AES /SM4 software implementation

1. **SM4**

1、加密过程概述：

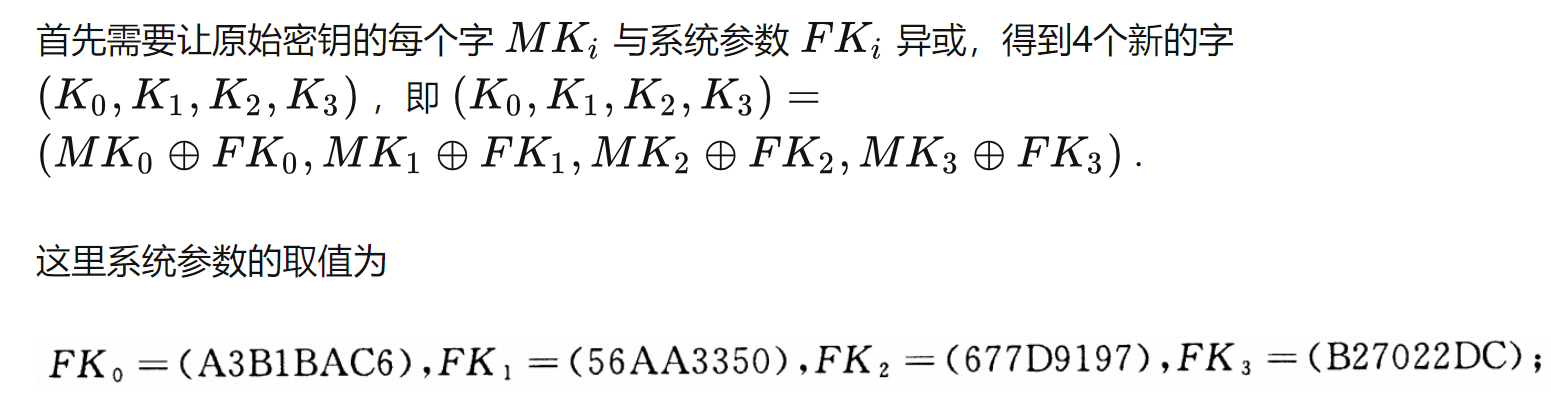
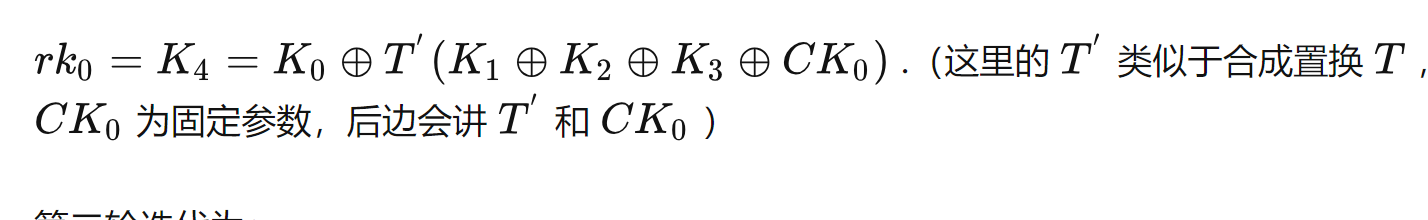
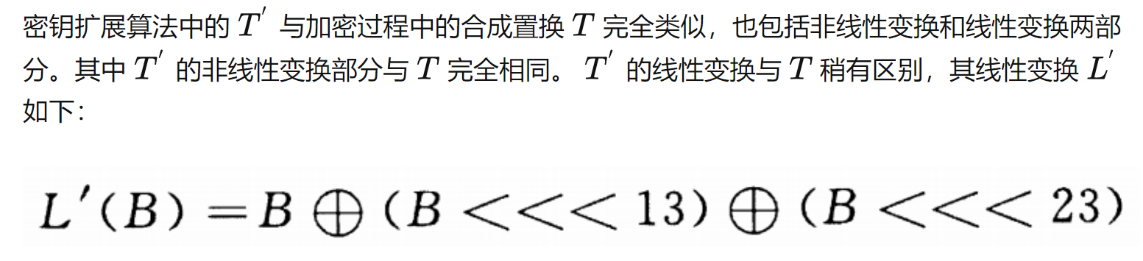
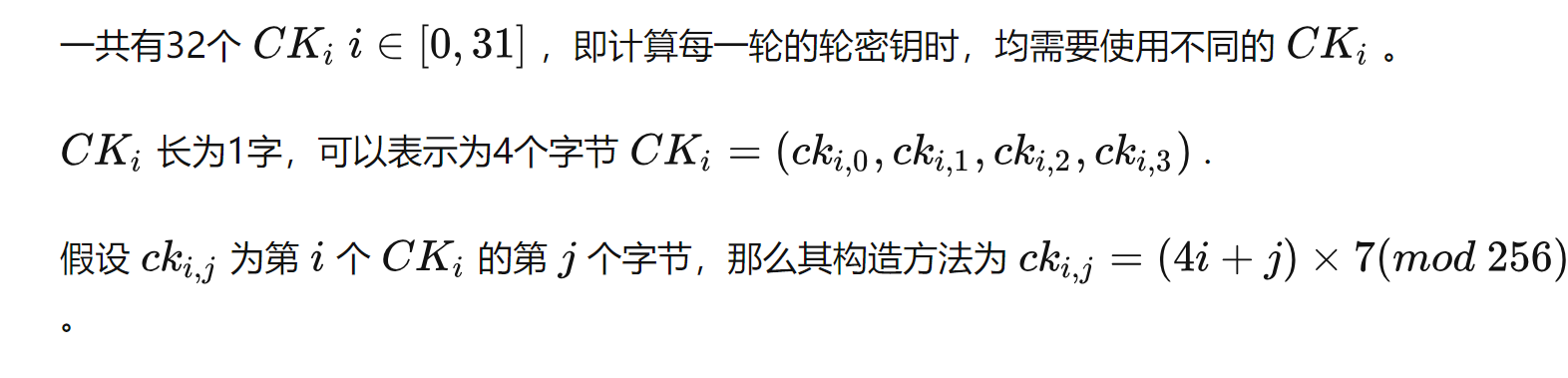
SM4的分组长度为4字，其输入是4字的明文经过加密后，得到的输出是4字的密文。加密过程分为两步，由32次轮迭代和1次反序变换组成。

