关于LBLOCK-S的相关密钥不可能回旋密码分析

介绍：随着电子信息的迅速发展和射频识别技术（RFID）等的普及，传统的分组密码已经不适合资源受限的环境。因此，在资源受限的环境下，兼顾安全性和硬件性能的轻量级分组密码成为了研究的热点。

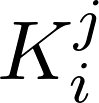
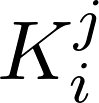
Lblocks作为和凯撒竞争的LAC的核心分组密码，是吴文玲等人在2011年的ANCS会议上提出的LBlock的改进版本。与LBlock算法类似，它也使用了feistel结构以及32轮加密，并且分组长度和密钥长度分别为64比特和80比特。LBlock-s算法和LBlock算法不同的地方在于LBlock-s采用了一种改进的密钥调度算法，具有更快的扩散速度，并将S盒中的10个不同的S盒改为了相同的盒，以降低硬件和软件的成本。在安全性方面，Shan[3]等人表明32轮相关差分验证中至少有32个活跃的盒子中的概率不会高于2-64，并给出轮了10轮和11轮的相关密钥差分特征。肖[4]利用差分密码分析给出了一个16轮的差分路径，李[5]等人用改进的多维零相关线性密码分析对LBlock-s进行了23轮的攻击。利用LBlock人员设计给出的LBlock的14轮微分可能特性，贾[6]对LBlock-s进行了21轮的攻击，他们给出了22轮和23轮的攻击结果，但没有给出具体的分析。并且结果表明，22轮的攻击时间复杂度是278.86次22轮加密的时间，接近穷举搜索的时间复杂度，远高于本文的相应攻击结果。

相关的密钥分析分别由Knudsen[7]和Biham[8]独立引进的。该技术的基本思想就是攻击者发现密钥调度算法的弱点，选择合适的密钥关系，然后预测这些密钥加密后的密文。Knudsen和Biham先后针对Skipjack提出了不可能差分密码分析，攻击者试图找到概率为0的差分特征，以消除错误的密钥，然后恢复正确的密钥。相关密钥密码分析和不可能差分密码分析都是分析各种分组密码安全性的有力技术，对蜂鸟-2，TEA，LBlock，MIBS等许多分组密码都有很好等攻击效果。回旋密码分析是Wagner在1999年提出的，它是差分密码分析的一个变种。回旋密码分析的基本思想就是利用概率较大的短差分特征形成概率较大的长差分特征。相关的不可能回旋密码分析是通过结合使用这三种攻击而获得的。迄今为止，利用这种密码分析技术在AES和LBlock上取得过许多令人满意的分析结果。

本文首次从相关密钥不可能回旋密码分析的角度研究了LBlock-s的安全性。通过分析LBlock-s的轮函数以及密钥调度函数的性质，实现了一个15轮相关的密钥不可能回旋识别器，得到轮一个22轮相关的密钥不可能回旋特征来回复68比特的密钥，时间复杂度为268.76，选择了258个明文。到目前为止，这是对22轮lBlock-s算法最佳对攻击效果。

概论：第二节对LBlock-s进行了描述，并给出了一些本文使用的一些符号。在第三节中，我们研究了相关的密钥不可能回旋密码分析。在第四节中，我们介绍了一个与15轮相关的密钥不可能回旋识别器和22轮的攻击，并在第五节给出结论。

1. ：LBlock-s的描述

* 符号：
* P，C：P为64比特明文和C为64比特密文
* *K*，*K*：80比特的主密钥以及和密钥的差异和密钥的变化率
* *Ki*，*Ki*：第i轮的次密钥以及密钥的变化率
* ，：*Ki*的第*j*次nibble攻击以及*Ki*的第*j*次nibble攻击
* *Xi*，*Xi* ：第*i*轮输入的左半边字符以及它的变化
* *X*0：第一轮输入的明文的右半边
* *Xij*，*Xij*：*Xi*的第j次nibble攻击和*Xi*的第j次nibble攻击
* *Xi* **||** *Xj*：*Xi*和*Xj*的拼接的组合
* *X*<<<*i：X*字符串循环向左移位i个比特
* X>>>i：*X*字符串循环向右移位i个比特
* [*i*]2：整数*i*的二进制形式
* LBlock-s算法概述：

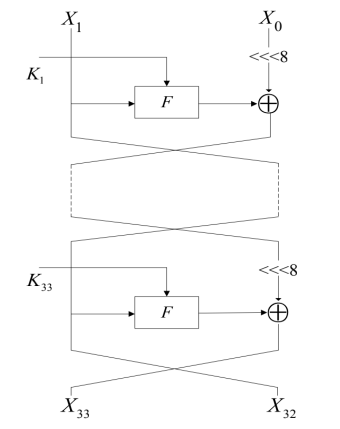
LBlock-s是LBlock的改进版本，具有Feistel结构的变体。它由32轮迭代组成，块长64位，主密钥长80位。加密过程如下，图1示出了一般结构。

