#### **DES补充材料**

初始置换(IP)

最终置换 (IP-1)

扩张函数 (E函数)

P置接

选择置换1(PC-1)

选择置换2(PC-2)

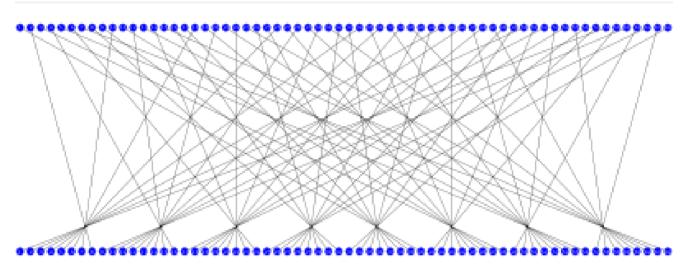
置换盒 (S盒)

密钥调度过程中的移位

# DES补充材料

本文档中的数据都是以大端序排列的,也即首位为MSB。

#### 初始置换(IP)

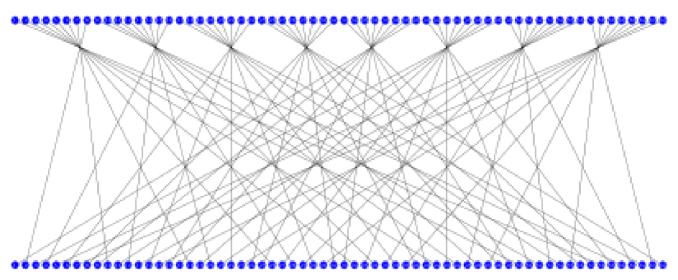


58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

该表显示了对64位块的初始置换,其意义如下:输出的首位为输入的第58位,第二位为50位,依此类推,输出的最后位为输入的第7位。

以上信息为了方便表示被写成表格形式,但它实际上是一个矢量(一维的就足够表示了),而非矩阵。

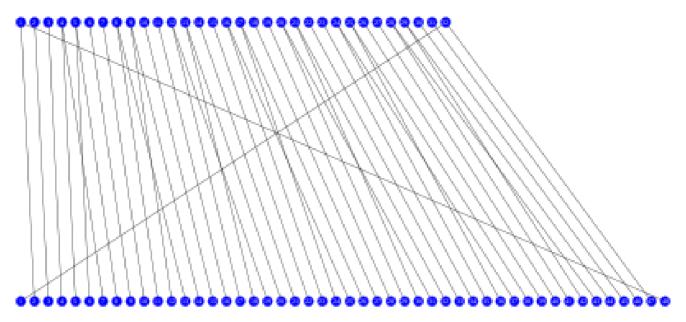
#### 最终置换 (IP-1)



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

IP-1(亦被称为FP)是IP的逆过程,上表的含义与IP的相似。

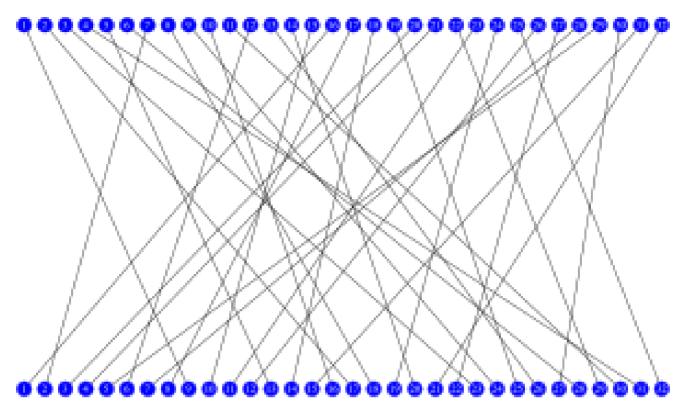
#### 扩张函数 (E函数)