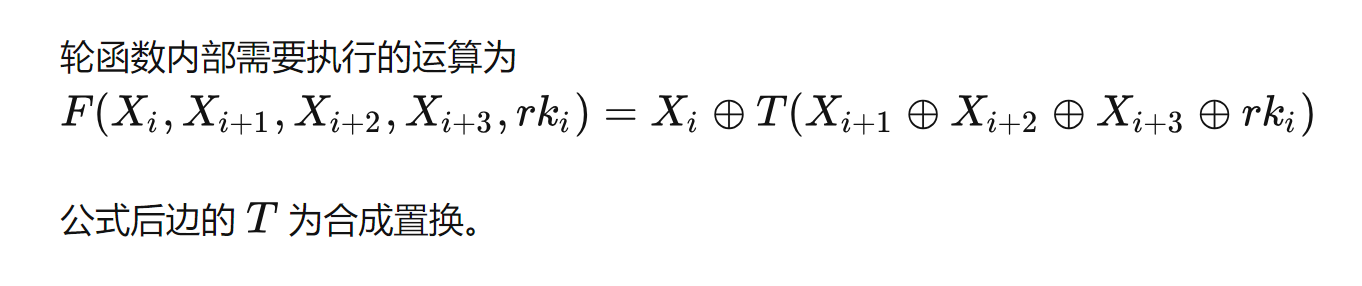
迭代：每一轮轮迭代都需要一个1字的轮密钥，总共需要32个轮密钥。每轮产生一个1字的结果，执行32轮，最终可以得到36个字

