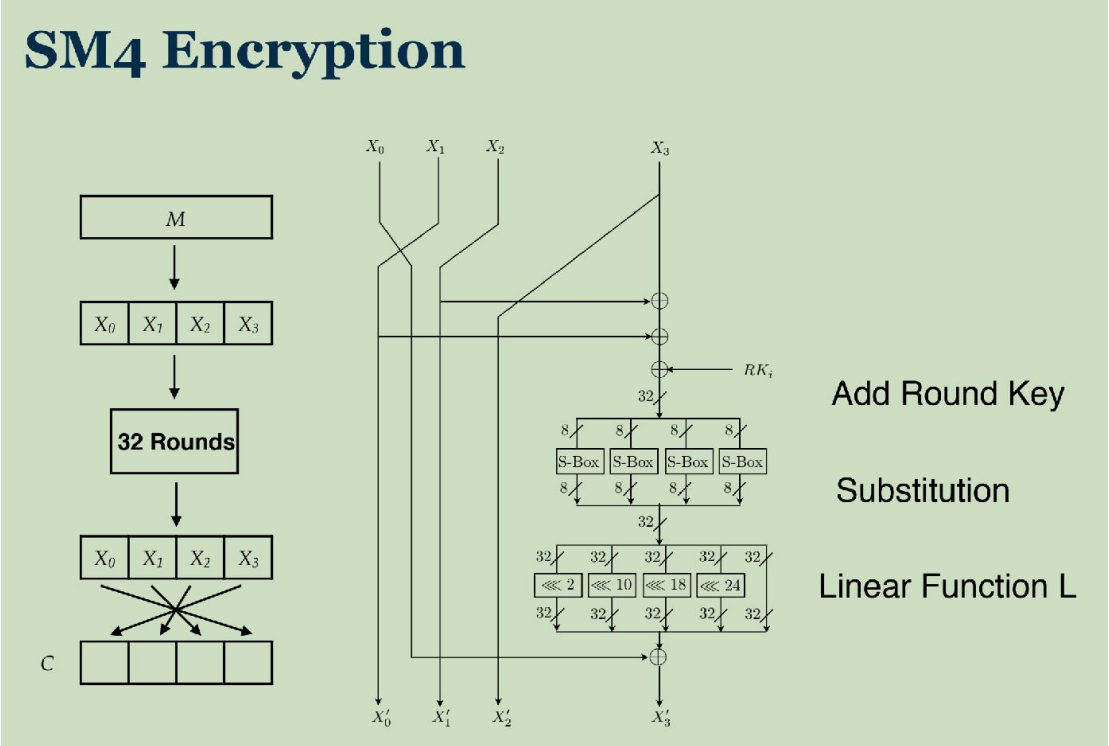
SM4 单次加密 128bit 的消息，首先将这 128bit 分成 4 个 32bit 的字 X0,X1,X2,X3。加密过程如下



加密的转换过程为：

X0’=X1　X1’=X2　X2’=X3　X3’=S&L(X1^X2^X3^RKi)^X0

解密时：已知 X0’、X1’、X2’、X3’和轮密钥 RKi

X1=X0’　X2=X1’　X3=X2’　X0=S&L(X1^X2^X3^RKi)^X3’　（利用了异或的可逆性）

SM4 可逆 证明结束