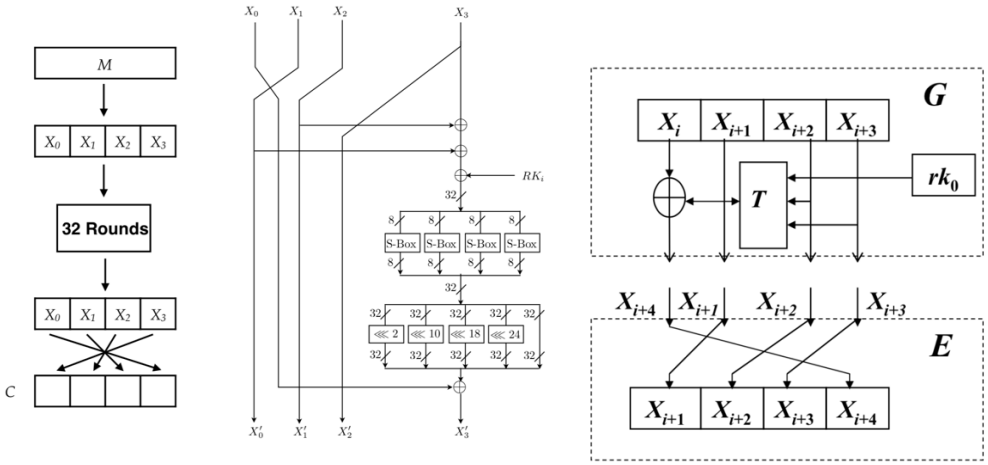
SM4 可逆性证明

1901210582 张津婵

如图所示，SM4 加密的轮函数分为加密函数 G 和数据交换 E，加密函数 G 进行加密处理，数据交换 E 进行数据顺序交换，而且 G 和 E 都具有对合性。



其轮函数为：

$$F_i = G_i E$$

根据 SM4 加密过程，可把加密过程写成：

$$SM4 = G_0 E G_1 E ... G_{30} E G_{31} R$$

根据 SM4 解密过程，可把解密过程写成：

$$SM4^{-1} = G_{31} E G_{30} E ... G_1 E G_0 R$$

比较 SM4 的加密和解密过程可知，加解密运算相同，只有密钥使用顺序不同

SM4 加密过程的数据变化（最后一步变换为反序）：

$$(X_0, X_1, X_2, X_3) \to (X_1, X_2, X_3, X_4) \to (X_2, X_3, X_4, X_5) \to ... \to (X_{32}, X_{33}, X_{34}, X_{35})$$
$$\to (X_{35}, X_{34}, X_{33}, X_{32}) = (Y_0, Y_1, Y_2, Y_3)$$

密文解密过程数据变化为（最后一步变换为反序）：

$$(Y_0, Y_1, Y_2, Y_3) \to (X_{35}, X_{34}, X_{33}, X_{32}) \to (X_{34}, X_{33}, X_{32}, X_{31}) \to (X_{33}, X_{32}, X_{31}, X_{30}) \to ... \to$$
$$(X_3, X_2, X_1, X_0) \to (X_0, X_1, X_2, X_3)$$

因此

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

所以，SM4 是可逆的