**北京电子科技学院**

**《对称密码设计与实现》课**

**分组密码设计材料**(模板)



**学生学号姓名： 20125326张阳**

**指导教师： 郑秀林**

**系 别： 信息安全系**

**专 业： 信息与计算科学**

**提交时间： 2015年3月12日**

**分组密码设计**

1. **总体设计思想**

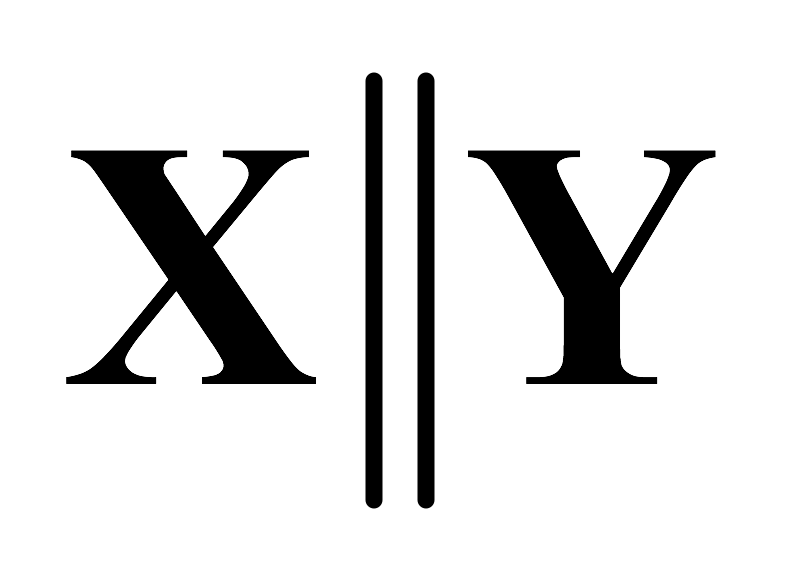
**Camelia 算法的主要部件没有进行更改，但是在分组后，加入一个扩散部件，使得每两块Block 互相关联**

