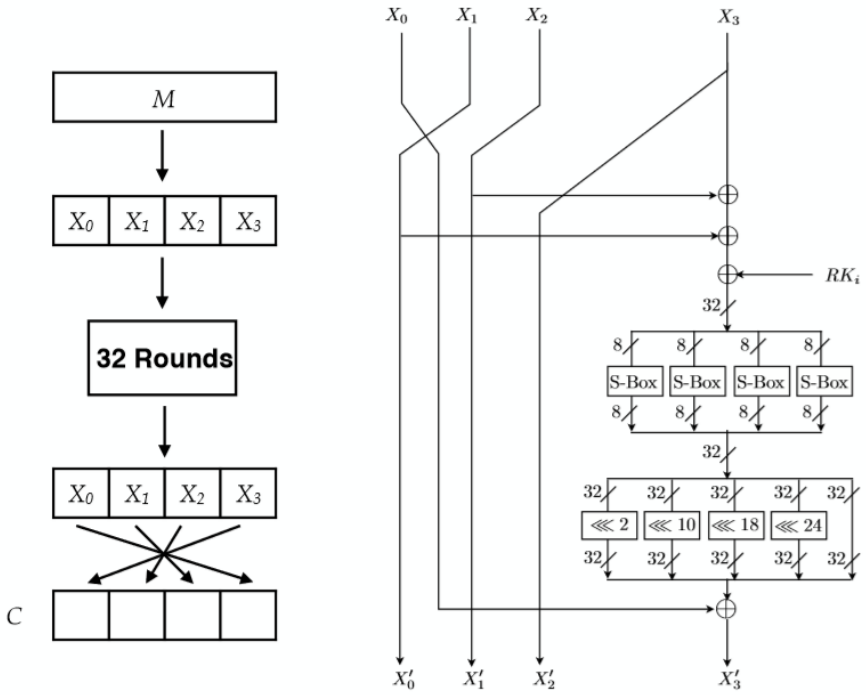
第二次作业（第 1 题：推导）

刘曼姝 1901210656　2019.10.24

证明 SM4 加密过程是可逆的：

1、SM4 加密过程：

流程图如下：



① **分块**：将 128bit 的消息明文块 M 分成 4 个 32bit 的小块：$XE_{0,0}$、$XE_{1,0}$、$XE_{2,0}$、$XE_{3,0}$。

② **32 轮在轮函数作用下的变换**：用 $XE_{0,i}$ 表示第 i 轮加密得到的第 1 个小块、$XE_{1,i}$ 表示第 i 轮加密得到的第 2 个小块、$XE_{2,i}$ 表示第 i 轮加密得到的第 3 个小块、$XE_{3,i}$ 表示第 i 轮加密得到的第 4 个小块、RK_i 表示第 i 轮的轮密钥，设轮函数为 F，则：

$$XE_{0,i}=XE_{1,i-1};$$

$$XE_{1,i}=XE_{2,i-1};$$

$$XE_{2,i}=XE_{3,i-1};$$

$$XE_{3,i}=XE_{0,i-1}\oplus F(XE_{1,i-1}\oplus XE_{2,i-1}\oplus XE_{3,i-1}\oplus RK_i);$$

因为“⊕”（异或）运算具有性质：$(a\oplus b)\oplus c=a\oplus(b\oplus c)$、$a\oplus a=0$、$a\oplus 0=a$，故可

做变换：

$$XE_{3,i} \oplus F(XE_{1,i-1} \oplus XE_{2,i-1} \oplus XE_{3,i-1} \oplus RK_i)$$

$$=(XE_{0,i-1} \oplus F(XE_{1,i-1} \oplus XE_{2,i-1} \oplus XE_{3,i-1} \oplus RK_i)) \oplus F(XE_{1,i-1} \oplus XE_{2,i-1} \oplus XE_{3,i-1} \oplus RK_i)$$

$$=XE_{0,i-1} \oplus (F(XE_{1,i-1} \oplus XE_{2,i-1} \oplus XE_{3,i-1} \oplus RK_i) \oplus F(XE_{1,i-1} \oplus XE_{2,i-1} \oplus XE_{3,i-1} \oplus RK_i))$$

$$=XE_{0,i-1} \oplus 0$$

$$=XE_{0,i-1};$$

故：

$$XE_{1,i-1}=XE_{0,i};$$

$$XE_{2,i-1}=XE_{1,i};$$

$$XE_{3,i-1}=XE_{2,i};$$

$$XE_{0,i-1}=XE_{3,i} \oplus F(XE_{1,i-1} \oplus XE_{2,i-1} \oplus XE_{3,i-1} \oplus RK_i)$$

$$=XE_{3,i} \oplus F(XE_{0,i} \oplus XE_{1,i} \oplus XE_{2,i} \oplus RK_i)。$$

③ **置换**：设密文 $C=XE'_{0,32} \| XE'_{1,32} \| XE'_{2,32} \| XE'_{3,32}$，则：

$$XE'_{0,32}=XE_{3,32};$$

$$XE'_{1,32}=XE_{2,32};$$

$$XE'_{2,32}=XE_{1,32};$$

$$XE'_{3,32}=XE_{0,32}。$$

2、SM4 解密过程：

① **置换**：设密文 $C=XD'_{0,1} \| XD'_{1,1} \| XD'_{2,1} \| XD'_{3,1}$，用 $XD_{0,i}$ 表示第 i 轮解密得到的第 1 个小块、$XD_{1,i}$ 表示第 i 轮解密得到的第 2 个小块、$XD_{2,i}$ 表示第 i 轮解密得到的第 3 个小块、$XD_{3,i}$ 表示第 i 轮解密得到的第 4 个小块，则：

$$XD_{0,0}=XE_{0,32}=XE'_{3,32}=XD'_{3,0};$$

$$XD_{1,0}=XE_{1,32}=XE'_{2,32}=XD'_{2,0};$$

$$XD_{2,0}=XE_{2,32}=XE'_{1,32}=XD'_{1,0};$$

$$XD_{3,0}=XE_{3,32}=XE'_{0,32}=XD'_{0,0}。$$

② **32 轮在轮函数作用下的变换**：由 1、②中推导可得：

$$XD_{1,i}=XE_{1,32-i}=XE_{0,33-i}=XD_{0,i-1};$$

$$XD_{2,i}=XE_{2,32-i}=XE_{1,33-i}=XD_{1,i-1};$$

$$XD_{3,i}=XE_{3,32-i}=XE_{2,33-i}=XD_{2,i-1};$$

$$XD_{0,i}=XE_{0,32-i}=XE_{3,33-i}\oplus F(XE_{0,33-i}\oplus XE_{1,33-i}\oplus XE_{2,33-i}\oplus RK_{33-i})$$

$$=XD_{3,i-1}\oplus F(XD_{0,i-1}\oplus XD_{1,i-1}\oplus XD_{2,i-1}\oplus RK_{33-i})$$

$$=XD_{3,i-1}\oplus F(XD_{1,i}\oplus XD_{2,i}\oplus XD_{3,i}\oplus RK_{33-i});$$

则得证：此解密过程成立，且是加密过程的逆过程，只是密钥的使用顺序相反，即 SM4 加密过程是可逆的。