第 5 章 Feistel 结构分组密码

Feistel 结构是分组密码经典结构之一，具有加解密结构相同或相似的特点，实际使用中占用软硬件存储资源少。基于此结构设计的分组密码有很多，本章介绍两个典型分组密码：DES 和 Camellia。

5.1 DES

1973 年，美国国家标准局开始研究除国防部外的其他部门计算机系统的数据加密标准，并于 1973 年 5 月 15 日和 1974 年 8 月 27 日先后两次向公众发出了征求加密算法的公告。1977 年 1 月，美国政府正式颁布 IBM 公司设计的方案 DES 作为非机密数据的数据加密标准。

5.1.1 DES 设计

DES 基于 Feistel 结构设计，主要由 S 盒查询、比特移位、异或运算构成。DES 的分组长度为 64 比特，密钥长度为 56 比特，迭代 16 轮，共使用 16 个轮密钥 K_1、K_2，…，K_{16}，这些轮密钥都是由主密钥 K 生成的。DES 的加密流程如图 5-1 所示。图 5-1 中 L_i 和 R_i 的长度都是 32 比特，最后一轮不进行左右交换，直接输入逆初始置换。

1. 加密变换

DES 加密流程分为 3 个步骤：

(1) 初始置换。

对明文 64 比特进行初始置换(IP)，如表 5-1 所示，输出仍然是 64 比特，然后分成左右两个 32 比特 L_0 和 R_0。

表 5-1 初始置换

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

续表

59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

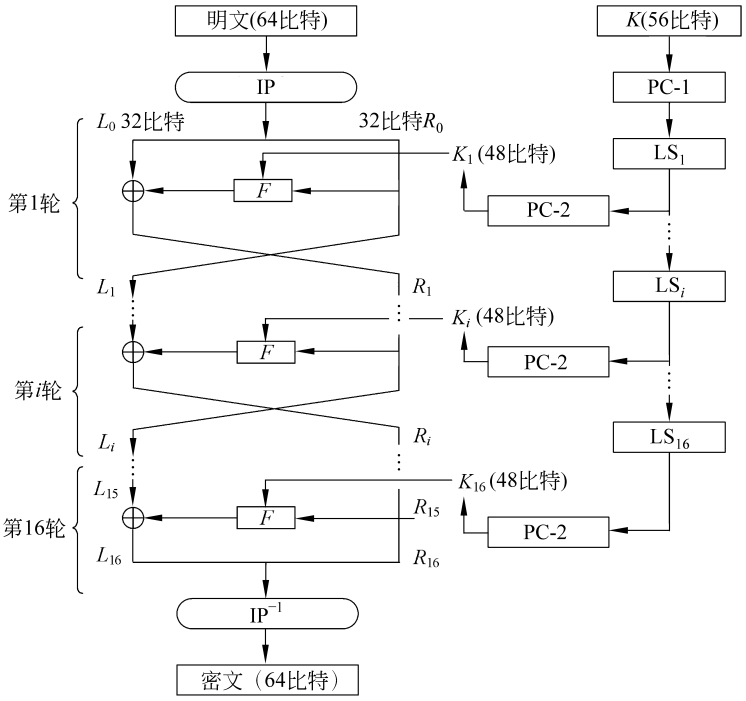

图 5-1　DES 的加密流程

(2) 轮函数迭代。

基于 Feistel 结构进行 16 轮迭代，第 i 轮表示如下：

- 当 $1 \leqslant i \leqslant 15$ 时，有 $L_i = R_{i-1}$，$R_i = L_{i-1} \oplus F(K_i, R_{i-1})$。
- 当 $i = 16$ 时，有 $L_i = L_{i-1} \oplus F(K_i, R_{i-1})$，$R_i = R_{i-1}$。

