LBlock算法描述

LBlock密码算法是由吴文玲等2011年提出的轻量级分组密码算法。加密算法采用Fistel结构，基于4比特模块设计。密钥扩展算法的设计借鉴了PRESENT算法的设计理念，采用非线性移位寄存器，利用S盒变换和循环移位生成轮密钥。

**1、LBlock加密算法**

LBlock加密算法采用Fistel结构，分组长度为64比特，密钥长度为80比特，迭代论述为32轮。使用表示64比特明文。加密流程见图1.1。



图1.1



图1.2 轮函数-F

(1)对，

(2)输出，作为64比特密文。

(3)轮函数（图1.2）

，，

其中:有

其中:有

**2、LBlock解密算法**

解密算法是加密算法的逆过程，输出64比特明文。

**3、LBlock密钥扩展算法**

将80比特密钥置入寄存器，次序为在最左边，在最右边。取最左边32比特作为子密钥。按照以下步骤执行31次。

（1）。

（2）

。

（3）。

（4）取寄存器最左端 32 bit 密钥作为。

79 78............50 49 48 47 46.........79-50+1=30