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

扩张函数被作为最初和最终的置换。输入中的**某些位在输出中被用到了不止一次**,因此32位的半块输入被**扩张**到了48位。

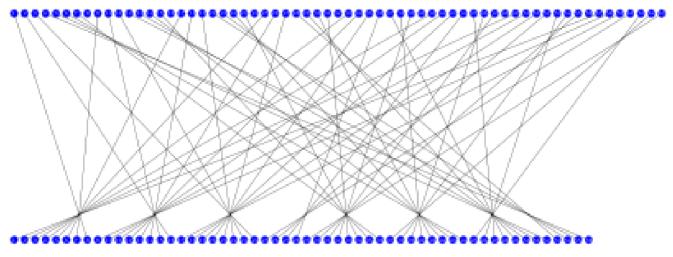
## P置换



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

P置换将32位的半块数据重新排列。

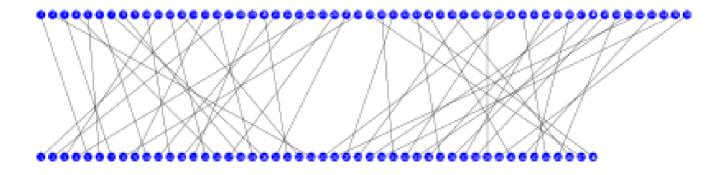
# 选择置换1(PC-1)



左						
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
右						
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