(3) 逆初始置换。

进行逆初始置换(IP^{-1})。IP^{-1}是 IP 的逆，如表 5-2 所示。最后输出当前明文对应的密文。

表 5-2　逆初始置换

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

续表

34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

第(2)步中 F 函数是 DES 的核心，主要包含扩展函数 E、轮密钥异或、S 盒查询和置换函数 P 四个组件，其执行过程如图 5-2 所示。

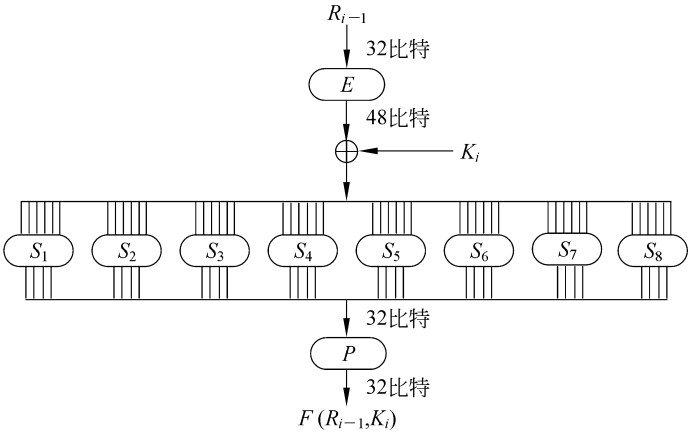

图 5-2　DES 的 F 函数

① 扩展函数 E 将 32 比特的输入扩展为 48 比特的输出，如表 5-3 所示。

表 5-3　扩展函数 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

② 轮密钥异或将 $E(R_{i-1})$ 与轮密钥 K_i 按位进行模二加运算，并将运算结果从左到右分为 8 组，每组 6 位，即

$$E(R_{i-1}) \oplus K_i = B_1B_2B_3B_4B_5B_6B_7B_8$$

其中，B_j 的长度为 6 位，$1 \leqslant j \leqslant 8$。

③ S 盒查询就是将每个 B_j 查询 S 盒后缩减为 4 位，共 8 个 S 盒 $S_1, S_2, \cdots, S_8$，每个 S 盒有 4 行 16 列数据。具体 S 盒查询参考 3.2 节中 S_1 的介绍。

④ 将 8 个 S 盒的输出经过表 5-4 的置换函数 P 进行换位处理后就得到 $F(R_{i-1}, K_i)$。

表 5-4　置换函数 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

2. 密钥扩展算法

主密钥 K 共 56 比特，在传输过程中加 8 比特奇偶校验位，分别位于 8，16，24，32，40，48，56，64 位。奇偶校验位用于检查密钥 K 在分配以及传输过程中可能发生的错误。密钥扩展算法的输入只有 56 比特，经过 PC-1（见表 5-5）打乱重新排列，从主密钥 K 生成轮密钥 K_i（48 位）的过程如图 5-3 所示。

表 5-5　PC-1

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

图 5-3 中 $C_i = \mathrm{LS}_i(C_{i-1})$，$D_i = \mathrm{LS}_i(D_{i-1})$，其中 LS_i 表示对 C_{i-1} 和 D_{i-1} 进行循环左移变换，LS_1、LS_2、LS_9、LS_{16} 是循环左移 1 比特输出变换，其余的 LS_i 是循环左移 2 比特变换。PC-2（见表 5-6）表示从数据状态 56 比特中选出 48 比特作为轮密钥 K_i。

表 5-6　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

3. 解密变换

DES 的解密过程和加密过程使用同一结构，只不过在 16 次迭代中使用轮密钥的次序正好相反。解密时，第 1 次迭代使用轮密钥 K_{16}，第 2 次迭代使用轮密钥 K_{15}，以此类推，第 16 次迭代使用轮密钥 K_1。

