SM4 加密可逆证明

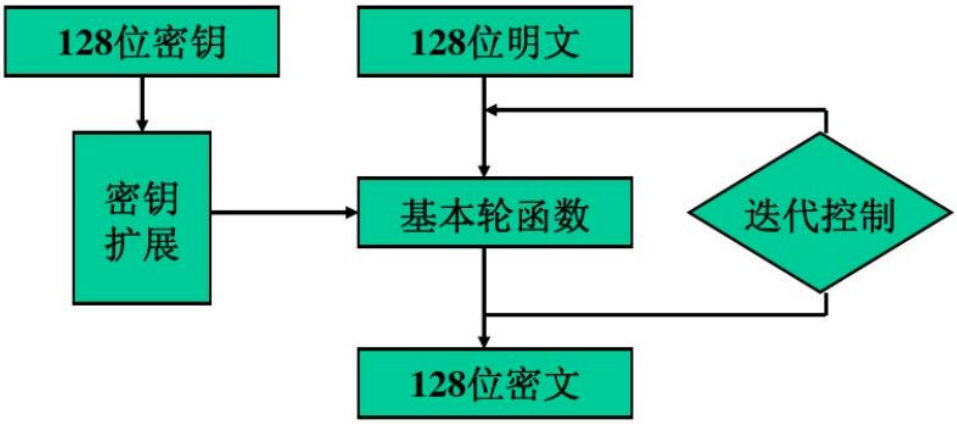
zhanxix

一、SM4 简介

2012 年 3 月，国家密码管理局正式公布了包含 SM4 分组密码算法在内的 6 项密码行业标准。

SM4 算法是一种分组密码算法，其分组长度为 128bit，密钥长度也为 128bit。SM4 加密算法与密钥扩展算法均采用 32 轮非线性迭代结构，以字（32 位）为单位进行加密运算，每一次迭代运算均为一轮变换函数 F。

SM4 算法加/解密算法的结构相同（对合运算），只是使用轮密钥相反，其中解密轮密钥是加密轮密钥的逆序。



二、轮函数 F

本算法采用非线性迭代结构，以字为单位进行加密运算，称一次迭代运算为一轮变换。

轮密钥表示为($rk_0, rk_1, \cdots, rk_{31}$)，其中 rk_i(i=0,⋯,31)为字。轮密钥由加密密钥生成。

设输入为(X_0, X_1, X_2, X_3)∈(Z_2^{32})^4，轮密钥为 rk∈Z_2^{32}，则轮函数 F 为：

$$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk)$$

其中 T 是一个可逆变换，由非线性变换τ和线性变换 L 复合而成。

τ由 4 个并行的 S 盒构成；非线性变换τ的输出是线性变换 L 的输入，设输入为 B，输出为 C，则 C = L(B) = B ⊕ (B <<< 2) ⊕ (B <<< 10) ⊕ (B <<< 18) ⊕ (B <<< 24)。

三、加密算法

定义反序变换 R 为：R(A_0, A_1, A_2, A_3)=(A_3, A_2, A_1, A_0)。

明文输入为(X_0, X_1, X_2, X_3)∈(Z_2^{32})^4，密文输出为(Y_0, Y_1, Y_2, Y_3)∈(Z_2^{32})^4。

则本算法的加密变换为：

$$X_{i+4}=F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)=X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i),\ i=0,1,\cdots,31$$

最后进行反序变换：

$$(Y_0, Y_1, Y_2, Y_3)=R(X_{32}, X_{33}, X_{34}, X_{35})=(X_{35}, X_{34}, X_{33}, X_{32})$$

从而得到密文。

四、解密算法（加密可逆）

SM4 算法是对合的，因此解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序。

加密时轮密钥的使用顺序为：$(rk_0, rk_1, \cdots, rk_{31})$。

解密时轮密钥的使用顺序为：$(rk_{31}, rk_{30}, \cdots, rk_0)$。

定义反序变换 R 为：$R(A_0, A_1, A_2, A_3)=(A_3, A_2, A_1, A_0)$。

密文输入为$(Y_0, Y_1, Y_2, Y_3) \in (Z_2^{32})^4$，明文输出为$(X_0, X_1, X_2, X_3) \in (Z_2^{32})^4$。

有$(X_{35}, X_{34}, X_{33}, X_{32})=(Y_0, Y_1, Y_2, Y_3)$。

于是有解密变换：

$$X_i=F(X_{i+4}, X_{i+3}, X_{i+2}, X_{i+1}, rk_i)=X_{i+4} \oplus T(X_{i+3} \oplus X_{i+2} \oplus X_{i+1} \oplus rk_i),\ i=31,\cdots,1,0$$

再进行反序变换：

$$(X_0, X_1, X_2, X_3)=R(X_3, X_2, X_1, X_0)$$

由此，可以进行解密，得出明文。