反序变换：将迭代最后得到的四个字进行反序，得到最终的密文

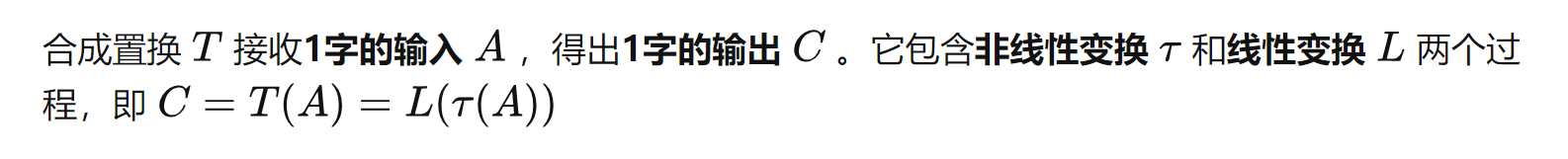
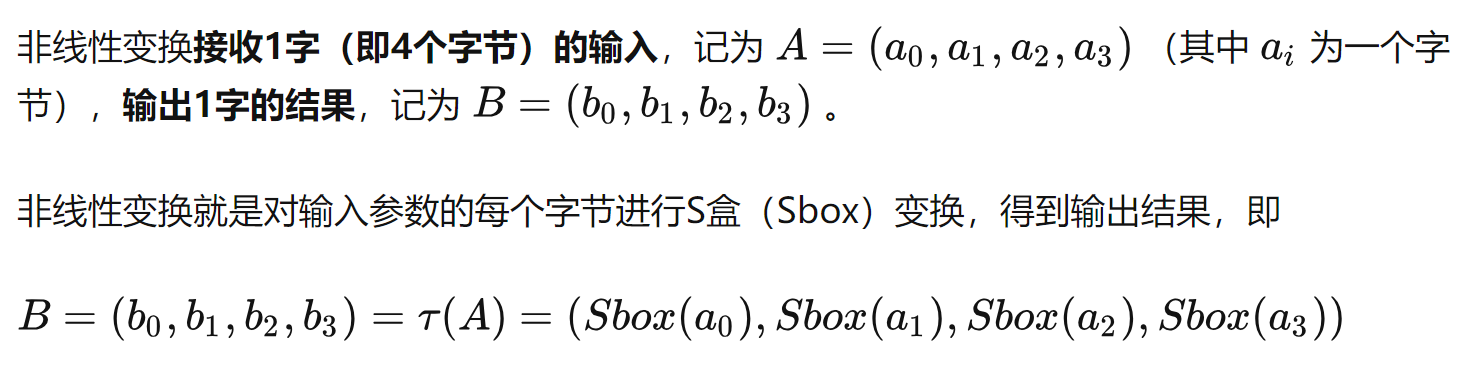
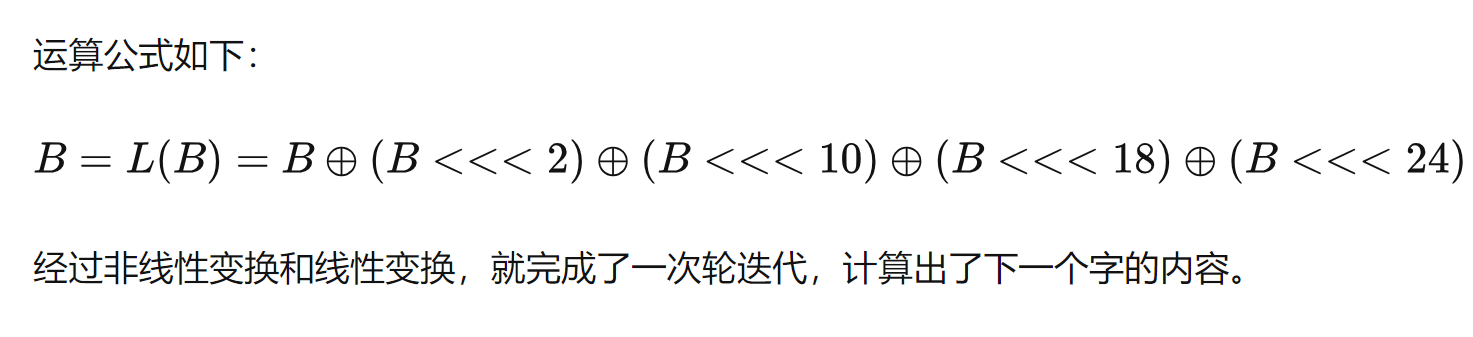
轮密钥生成（密钥扩展算法）：SM4密钥为128位（4字）→32个1字的轮密钥