4. 设计特点

分组密码 DES 的主要特点也是 Feistel 结构的特点，即加密结构与解密结构相同。

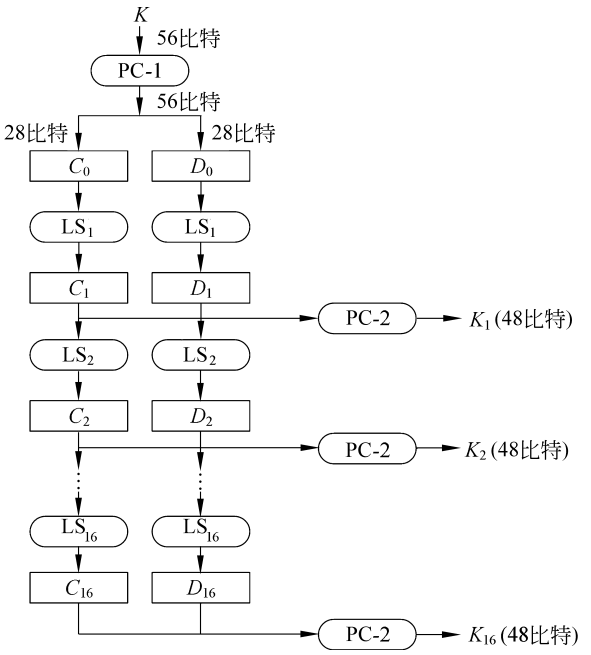

图 5-3　DES 密钥扩展算法

除此之外，DES 的组件大都是面向比特设计的，如初始置换 IP、逆初始置换 IP^{-1}、扩展变换 E、置换 P 以及密钥扩展算法中的压缩变换 PC-1、PC-2 等，与软件实现相比更适合硬件实现，这与该分组密码设计之初的计算机发展水平有一定的关系。

5.1.2　DES 安全性评估

DES 自 1977 年公布之后，经历了穷举攻击、滑动攻击、差分分析、线性分析等。20 世纪 90 年代初，Biham、Matsui 等人分别用差分分析、线性分析攻破了全轮 DES[3][40]。Matsui 在 1994 年的美密会上第一次通过实验给出了 16 轮 DES 的线性分析。这两种方法在此后的对称密码分析方法中占据主要地位。

1. 差分分析

差分分析是一种选择明文攻击。在分组密码中由于非线性组件的引入，存在以一定概率传播的差分路径，对于一定的输入/输出差分，所有路径概率之和就是对应的差分特征概率。对于 r 轮分组密码，输入差分 ΔX_0 为 α，加密 $r-1$ 轮后的输出差分 ΔX_{r-1} 为 β，且对应差分概率 $P(\alpha \rightarrow \beta)=p$。恢复最后一轮密钥的步骤简述如下：

第一步，明文采样。选择 m 对明文，每对明文差分为 α。

第二步，过滤正确对。根据差分特征的输出可以推导或观察到密文对的输出特点，可以将一部分不是正确对的明文对过滤掉，这样可以避免错误对蕴含密钥的干扰，以提高效率。

第三步，提取信息。猜测最后一轮的部分密钥并解密得到 $r-1$ 轮的输出，一般情况下，若满足输出差分为 β 的对数近似等于 mp，则猜测的最后一轮部分密钥正确；否则猜

测的密钥错误。

上述第二步中过滤正确对也称为去噪阶段，主要目的是过滤掉错误对，排除干扰。假设过滤系数为 λ，$0<\lambda\leqslant 1$，该取值与差分区分器输出有关，表示过滤之后的明文对数量与总明文对数量的比值。

在提取信息阶段设置两个参数：攻击猜测的密钥比特量 l 和平均每对密文蕴含的密钥个数 v，v 的取值与算法组件(如 S 盒)的差分分布特性有关。

根据以上几个参数，正确密钥至少被统计了 mp 次，所有猜测密钥平均被统计了 $m\lambda v/2^l$ 次，这两者之比就是 Biham 和 Shamir 给出的信噪比。

定义 5-1 若采用计数原理对密码算法进行差分攻击，则正确密钥至少被统计的次数与所有猜测密钥平均被统计的次数之比称为该计数系统中的信噪比，记为 $\frac{S}{N}$，表示如下：