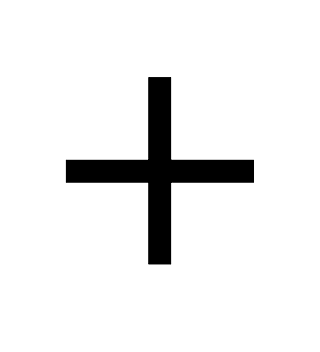
1. **加解密算法**

本部应包括以下内容：

1. **符号及约定**

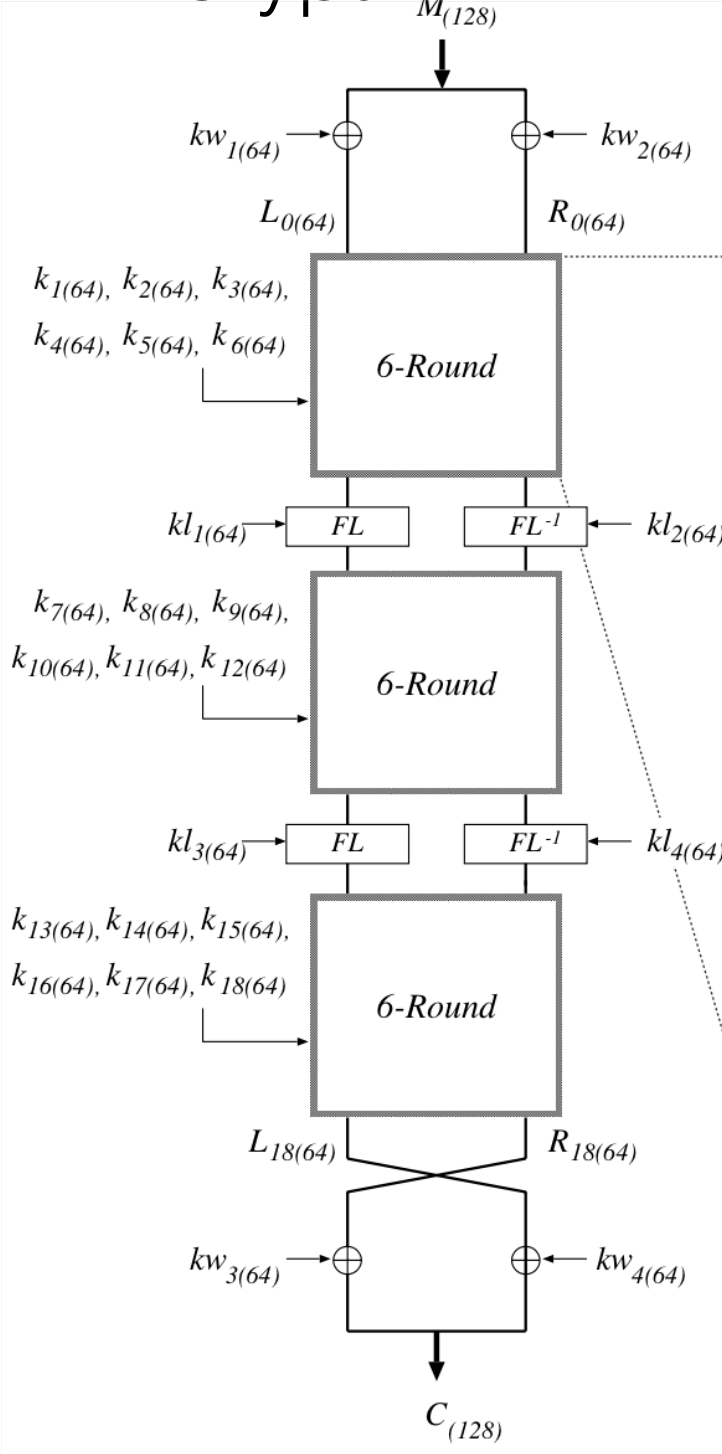
例如：X(nbit)<<<k---将nbit数据X循环左移k位

---变量X与Y的连接

 X□Y——(X+Y)mod232

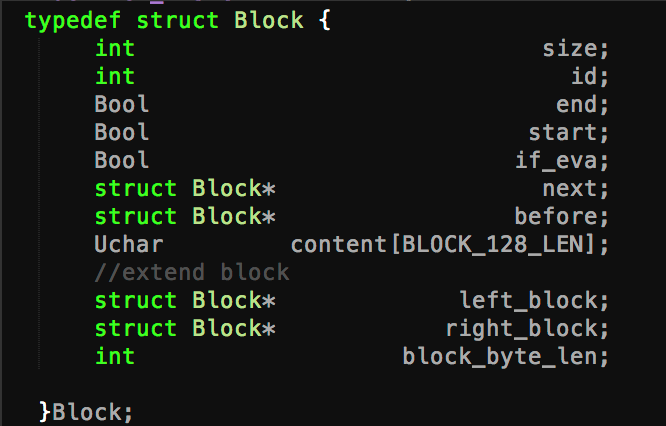
1. **加密算法描述**

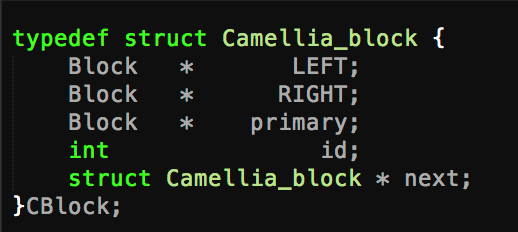
此部分内容应包括：

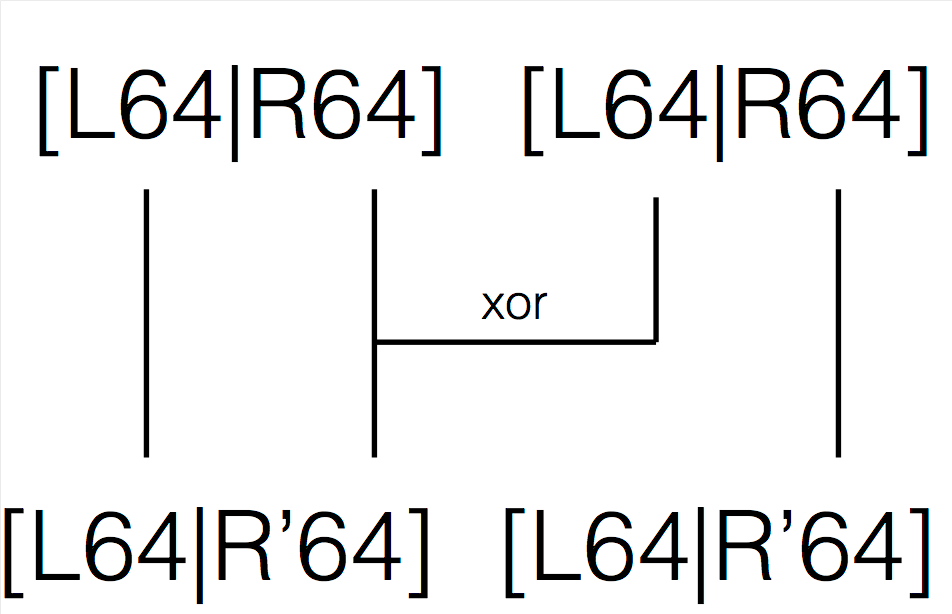
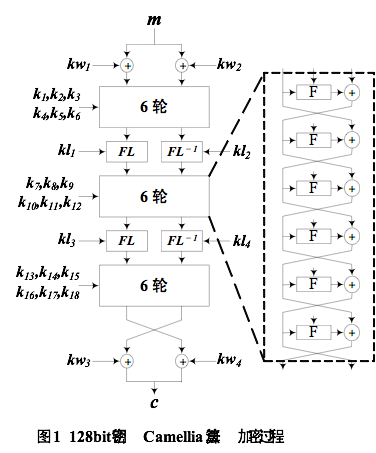
(1) 加密算法主框图(如图1所示)

依据子密钥如何将一组明文数据分层次一步一步地加密成一组密文数据。

