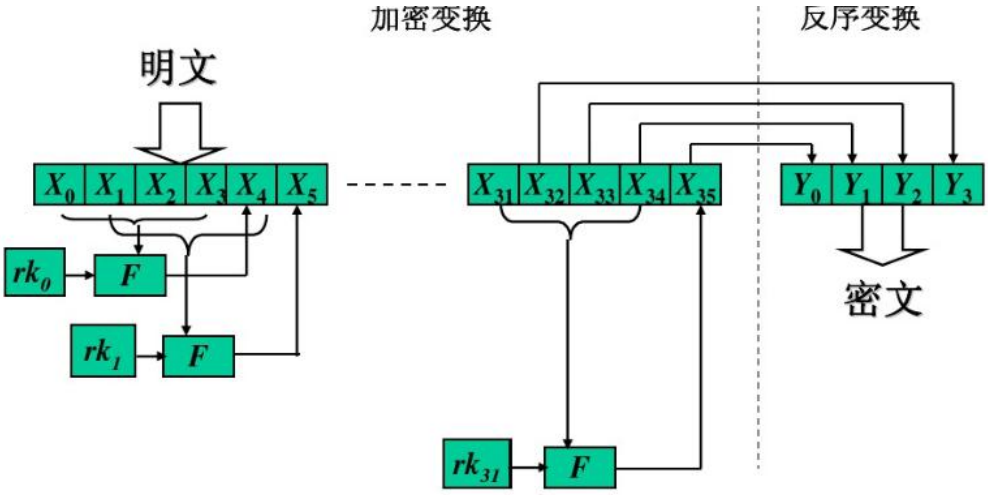
SM4 可逆性证明

加密过程:对于明文(M_1，M_2，M_3，M_4),和秘钥（rK_i），i∈（0,1,2……31），SM4 对这样的 4 字节明文进行 32 轮的轮函数

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$$
$$= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), i = 0,1,2\ldots\ldots31$$



迭代得到（X_{32}，X_{33}，X_{34}，X_{35}），在经过反序操作得到密文（Y_1，Y_2，Y_3，Y_4），

解密操作：首先对密文（Y_1，Y_2，Y_3，Y_4）反序操作得到（X_{32}，X_{33}，X_{34}，X_{35}）

由于异或运算本身可逆，即对于 X⊕K=Y 有 Y⊕K=X，故逆序使用轮秘钥 rk_i (i=31,30……,0)

$$X_i = F(X_{i+4}, X_{i+3}, X_{i+2}, X_{i+1}, rk_i)$$
$$= X_{i+4} \oplus T(X_{i+3} \oplus X_{i+2} \oplus X_{i+1} \oplus rk_i), i = 31,30,\ldots\ldots1,0$$

得到(X_3，X_2，X_1，X_0),再进过反序操作可以得到明文（M_1，M_2，M_3，M_4）

可见由密文可以解得明文，故 SM4 算法可逆。