$$\frac{S}{N}=\frac{mp}{m\lambda v/2^l}=\frac{2^l p}{\lambda v}$$

信噪比越大，正确密钥被统计的次数越多，这样能更有效地得到正确密钥。根据对 DES 算法的大量分析数据统计，信噪比的取值可以进一步确定所需的选择明文量：

$$m\approx c\,\frac{1}{p}$$

其中，c 为一个固定常数，根据信噪比近似估算，Biham 和 Shamir 总结如下：

(1) 当 $\frac{S}{N}$ 为 1～2 时，c 取值为 20～40。

(2) 当 $\frac{S}{N}$ 取值较大时，c 取值为 3～4。

(3) 当 $\frac{S}{N}$ 取值较小时，c 需取更大的值。

接下来对 DES 进行差分分析。DES 的 F 函数使用了 8 个不同的 6×4 规模的 S 盒，从任何一个 S 盒的差分分布表出发，都可以寻找差分路径。表 5-7 是第 2 个 S 盒(S_2)的部分差分分布表，结合 F 函数的扩展变换 E 和置换 P，给出 F 函数的差分路径。

表 5-7 S_2 的差分分布表(部分)

输入\输出	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	2	6	4	0	14	8	6	8	4	6	2
2	0	0	0	2	0	4	6	4	0	0	4	6	10	10	12	6
3	4	8	4	8	4	6	4	2	4	2	2	4	6	2	0	4
4	0	0	0	0	0	6	0	14	0	6	10	4	10	6	4	4
5	2	0	4	8	2	4	6	6	2	0	8	4	2	4	10	2
6	0	12	6	4	6	4	6	2	2	10	2	8	2	0	0	0
7	4	6	6	4	2	4	4	2	6	4	2	4	4	6	0	6
8	0	0	0	4	0	4	0	8	0	10	16	6	6	0	6	4

续表

输入\输出	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
9	14	2	4	10	2	8	2	6	2	4	0	0	2	2	2	4
10	0	6	6	2	10	4	10	2	6	2	2	4	2	2	4	2

例 5-1　如图 5-4 所示，当函数 F 的输入差分为 $\Delta=(04000000)_{\mathrm{H}}$（H 表示十六进制）时，非零差分比特经过 E 没有扩散，只是发生了移位，使得 S_2 活跃，其输入差分为 $(001000)_{\mathrm{B}}$（B 表示二进制），选择概率最大的输出差分 1010_{B}，再经过 P 变换之后，函数 F 的输出差分为 $\Delta=(40080000)_{\mathrm{H}}$。差分概率由 S_2 的差分分布表查得，即 $p(001000\rightarrow 1010)=\frac{16}{64}=0.25$。若函数 F 是随机函数，则对应的输出差分概率应该为随机概率 2^{-32}。显然，上述差分概率远远大于此随机概率。

由例 5-1 的函数 F 差分特征容易构造如图 5-5 所示的 3 轮差分路径。

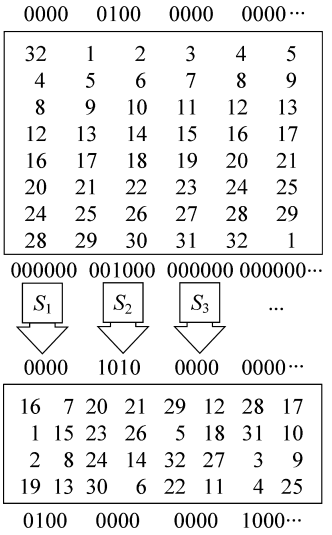

图 5-4　函数 F 差分传播

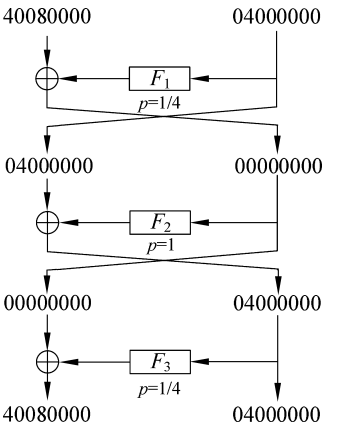

图 5-5　DES 的 3 轮差分路径

例 5-2　选取明文对 (X,X')，满足 $\Delta X=X\oplus X'=(40080000\ 04000000)_{\mathrm{H}}$，此处采用十六进制表示，忽略 DES 算法中 IP 和 IP^{-1}。