(2) 加密算法分层(或模块)的描述

模块：Block 和 Camellia\_Block 分为128位和64位，为了Camellia 和之后算法开发出的模块，



单轮加密前进行一次所有块的亦或扩散如图2

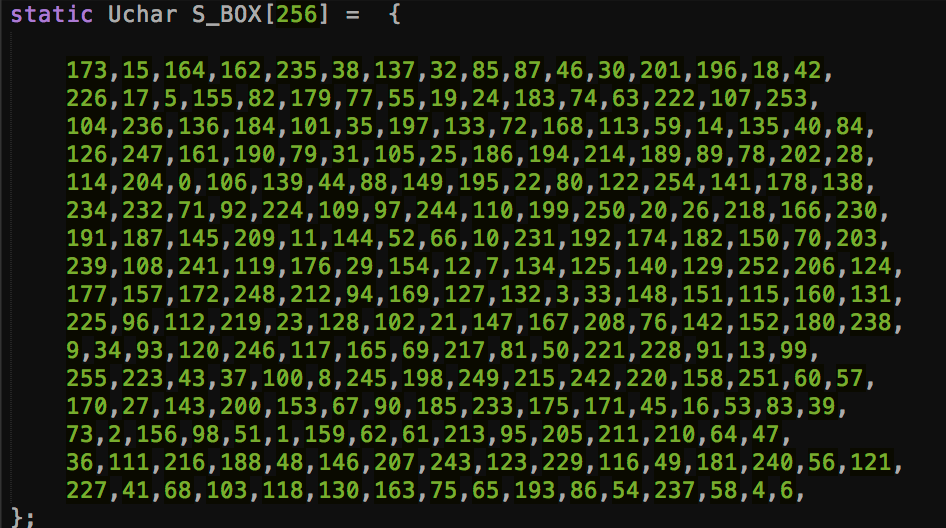
**图1说明：**

* + - 1. 框图中每个模块都有一个**有意义的名称**，如：轮函数F，S盒，L扩散，FL函数等等。
      2. 框图中用到的运算符号都应在前面的符号及约定中给出。

说明或数学公式描述。

1. **密钥扩展算法**

同原始的算法一样

1. **附表及其他说明**

**S盒由python 生成**

1. **体会与建议**

**算法实现前期开发较慢，后期适应性不强，这种不成系列的数学性质代码，比起官方的代码会慢很多。建议一开始就作为一个一个完整的大型的项目一点一点地实现所有子模块，不然不具有开发价值**