上表的"左"和"右"两部分表现了输入密钥组成密钥调度状态中左右两部分的过程。主要输入的64位数据中只用到了56位,剩余的8位可以用于奇偶校验。

## 选择置换2(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

该置换从56位的密钥调度状态中取出48位的子密钥。

# 置换盒 (S盒)

S盒

								s <sub>1</sub>								
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
ОууууО	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0уууу1	L 0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	) 4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
<b>1</b> yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
								S <sub>2</sub>								
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
ОууууО	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0уууу1	. 3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
<b>1</b> yyyy0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1уууу1	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
					1		ı	S <sub>3</sub>								
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
ОууууО	10			14	6	3	15	5	1	13	12	7	11	4	2	8
0уууу1				9	3	4	6	10	2	8	5	14	12	11	15	1
1уууу0			4	9	8	15	3	0	11	1	2	12	5	10	14	7
<b>1</b> yyyy1	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	$S_4$															
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111
0уууу0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	. 4	1
0уууу1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	
1уууу0	10	6	9	0	12	11	7	13	15	1	3	14	5	2	. 8	
1уууу1	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	1
								S <sub>5</sub>								
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111
0уууу0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	. !
0уууу1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	
1уууу0	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1уууу1	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	;
			$s_{6}$													
	x0000x							56				1	1			
0уууу0		x0001x	x0010x		x0100x		x0110x	_	x1000x		x1010x		x1100x			
		1	10	15	9	2	6	<b>x0111</b> x	0	13	3	4	14	7	5	1
0уууу1	10	1 15	10	15 2	9	2	6	<b>x0111x</b> 8 5	0	13	3 13	4	14	7	5	1:
0yyyy1 1yyyy0	10	1 15 14	10 4 15	15 2 5	9 7 2	2 12 8	6 9 12	<b>x0111x</b> 8 5	0 6 7	13 1 0	3 13 4	4 14 10	14 0 1	7 11 13	5 3	1
0уууу1	10	1 15	10	15 2	9	2	6	<b>x0111x</b> 8 5	0	13	3 13 4	4 14 10	14 0 1	7 11 13	5 3	1:
0yyyy1 1yyyy0	10	1 15 14	10 4 15	15 2 5	9 7 2	2 12 8	6 9 12	x0111x 8 5 3	0 6 7	13 1 0	3 13 4	4 14 10	14 0 1	7 11 13	5 3	1
0yyyy1 1yyyy0	10 9 4	1 15 14 3	10 4 15 2	15 2 5 12	9 7 2 9	2 12 8 5	6 9 12 15	x0111x 8 5 3 10	0 6 7 11	13 1 0 14	3 13 4 1	4 14 10 7	14 0 1 6	7 11 13 0	5 3 11 8 8	1:
0yyyy1 1yyyy0 1yyyy1	10 9 4 x0000x	1 15 14 3 x0001x	10 4 15 2 <b>x0010x</b>	15 2 5 12 <b>x0011x</b>	9 7 2 9 x0100x	2 12 8 5 <b>x0101x</b>	6 9 12 15	x0111x	0 6 7 11 <b>x1000</b> x	13 1 0 14 <b>x1001</b> x	3 13 4 1	4 14 10 7 <b>x1011</b> x	14 0 1 6 <b>x1100</b> x	7 11 13 0 <b>x1101x</b>	5 3 11 8 x1110x	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
0yyyy1 1yyyy0 1yyyy1 0yyyy0	10 9 4 x0000x 4	1 15 14 3 x0001x 11	10 4 15 2 <b>x0010x</b> 2	15 2 5 12 <b>x0011x</b> 14	9 7 2 9 x0100x 15	2 12 8 5 5 <b>x0101x</b> 0	6 9 12 15 <b>x0110x</b> 8	x0111x 8 5 3 10 S <sub>7</sub> x0111x	0 6 7 11 <b>x1000x</b> 3	13 1 0 14 <b>x1001x</b> 12	3 13 4 1 1 <b>x1010x</b> 9	4 14 10 7 x1011x 7	14 0 1 6 <b>x1100x</b> 5	7 11 13 0 0 x1101x 10	5 3 11 8 <b>x1110x</b> 6	11:
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1	10 9 4 x0000x 4 13	1 15 14 3 x0001x 11 0	10 4 15 2 <b>x0010x</b> 2 11	15 2 5 12 <b>x0011x</b> 14 7	9 7 2 9 <b>x0100x</b> 15 4	2 12 8 5 5 <b>x0101x</b> 0 9	6 9 12 15 <b>x0110x</b> 8 1	x0111x	0 6 7 11 <b>x1000x</b> 3 14	13 1 0 14  x1001x 12 3	3 13 4 1 1 <b>x1010x</b> 9	4 14 10 7 x1011x 7 12	14 0 1 6 <b>x1100x</b> 5 2	7 11 13 0 0 x1101x 10 15	5 3 3 111 8 x1110x 6 8	1 1 x1111x 1 1 6
