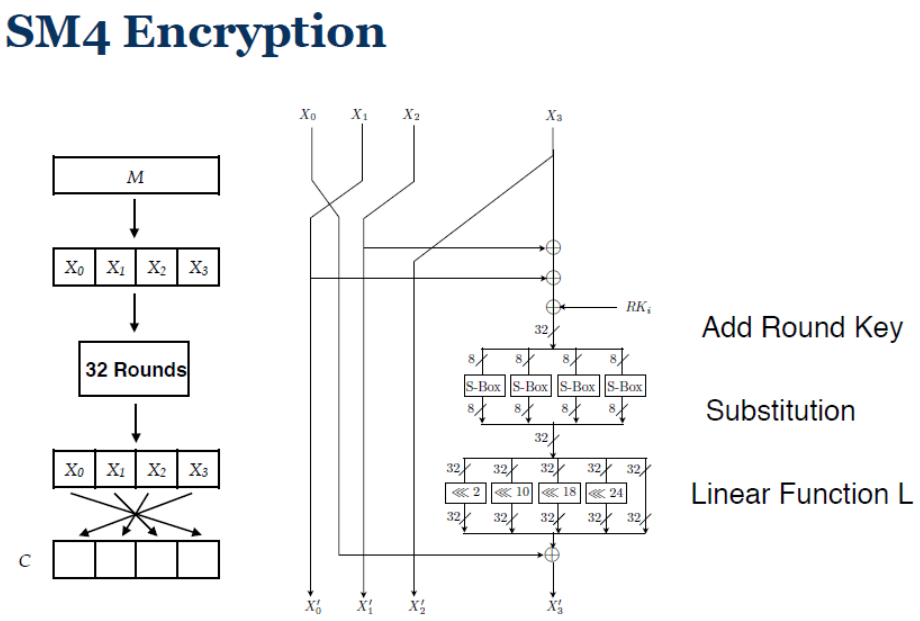
SM4 加密可逆性证明

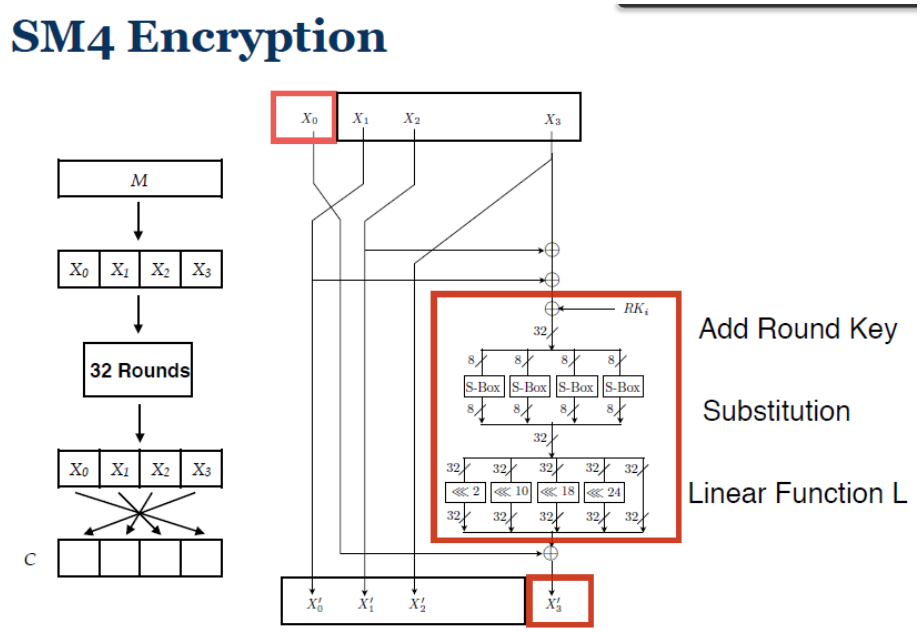
——叶明聪

流程图:

加密过程：



解密过程：



公式推导:

1.根据加密的图解，SM4 的解密过程中的数据如下方式变化：

(X_0, X_1, X_2, X_3)-> (X_1, X_2, X_3, X_4)-> (X_2, X_3, X_4, X_5)->…$(X_{32}, X_{33}, X_{34}, X_{35})$-> $(X_{35}, X_{34}, X_{33}, X_{32})= (Y_0, Y_1, Y_2, Y_3)$

上始终最后一步$(X_{35}, X_{34}, X_{33}, X_{32})$是反序.

2.根据上面的解密的图解，密文(Y_0, Y_1, Y_2, Y_3)在解解密过程中的变换为：

$(X_{35}, X_{34}, X_{33}, X_{32})$-> $(X_{34}, X_{33}, X_{32}, X_{31})$-> $(X_{33}, X_{32}, X_{31}, X_{30})$->…$(X_3, X_2, X_1, X_0)$-> (X_0, X_1, X_2, X_3)

最后面一步(X_3, X_2, X_1, X_0)-> (X_0, X_1, X_2, X_3)是反序。

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

得证