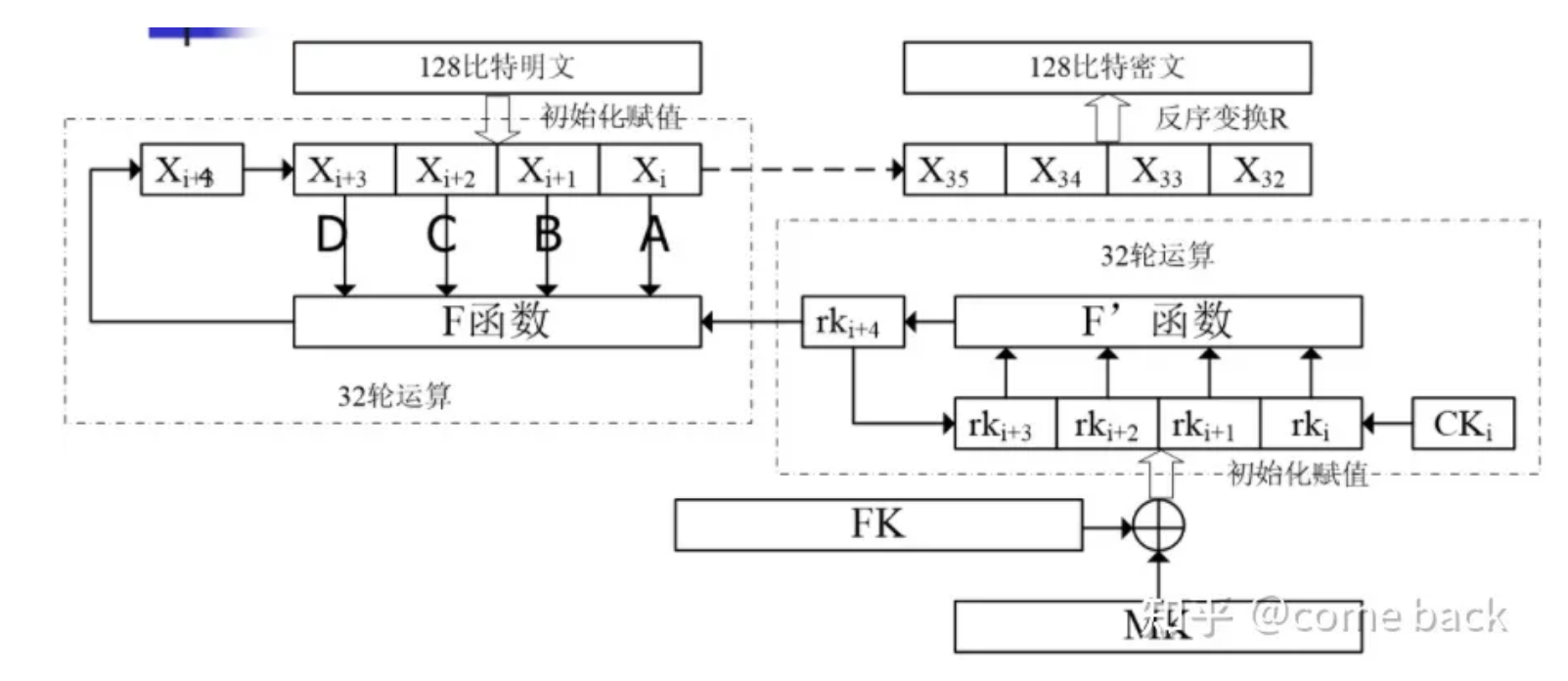
实现：

1. 密钥初始化
2. 迭代
3. 置换
4. CKi获取

轮函数：F（非线性+线性）

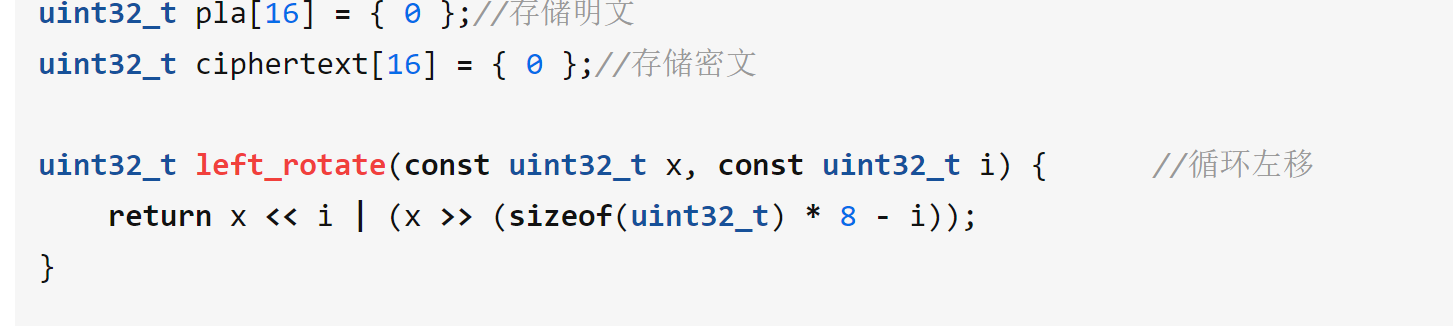
实现：

1. 合成置换（非线性）
2. 过s盒（非线性）
3. 循环移动，线性变换

加密总流程图：

算法实现：

重要部分：

明文与密钥输入；明文（密文）处理与分组；密钥扩展；T变换的实现：τ变换、L变换、L1变换；轮函数F的实现；循环左移的实现；密文变序；结果输出 加解密过程的转换（部分截图）



1. **AES**

AES是一种对称密钥加密算法，采用固定长度的密钥进行加密和解密，密钥长度可以是128位、192位或256位。