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1 1yyyy0	x0000x 4 13 1	1 15 14 3 x0001x 11 0 4	10 4 15 2  x0010x 2 11 11	15 2 5 12 <b>x0011x</b> 14 7	9 7 2 9 <b>x0100x</b> 15 4 12	2 12 8 5 5 <b>x0101x</b> 0 9 3	6 9 12 15 x0110x 8 1 7	x0111x	0 6 7 11 <b>x1000x</b> 3 14	13 1 0 14 x1001x 12 3 15	3 13 4 1 1 x1010x 9 5 6	x1011x 7 12 8	14 0 1 6 <b>x1100x</b> 5 2	7 11 13 0 0 x1101x 10 15 5	x1110x 6 8	1 1 x1111x 1 1 6 2
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1	10 9 4 x0000x 4 13	1 15 14 3 x0001x 11 0	10 4 15 2 <b>x0010x</b> 2 11	15 2 5 12 <b>x0011x</b> 14 7	9 7 2 9 <b>x0100x</b> 15 4	2 12 8 5 5 <b>x0101x</b> 0 9	6 9 12 15 <b>x0110x</b> 8 1	x0111x	0 6 7 11 <b>x1000x</b> 3 14	13 1 0 14  x1001x 12 3	3 13 4 1 1 <b>x1010x</b> 9	4 14 10 7 x1011x 7 12	14 0 1 6 <b>x1100x</b> 5 2	7 11 13 0 0 x1101x 10 15	5 3 3 111 8 x1110x 6 8	11: 3: 4: 11: 11: 11: 11: 12:
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1 1yyyy0	x0000x 4 13 1 6	1 15 14 3 x0001x 11 0 4 11	10 4 15 2  x0010x 2 11 11 13	15 2 5 12 x0011x 14 7 13 8	9 7 2 9 x0100x 15 4 12 1	2 12 8 5 5 x0101x 0 9 3 4	6 9 12 15 <b>x0110x</b> 8 1 7 10	x0111x     8     5     3     10  S <sub>7</sub> x0111x     13     10  14     7 S <sub>8</sub>	0 6 7 11 <b>x1000x</b> 3 14 10 9	13 1 0 14 <b>x1001x</b> 12 3 15	3 13 4 1 <b>x1010x</b> 9 5 6	4 14 10 7 x1011x 7 12 8 15	14 0 1 6 <b>x1100x</b> 5 2 0	7 11 13 0 0 x1101x 10 15 5 2	x1110x 6 8 9	11. x1111x 11 66 2 12
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1 1yyyy0 1yyyy1	x0000x 4 13 1 6	1 15 14 3 x0001x 11 0 4 11 x0001x	10 4 15 2  x0010x 2 11 11 13	15 2 5 12 x0011x 14 7 13 8	9 7 2 9 x0100x 15 4 12 1 x0100x	2 12 8 5 5 x0101x 0 9 3 4 x0101x	6 9 12 15 x0110x 8 1 7 10 x0110x	x0111x	0 6 7 11 <b>x1000x</b> 3 14 10 9	13 1 0 14  x1001x 12 3 15 5	3 13 4 1 <b>x1010x</b> 9 5 6 0	4 14 10 7 x1011x 7 12 8 15 x1011x	14 0 1 6 <b>x1100x</b> 5 2 0 14	7 11 13 0 0 x1101x 10 15 2 x1101x	x1110x 6 8 9 3 x1110x	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1 1yyyy0 1yyyy1	x0000x 4 13 1 6 x0000x 13	1 15 14 3 x0001x 11 x0001x 2 x0001x 2	10 4 15 2  x0010x 2 11 11 13  x0010x 8	15 2 5 12  x0011x 14 7 13 8  x0011x 4	9 7 2 9  x0100x 15 4 12 1  x0100x 6	2 12 8 5 5 x0101x 0 9 3 4 x0101x 15	6 9 12 15 x0110x 8 1 7 10 x0110x 11	x0111x	0 6 7 11 <b>x1000x</b> 3 14 10 9	13 1 0 14  x1001x 12 3 15 5  x1001x 9	3 13 4 1 1 <b>x1010x</b> 9 5 6 0 <b>x1010x</b>	4 14 10 7 <b>x1011x</b> 7 12 8 15 <b>x1011x</b>	14 0 1 6 <b>x1100x</b> 5 2 0 14 <b>x1100x</b> 5	7 111 13 0  x1101x 10 15 5 2  x1101x 0	x1110x 6 8 9 3 x1110x	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1 1yyyy0 1yyyy1	x0000x 4 13 1 6 x0000x 13	1 15 14 3 x0001x 11 0 4 11 x0001x 2 15	10 4 15 2  x0010x 2 11 11 13  x0010x 8 13	15 2 5 12 x0011x 14 7 13 8 x0011x 4 8	9 7 2 9  x0100x 15 4 12 1  x0100x 6 10	2 12 8 5 5 x0101x 0 9 3 4 x0101x 15 3	6 9 12 15 x0110x 8 1 7 10 x0110x 11 7	x0111x  8  5  3  10  S <sub>7</sub> x0111x  13  10  14  7  S <sub>8</sub> x0111x  1	0 6 7 11 <b>x1000x</b> 3 14 10 9 <b>x1000x</b> 10	13 1 0 14  x1001x 12 3 15 5  x1001x 9 5	3 13 4 1 x1010x 9 5 6 0 x1010x	4   14   10   7	14 0 1 6 <b>x1100x</b> 5 2 0 14 <b>x1100x</b> 5	x1101x 10 15 5 2 x1101x 0 14	x1110x 6 8 9 3 x1110x 9 9	11. x1111x
0yyyy1 1yyyy0 1yyyy1 0yyyy0 0yyyy1 1yyyy0 1yyyy1	x0000x 4 13 1 6 x0000x 13	1 15 14 3 x0001x 11 x0001x 2 x0001x 2	10 4 15 2  x0010x 2 11 11 13  x0010x 8	15 2 5 12  x0011x 14 7 13 8  x0011x 4	9 7 2 9  x0100x 15 4 12 1  x0100x 6	2 12 8 5 5 x0101x 0 9 3 4 x0101x 15	6 9 12 15 x0110x 8 1 7 10 x0110x 11	x0111x	0 6 7 11 <b>x1000x</b> 3 14 10 9	13 1 0 14  x1001x 12 3 15 5  x1001x 9	3 13 4 1 1 <b>x1010x</b> 9 5 6 0 <b>x1010x</b>	4 14 10 7 <b>x1011x</b> 7 12 8 15 <b>x1011x</b>	14 0 1 6 <b>x1100x</b> 5 2 0 14 <b>x1100x</b> 5	7 111 13 0  x1101x 10 15 5 2  x1101x 0	x1110x 6 8 9 3 x1110x	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

上表列出了DES中使用的8个S盒。每个S盒将6位输入变为4位输出。给定输入后,输出行由外侧两位确定,列由内侧的4位确定,例如"011011"的输入的外侧位为"01",内侧位为"1101",而每张表的第一行为"00",第一列为"0000"因此在S5中的对应输出为"1001"(十进制的9),即第2行,第14列

#### 密钥调度过程中的移位

回次	左移位数
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

在子密钥生成完成前,密钥调度状态的每个半块都要向左循环移动特定的位,上表显示了移位的数量。