**DES算法**

DES为64位的16轮的Feistel结构（见图1），每一轮的变换为FKr(L,R)=(R,L^fKr(R))，其中L，R分别表示数据的左右部分，f是以48位轮密钥Kr为参数的32位到32位的映射函数（见图2）。

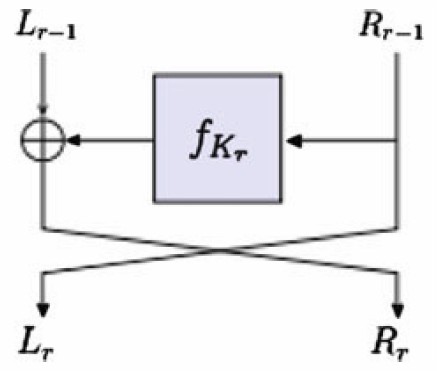


图1：Feistel结构

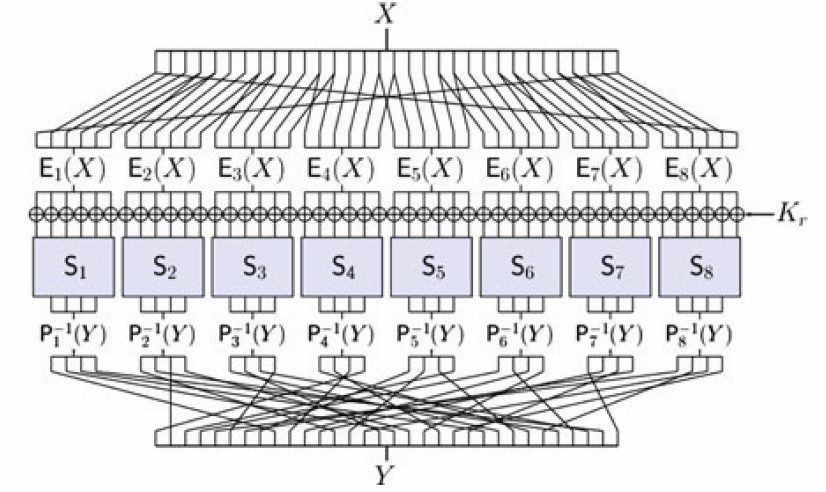


图2: f函数

**对DES的第16轮攻击**

假设在第16轮开始的时候，R15的一些比特翻转，那么由图1可得R16和R16’的差分满足等式：

（等式3.1）

由图2可知，f函数中的S盒独立进行计算，所以上式可以转换成8个等式：

（等式3.2） 1<=i<=8

因此攻击击可以测试K16,i的所有值｛0，1｝6，排除不满足等式3.2的值，最终得到密钥。本攻击适用于注入的故障只影响R15的情况，并且影响的位数越多，受影响的S盒也越多，所需要的密文对（C,C’）也越少。

对DES的第16轮攻击

假设在第15轮开始的时候，在R14上注入单比特故障，使R14’=R14^e,由图3得

（等式3.3）

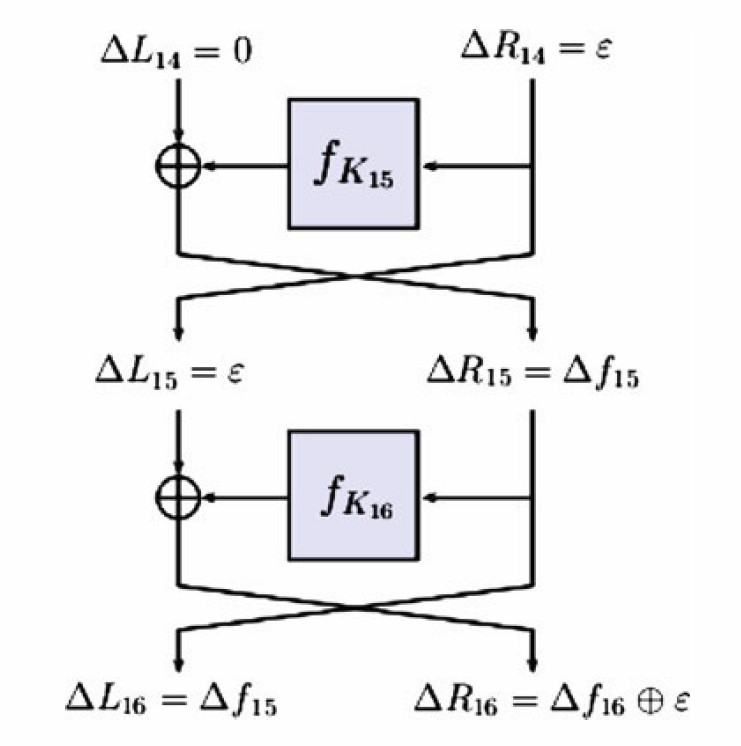


图3 第15轮的错误扩散

在上式中K16不是唯一的未知参数，接下来需要确定或者缩小e的范围。利用下式可以推出第15轮的有效S盒（即被故障影响的S盒），如果两个S盒有效，则e的值有2种可能，因为由图2可知每对S盒最多共享两个输入比特，同理如果只有一个S盒有效，e的值也有2种可能。

（等式3.4）

一旦e 的候选值被选定，就可以用等式3.3区分K16,同上一节中的攻击一样，可以根据

等式3.5

筛选出K16的值。

与上一节中的攻击相比，为了缩小e的取值范围，本攻击为单比特故障模型（或者只有几个比特故障）。因为错误被扩散到第16轮的多个S盒，所以K16的筛选效率并不比前面的攻击慢。