SM4 加密可逆证明

一． SM4 加密算法背景知识简介

1 输入明文：（M_0,M_1,M_2,M_3）=（X_0,X_1,X_2,X_3），128bit，四个字

2 输入轮密钥：rk_i, i=0,1,2,3,….31，共 32 个密钥

3 输出密文：（Y_0,Y_1,Y_2,Y_3）,共 128bit,四个字。

4 算法结构：轮函数 32 轮迭代，每轮使用一个轮密钥。

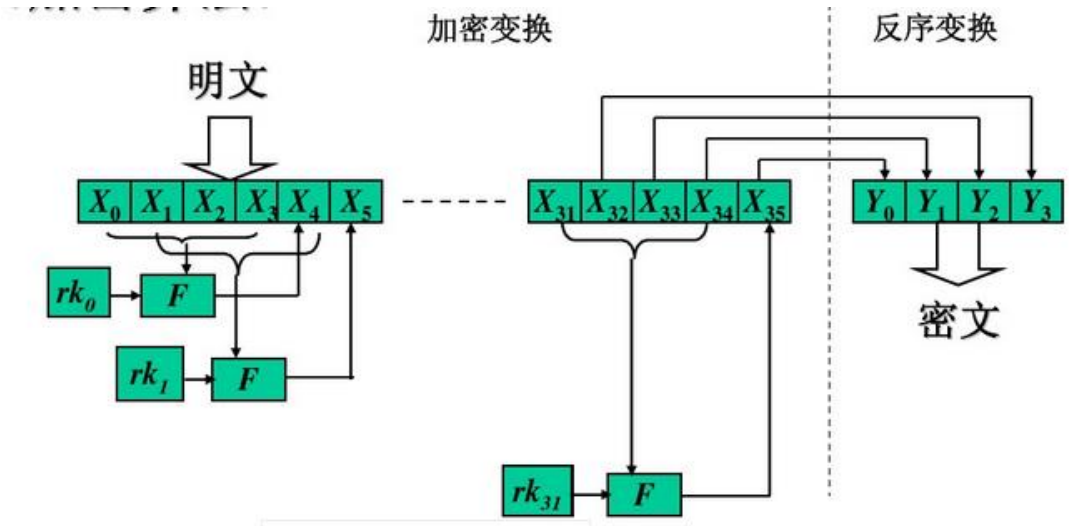
5 加密算法：

① 加密变换：$X_{i+4}=F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$

$= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i)$，$i = 0,1\ldots31$

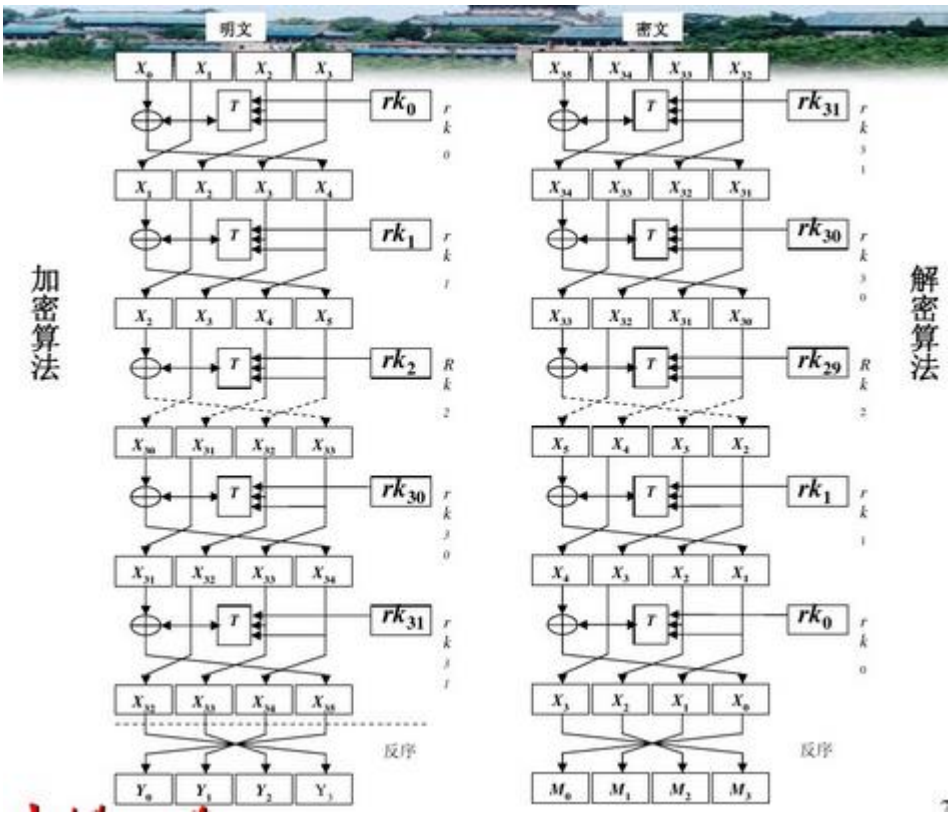
② 反序变换：$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32})$

流程图：



二． SM4 加密可逆证明：

加密、解密框图：



可逆性证明：

根据加密框图，SM4 的加密过程的数据变化：

(X_0,X_1,X_2,X_3)->(X_1,X_2,X_3,X_4)->(X_2,X_3,X_4,X_5)->...->$(X_{32},X_{33},X_{34},X_{35})$

->$(X_{35},X_{34},X_{33},X_{32})$ = (Y_0,Y_1,Y_2,Y_3)(最后一步变换为反序)

根据解密框图，密文(Y_0,Y_1,Y_2,Y_3)解密过程数据变化为：

$(X_{35},X_{34},X_{33},X_{32})$ -> $(X_{34},X_{33},X_{32},X_{31})$ -> $(X_{33},X_{32},X_{31},X_{30})$ ->...->

(X_3,X_2,X_1,X_0)->(X_0,X_1,X_2,X_3)(最后一步变换为反序)

所以可以得到:

$SM4^{-1}(SM4(X_0,X_1,X_2,X_3)) = (X_0,X_1,X_2,X_3)$

故 SM4 是可逆的。