第 1 轮中函数 F_1 的输入差分为 $(04000000)_{\mathrm{H}}$，利用例 5-1 中的差分传播，得到 F_1 的输出差分 $(40080000)_{\mathrm{H}}$，差分概率为 2^{-2}，与左边明文差分异或之后为 0。

第 2 轮输入差分为 $(04000000\ 00000000)_{\mathrm{H}}$，即函数 F_2 的输入差分为 0，输出必为 0。

第 3 轮输入差分为 $(00000000\ 04000000)_{\mathrm{H}}$，进入函数 F_3 的输入差分与 F_1 相同，因此输出差分 $(40080000)_{\mathrm{H}}$，概率为 2^{-2}。

由此得到输出密文对 (Y,Y') 的差分为 $(40080000\ 04000000)_{\mathrm{H}}$，3 轮差分路径概率为 $2^{-2}\times 2^{-2}=2^{-4}$。

值得注意的是，DES 的 S 盒是 6 比特输入、4 比特输出，平均 4 个不同的输入值对应同一个输出值，所以必然会存在输入差分非零、输出差分为零的情况。这种性质说明函数

F 不是置换。

例 5-3 如图 5-6 所示，设明文左边 32 比特 P_L 输入差分 $\Delta=(19600000)_H$ 时，该非零差分会进入第 2 轮的函数 F_2 中，经过 E 扩展置换，共引起 3 个 S 盒 S_1、S_2、S_3 活跃。查表 5-8～表 5-10 对应的 3 个 S 盒的差分分布表，得 S_1、S_2、S_3 的输出差分为 0 的概率分别为$\frac{14}{64}$、$\frac{8}{64}$、$\frac{10}{64}$，所以函数 F 输出差分为 0 的概率为三者之积，即$\frac{1}{234}$。

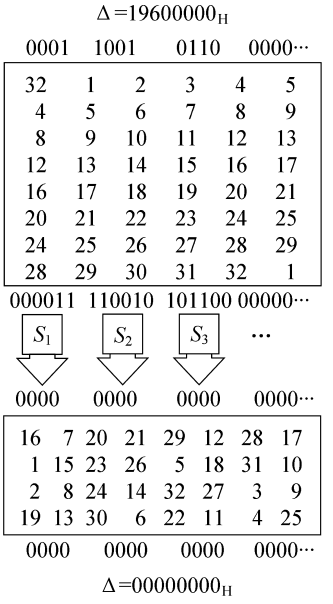

图 5-6 函数 F 的差分传播(输出差分为 0)

表 5-8 S_1 的差分分布表(部分)

输入\输出	0	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2

表 5-9 S_2 的差分分布表(部分)

输入\输出	0	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
48	0	4	0	2	4	4	8	6	10	6	2	12	0	0	0	6
49	0	10	2	0	6	2	10	2	6	0	2	0	6	6	4	8
50	8	4	6	0	6	4	4	8	4	6	8	0	2	2	2	0
51	2	2	6	10	2	0	0	6	4	4	12	8	4	2	2	0
52	0	12	6	4	6	0	4	4	4	0	4	6	4	2	4	4

表 5-10　S_3 的差分分布表(部分)

输入\输出	0	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
41	0	2	8	4	0	4	0	6	4	10	4	8	4	4	4	2
42	2	6	0	4	2	4	4	6	4	8	4	4	4	2	4	6
43	10	2	6	6	4	4	8	0	4	2	2	0	2	4	4	6
44	10	4	6	2	4	2	2	2	4	10	4	4	0	2	6	2
45	4	2	4	4	4	2	4	16	2	0	0	4	4	2	6	6

由于 F 不是置换,所以 DES 算法存在 2 轮循环差分路径,即在加密 2 轮之后输出差分与输入差分相同,如图 5-7 所示,这样的差分特征可以用来连接构造成倍轮数的差分路径。当然,若 F 函数为置换,那么不存在 2 轮循环差分路径,但是可能存在多轮循环差分路径。

由上述 2 轮循环差分路径可以构造 16 轮差分路径,概率为 $\left(\frac{1}{234}\right)^8 \approx 2^{-62.85}$,小于随机置换概率 2^{-64},由此可见 16 轮 DES 算法不能完全保证其输出密文的随机性。

