。

九、DES的对和性证明

1、可逆性证明

③结合①、②，便构成DES的轮运算

$$H_i = F_i T$$

- *因为*（$F_i T$）（TF_i）=（F_i（TT）F_i）=$F_i F_i = I$，
- 所以

$$(F_i T)^{-1} = (TF_i)$$

$$(F_i T) = (TF_i)^{-1}$$

九、DES的对和性证明

1、可逆性证明

④加解密表示

(1) $DES(M) = IP^{-1}(F_{16})(TF_{15})\ldots(TF_2)(TF_1)IP$（M）＝C

(2) $DES^{-1}(C) = IP^{-1}(F_1)(TF_2)(TF_3)\ldots(TF_{15})(TF_{16})IP$（C）

- *把(1) 式代入(2)式可证：*

  $DES^{-1}(DES(M)) = M$

- 所以，DES是可逆的。

九、DES的对和性证明

2、对合性证明

$$DES = IP^{-1}(F_{16})\ (TF_{15})\ (TF_{14})\ldots(TF_3)\ (TF_2)\ (TF_1)IP$$

$$DES^{-1} = IP^{-1}(F_1)\ (TF_2)\ (TF_3)\ldots(TF_{14})\ (TF_{15})\ (TF_{16})IP$$

DES和DES^{-1} 除了子密钥的使用顺序相反之外是相同的，

所以DES的运算是对合运算。

十、DES的安全性

①攻击

- 穷举攻击。目前最有效的方法。
- 差分攻击。
- 线性攻击。

②安全弱点

- 密钥太短。
- 存在弱密钥。
- 存在互补对称性。

十一、3重DES

①美国NIST在1999年发布了一个新版本的DES标准（FIPS PUB46-3）：

- DES只用于遗留系统。
- 3DES将取代DES成为新的标准。
- 国际组织和我国银行都接受3DES。

十一、3重DES

② 3DES的优势：

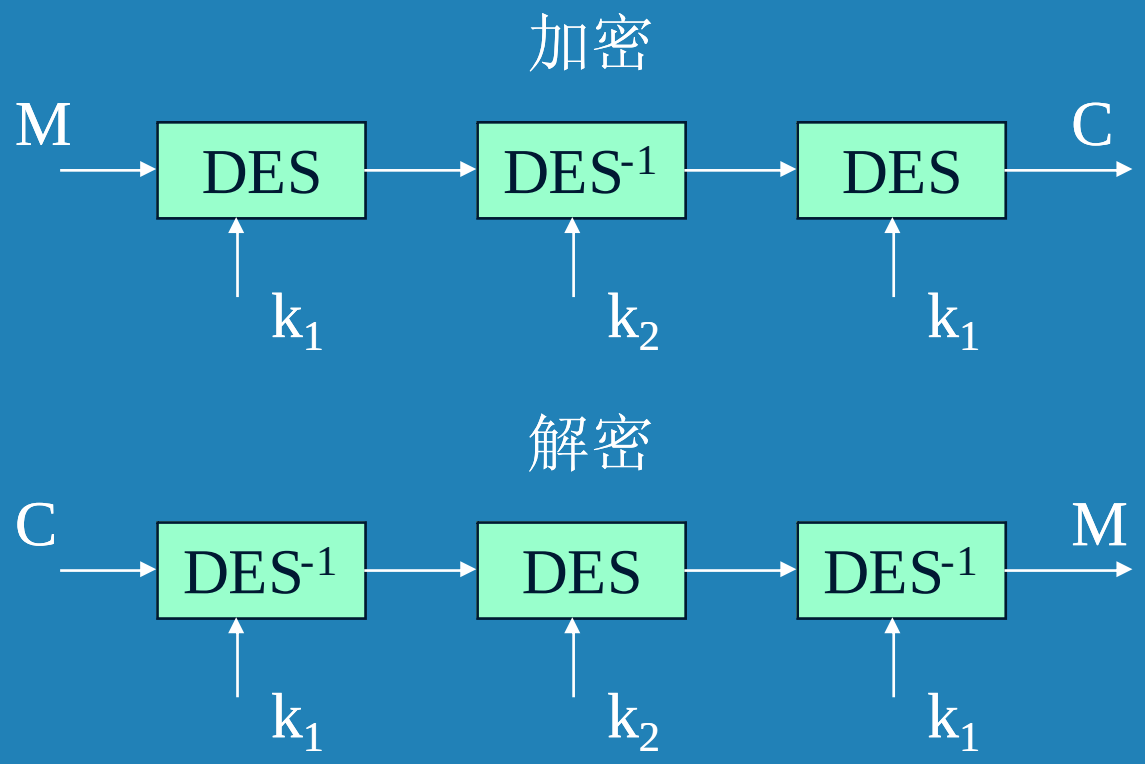
- 3密钥的3DES：密钥长度是168位。
- 2密钥的3DES：密钥长度是112位。
- 安全：密钥足够长；
  经过最充分的分析和实践检验。
- 兼容性好。

③ 3DES的弱势：

- 速度慢。

十一、3重DES

④2密钥3DES框图



十一、DES的历史回顾

- *DES的体现*
  - *DES的出现标志着商业密码需求的增加。*
  - *DES体现商农的密码设计理论。*
  - *体现了公开设计原则，开创公开算法的先例。*
  - *DES代表当时商业密码的最高水平。*
- *DES给我们的启示*
  - *商业密码应当坚持公开设计原则；*
  - *商业密码标准应当公布算法。*

大作业1

以3DES作为加密算法开发出文件加密软件系统：

- *具有文件加密和解密功能；*
- *具有加解密速度统计功能；*
- *采用密文反馈链接和密文挪用短块处理技术；*
- *具有较好的人机界面。*

复习题

1、分析DES的弱密钥。

2、证明DES具有互补对称性。

3、画出3密钥3DES的框图。