AES加密过程分为四个步骤：字节替换（SubBytes）、行移位（ShiftRows）、列混淆（MixColumns）和轮密钥加（AddRoundKey）。在每个步骤中，AES算法通过对数据块进行一系列复杂的变换来实现加密。

1、字节替换

字节替换就是简单的查表操作，AES定义了加密用的S盒和解密用的逆S盒来进行字节替换。

将每个字节替换为S盒中的相应字节来混淆数据。S盒是一个固定的256字节表，包含了一系列非线性变换。

2、行移位

将每行数据进行循环左移，使得数据在行内发生位移。这样可以增加数据的扩散性，增加了算法的强度。

3、列混淆

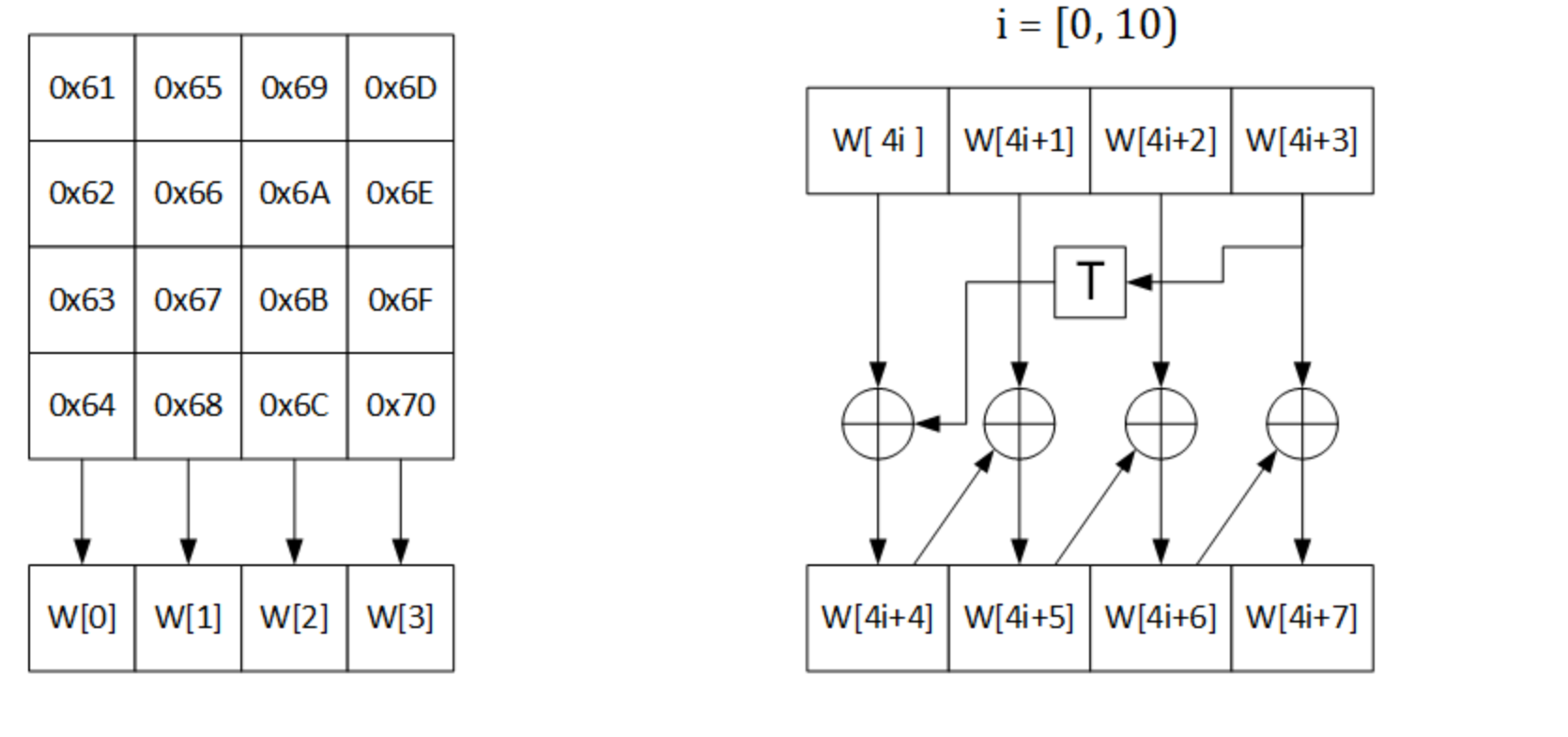
对数据矩阵的每列进行线性变换，进一步增加了算法的非线性性质。通过这个步骤，数据在不同列之间进行混淆，增加了加密的难度。