输入：X=*X*1 **||** *X*0

for *i* in [2,33]:

*Xi*=*F*(*Xi*-1,*Ki*-1) **⊕** *Xi-2*<<<8

输出：C=*X*33 **||** *X*32

图1

F轮函数定义为： (见图2)。它包括三个基本函数：键加法层、非线性变换和线性扩散函数。混淆函数S包括8个相同的并行4位S盒，这是LBlock中使用的第一个S盒(见表一，16进制表示法)，并且函数P是图2中详细说明的4位逐字排列。

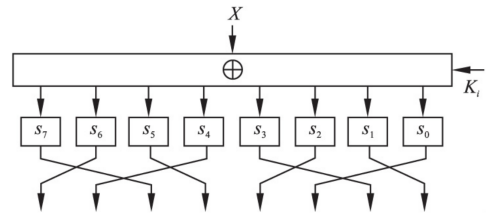
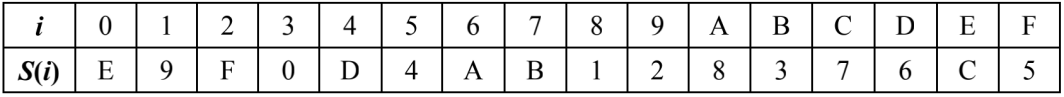
图2

表1 S盒的成分

LBlock-s的解密算法与加密算法相反。因此，这里仅作简要说明：我们让 C = *X*32 **||** *X*33表示密文，随后进行循环运算：

for *i* in [31,0]:

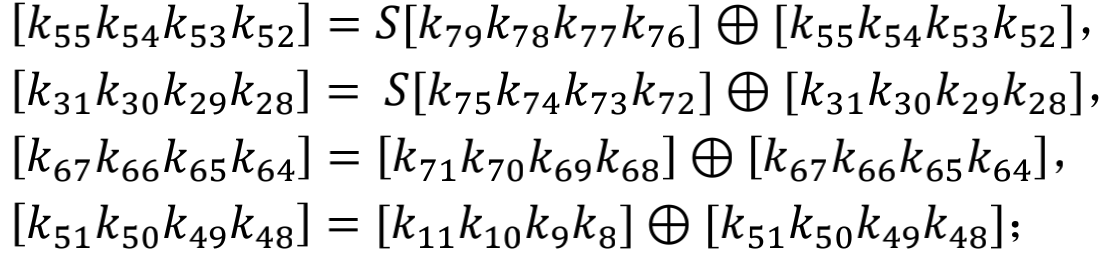
*Xi*=*F*(*Xi+*1,*Ki+*1) **⊕** *Xi+2>>>*8

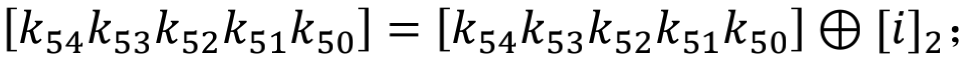
输出：P=*X*1 **||** *X0*

* 密钥调度算法

LBlock-s采用了一种改进的密钥调度算法，该算法具有更好的抗双液密码分析的扩散性能。LBlock-s的密钥调度每次更新16位，这些更新的位受密钥寄存器的32位的影响。相反，原始密钥调度仅基于密钥寄存器的13位更新13位。主密钥 存储在密钥寄存器中。输出最左边的32位作为子密钥*K1*。对于*for i* =1,2，⋯，31，按如下方式更新密钥寄存器：

1.

2.

3.

1. 输出寄存器K最左边的32位作为轮次密钥.

其中S盒与加密算法中使用的S盒相同。

1. :相关密钥不可能回旋密码分析

相关密钥不可能回旋密码分析包括相关密钥密码分析、不可能差分密码分析和回旋密码分析。如图3所示，该技术将密码*E*视为两个子密码*E*0和*E*1，即。通常*E=E*0**||** *E*1，每个子密码包含两个相关的密钥微分特性，概率为1。

它们如下所示：

* α→β：是*E0*的第一个相关键差分特性
* α’→β’：是*E0*的第二个相关键差分特性
* δ→γ：是*E1*-1的第一个相关键差分特性
* δ’→γ‘：是*E1*-1的第二个相关键差分特性

这些α、β、α’、β’、δ、γ、δ’、γ‘都是*n*比特的块。四个特征中使用的对应密钥分别是：*K*A,*K*B,*K*C,*K*D，当β、β’、γ、γ‘满足条件*β***⊕***β*‘**⊕***γ***⊕***γ*‘≠0时，