第5章 DES算法和AED算法

DES

Feature（特征）

data encryption standard
多表替换：sbox(数组)

- 块加密
- 每次加密8字节，明文64位，密钥64位
- 加密与解密的密钥相同（对称密钥加密算法）加密函数与解密函数并不相同

SBOX

- 每个sbox内容都不一样，相当于多表
- 每行16个元素，且每行元素一定在0-15之间
- 一个SBOX有4行，一共有8个SBOX
- SBOX输入48位，输出32位
- 48位分成8组，对应8个sbox，每一组6位。
- 进入48位，输出32位

	第1组	**第2组**	**第3组**	**第4组**	**第5组**	**第6组**	**第7组**
	101101	101101	101011	011001	010101	010101	100101
	sbox[0]	sbox[1]	sbox[2]	sbox[3]	sbox[4]	sbox[5]	sbox[6]
sbox行号	11	11	11	01	01	01	11
sbox列号	0110	0110	0101	1100	1010	1010	0010

$$\begin{cases} \text{第5位和第0位 } sbox\text{行号} \\ \text{第4位到第1位 } sbox\text{列号} \end{cases}$$

据此查找sbox[i],找到对应数值（0-15之间）即为输出的4位二进制值
所以sbox每个4行16列，且每个元素都在0-15之间

Procedure

- 打乱 permutation
  - 64位明文进入16位循环前需要对各个位的顺序进行打乱
  - 完成16轮加密后需要对64位密文的各个位的顺序进行打乱
  - sbox的32位输出要打乱
  - L_{28}, R_{28}变成28位时也要打乱

    打乱查询表IP（initial permutation）

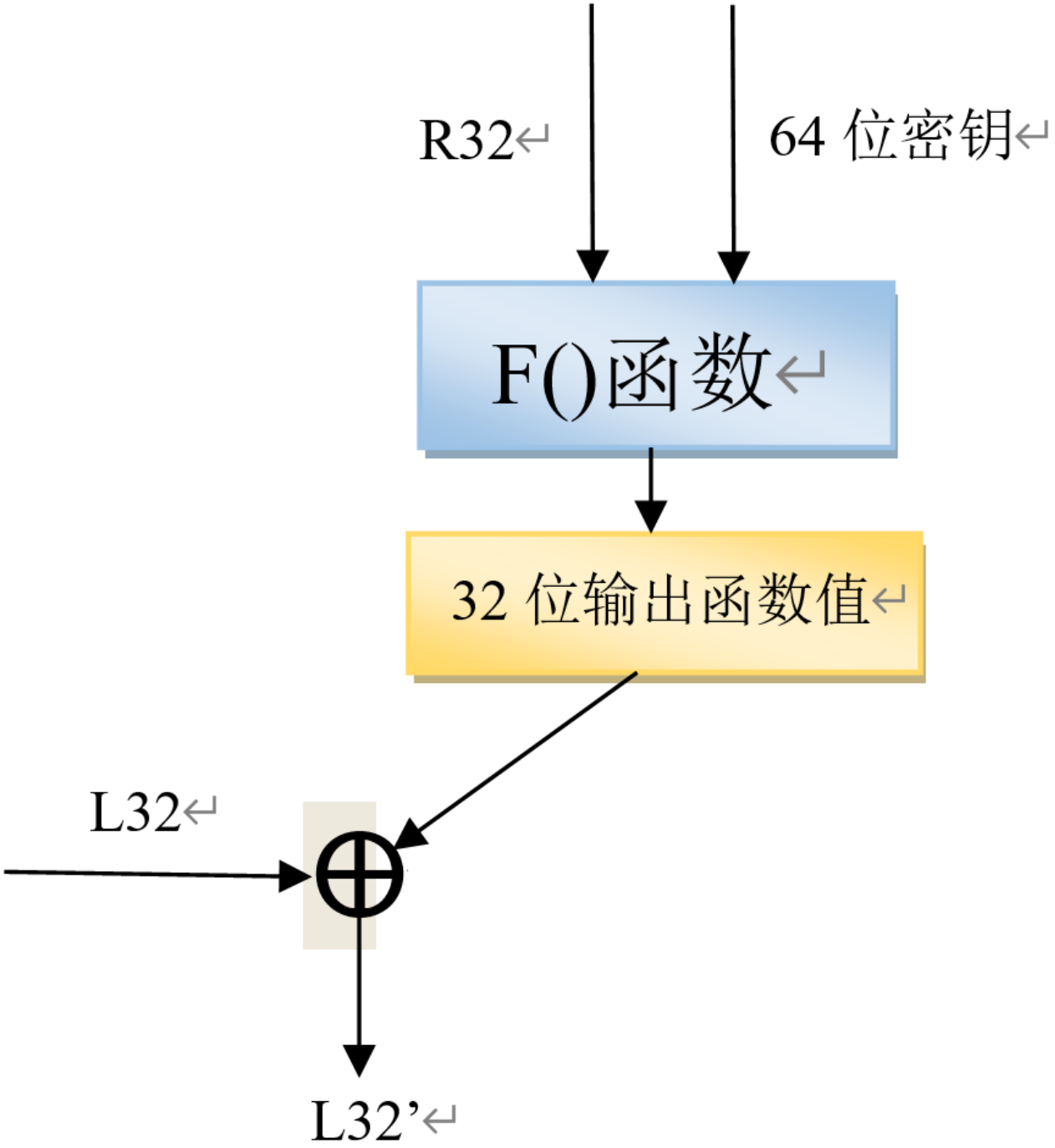
```
static char ip[64] = { /* [%] source Bit58-> target Bit1, Bit50->Bit2, ..., Bit7->Bit64 */
 58, 50, 42, 34, 26, 18, 10,  2,
 60, 52, 44, 36, 28, 20, 12,  4,
 62, 54, 46, 38, 30, 22, 14,  6,
 64, 56, 48, 40, 32, 24, 16,  8,
 57, 49, 41, 33, 25, 17,  9,  1,
 59, 51, 43, 35, 27, 19, 11,  3,
 61, 53, 45, 37, 29, 21, 13,  5,
 63, 55, 47, 39, 31, 23, 15,  7
  };
  //以1为基数的位的编号，下标是目标位号，数组元素的值是源数据的位号
  //ip[0]=58 表示源第57位数据要变成第0位
```

$$ByteIndex = SrcBit/8$$

$$BitIndex = SrcBit\%8$$

- 外迭代

  DES对位的表示采用**大端格式**



L_{32}表示明文的高32位，R_{32}表示明文的低32位

左右32位各加密8轮，两边一共加密16轮，每轮加密的密钥要不相同

第一轮

$L'_{32} = L_{32} \bigoplus f(R_{32}, key)$

$R'_{32} = R_{32} \bigoplus f(L'_{32}, key)$

第二轮

$L''_{32} = L'_{32} \bigoplus f(R'_{32}, key)$

$R''_{32} = R'_{32} \bigoplus f(L''_{32}, key)$

- F()函数的操作

  A R_{32}通过重复某些位(在DES中是固定的位)使其展开位48位

B 对于64位密钥key，丢弃8位变成56位，并分成左右各28位（L_{28}, R_{28}），循环左移后，合并成56位，再丢弃8位变成48位

C=A⊕B

C进入SBOX，输出的32位值就是F()的输出结果