4、轮密钥加

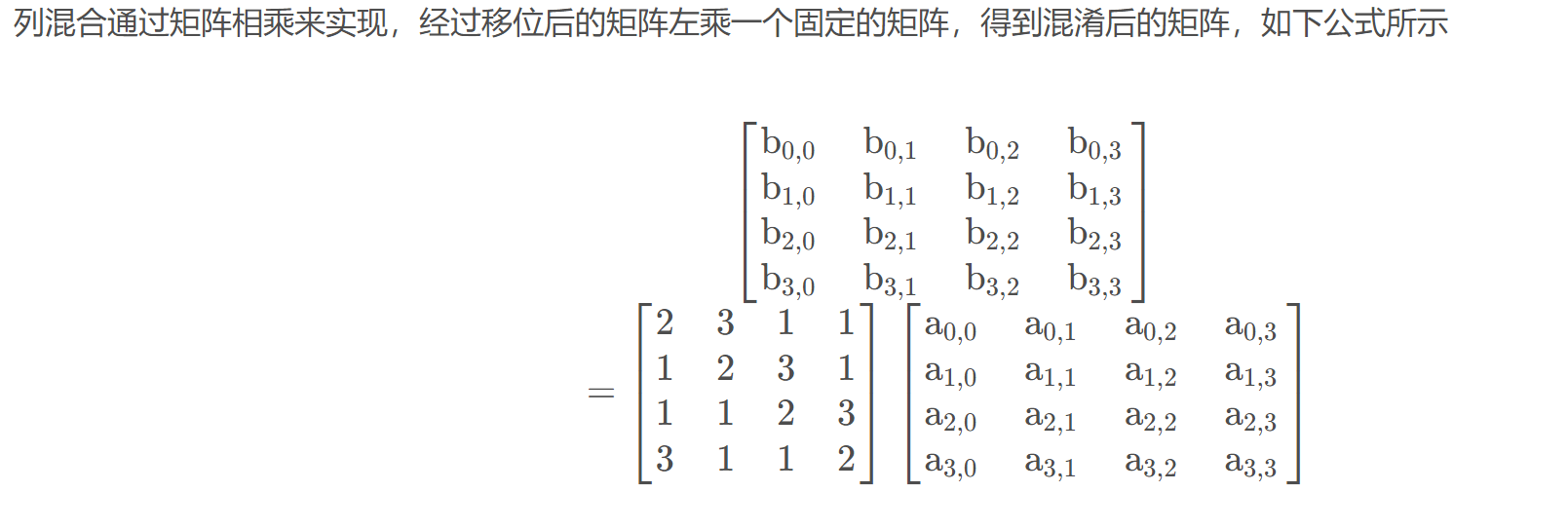
将轮密钥与数据进行异或运算，混淆数据并增加随机性。轮密钥是根据初始密钥扩展生成的，用于多轮加密或解密过程。每一轮加密都会使用不同的轮密钥，增加了算法的强度和随机性。

