Fishingrod算法描述

Fishingrod算法输入为128比特，轮秘钥为64比特，输出为128比特,轮数为18轮，轮函数结构图如图1所示。输入左右分支均为64比特，左分支与轮秘钥做“与”运算结果亦或上右分支的结果作为轮函数的输入。F的输出亦或上一轮加密的右分支输出，F的输出与轮秘钥做“与”运算结果亦或上右分支一轮加密的右分支输出。

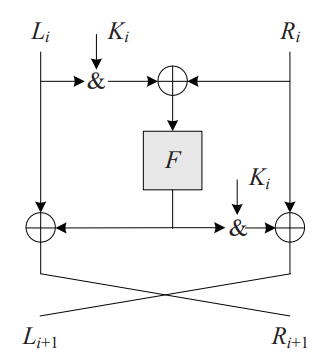


图 1 Fishingrod轮函数结构图

F函数

F函数输入为64比特，输出为64比特，F函数包含三个操作：通过S层(S)，循环移位(SR)，列混合(MC),即。

S：S层由8个8比特S盒组成，64比特通过S盒，S盒使用AES的S盒。经过S盒子运算后的状态表示为：

SR：将S层的输出循环左移两个字节。经过移位后的状态表示为：

MC：采用AES的MC矩阵进行列混淆操作，具体运算如下：