构造差分特征之后是密钥恢复阶段,基于以上得到的差分路径,可以进行更多轮数的密钥恢复攻击。为了描述简洁,下面只对 4 轮 DES 进行密钥恢复攻击,如图 5-8 所示。

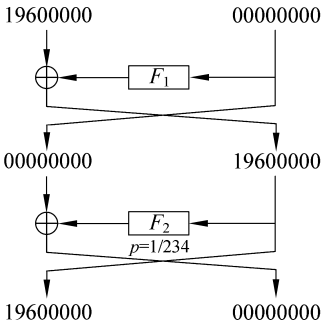

图 5-7　DES 的 2 轮循环差分路径

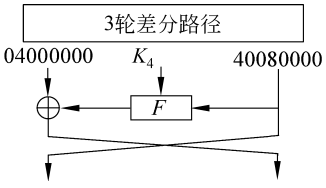

图 5-8　密钥恢复阶段

例 5-4　在例 5-1 的 3 轮差分路径之后再加一轮,写出恢复最后一轮部分密钥的步骤。

由于 3 轮差分路径概率为 2^{-4},所以选择 2^5 对明文(X, X'),满足差分 $\Delta X = X \oplus X' = (40080000\ 04000000)_H$。具体步骤如下:

第一步,选择 2^5 对明文,进行 4 轮加密,至少有 2 对输出密文满足 C_L 的差分为 $(40080000)_H$。

第二步,因为第 4 轮非零差分比特进入函数 F_4 后引起 3 个 S 盒活跃,见表 5-11,即 S_1、S_3、S_4,需要猜测对应的 18 比特密钥,得到 F_4 的输出,将这个差分与 ΔC_R 异或。

表 5-11　非零差分比特扩散

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

第三步，若得到差分$(04000000)_{\mathrm{H}}$，则猜测密钥正确；否则猜测密钥错误。

对于猜测的错误密钥，平均留下的密文对为 $2\times 2^{-12}=2^{-11}$ 个；对于猜测的正确密钥，至少有 2 个密文对满足 3 轮差分路径，所以多个密文推荐的密钥一般为正确密钥。

Biham 等人在攻击全轮 DES 时，将 2 轮循环差分用在了第 2～14 轮，然后猜测第 1 轮和第 16 轮部分密钥，整个攻击的数据复杂度大约为 2^{47} 个选择明文。

2. 线性分析

线性分析的主要思想是寻找明文、密文和密钥之间有效的线性表达式，根据有效性以一定概率猜测出对应的密钥比特。

1）线性表达式构建

根据分组密码结构可以构建有效的线性表达式，步骤如下：

第一步，利用统计测试的方法给出分组密码中非线性组件（如 S 盒）的输入、输出之间的一些线性逼近等式及其成立的概率。

第二步，结合轮函数中的线性变换组件构造每一轮的输入、输出之间的线性逼近等式，并计算出其成立的概率。

第三步，将各轮的线性逼近等式按顺序级联起来，削除中间相同的变量，就得到了仅涉及明文、密文和密钥的线性逼近，如式(5-1)所示：

$$P_{[i_1,i_2,\cdots,i_a]}\oplus C_{[j_1,j_2,\cdots,j_b]}=K_{[k_1,k_2,\cdots,k_c]} \tag{5-1}$$

这里 $i_1,i_2,\cdots,i_a$、$j_1,j_2,\cdots,j_b$ 和 $k_1,k_2,\cdots,k_c$ 表示固定的比特位置。对特定的分组密码，随机给定明文 P 和相应的密文 C，很多情况下存在概率 $p\neq\frac{1}{2}$ 的式(5-1)，通常用 $\left|p-\frac{1}{2}\right|$ 刻画其有效性，称为线性逼近优势。

2）密钥比特猜测

假定已获得一个有效的线性表达式，可以通过基于最大似然方法的算法 5-1 推测一个密钥比特 $K_{[k_1,k_2,\cdots,k_c]}$ 信息，其中 N 是给定的已知明文的个数。