5、迭代

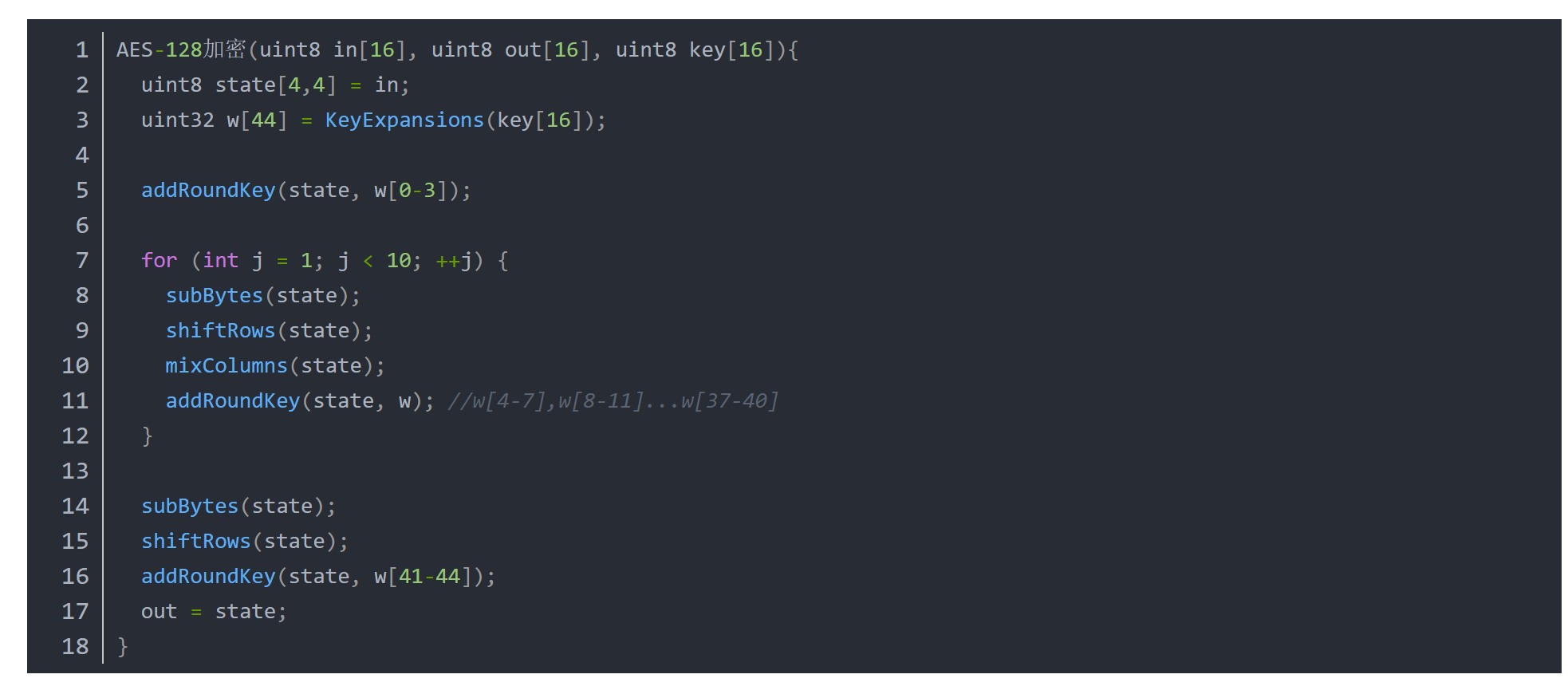
AES算法多次应用上述四个步骤，对数据进行加密，加密轮数与密钥长度有关。

密钥扩展：

实现：

1. 列混合
2. 轮秘钥加

是将数据与相应的秘钥逐位进行异或操作。上面已经讲到扩展后的秘钥结构为uint32\_t W[44]，轮秘钥加操作取16字节长度的秘钥，即取uint32\_t W[4]作为一个单元，把这个总长度为16字节的秘钥按照加密数据同样的格式写成uint8\_t b[4][4]二维数组矩阵，然后将此4x4矩阵与4x4的数据矩阵逐位进行异或操作。

1. 伪代码展示
2. **参考资料**

【1】AES算法原理https://blog.csdn.net/shaosunrise/article/details/80219950

【2】SM4加密算法<https://zhuanlan.zhihu.com/p/363900323>

【3】SM4实现方法https://zhuanlan.zhihu.com/p/379157716