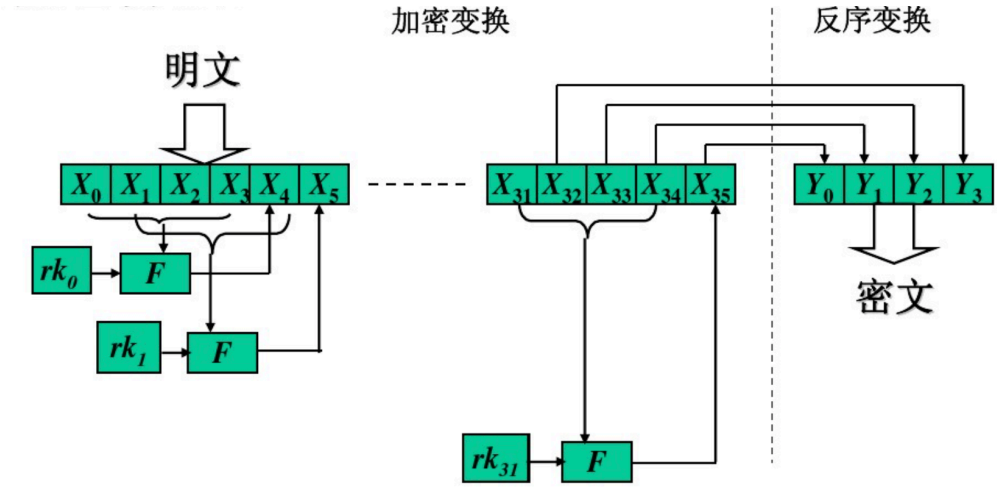
# Sm4 可逆证明

## 1901210447 刘嘉欣

1. 算法加密流程




其中:

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

因此，$(X_0, X_1, X_2, X_3)$-> $(X_1, X_2, X_3, X_4)$->⋯-> $(X_{35}, X_{34}, X_{33}, X_{32}) = (Y_0, Y_1, Y_2, Y_3,)$

2. 算法解密流程

Sm4 算法的解密流程和加密流程是一样的，不同之处仅在于轮密钥的使用顺序，与加密时的顺序相反。

$$X_j = F(X_{j+4}, X_{j+3}, X_{j+2}, X_{j+1}, rk_i)$$
$$= X_{j+4} \oplus T(X_{j+3} \oplus X_{j+2} \oplus X_{j+1} \oplus rk_j))$$

当 j=31 时：

$$X_{31} = F(X_{35}, X_{34}, X_{33}, X_{32}, rk_{31}) = X_{35} \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31}))$$

而在加密阶段，

$$X_{35} = F(X_{31}, X_{32}, X_{33}, X_{34}, rk_{31}) = X_{31} \oplus T(X_{32} \oplus X_{33} \oplus X_{34} \oplus rk_{31}))$$

因此，解密阶段：

$X_{31} = X_{31} \oplus T(X_{32} \oplus X_{33} \oplus X_{34} \oplus rk_{31})) \oplus T(X_{34} \oplus X_{33} \oplus X_{32} \oplus rk_{31})) = X_{31}$

由此可知，在解密阶段一轮轮解密下来的 X 与加密阶段对应的 X 相同，即：

$(X_{35}, X_{34}, X_{33}, X_{32})$-> $(X_{34}, X_{33}, X_{32}, X_{31})$->…-> $(X_3, X_2, X_1, X_0)$

将结果逆转后即可得明文$(X_0, X_1, X_2, X_3)$