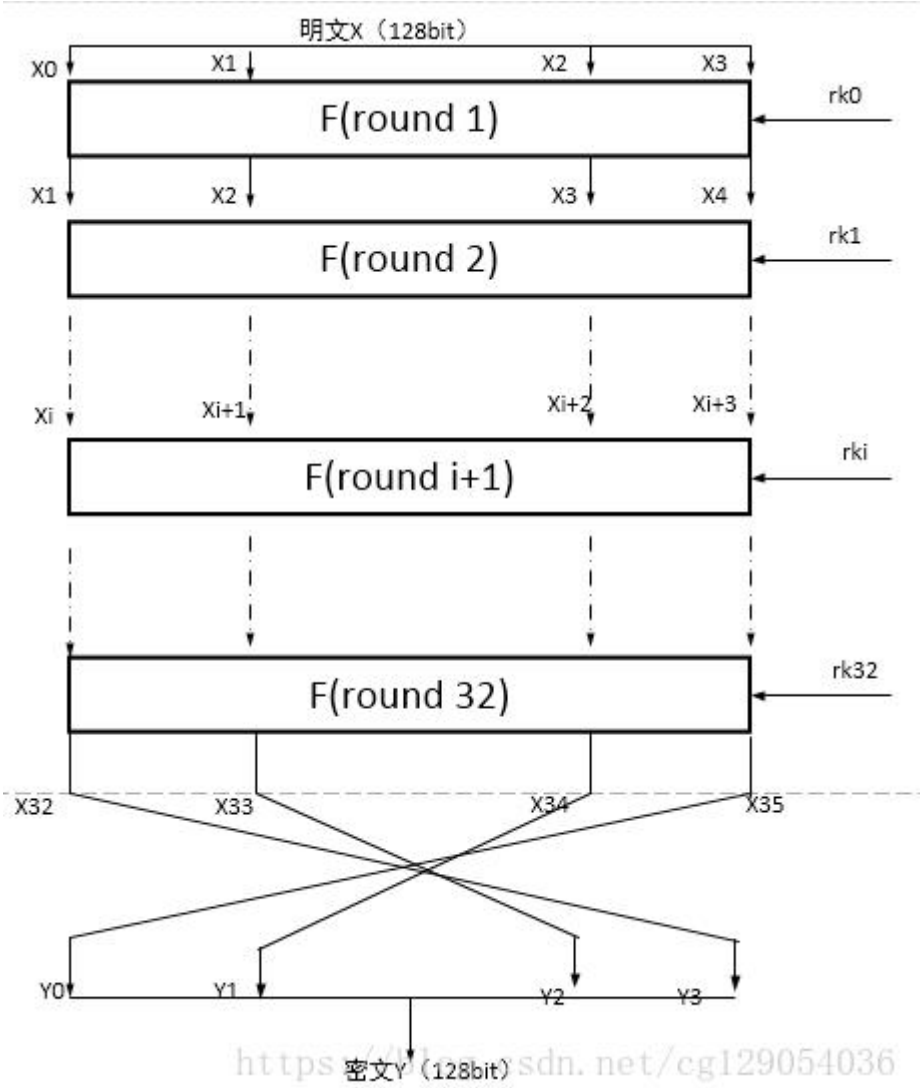
应用密码学 SM4 可逆性证明

1901210443 刘高原

1. SM4 算法结构图



2.轮函数

整体的加密函数为：

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

其中 T 为一个合成置换，由非线性变换和线性变换复合而成。

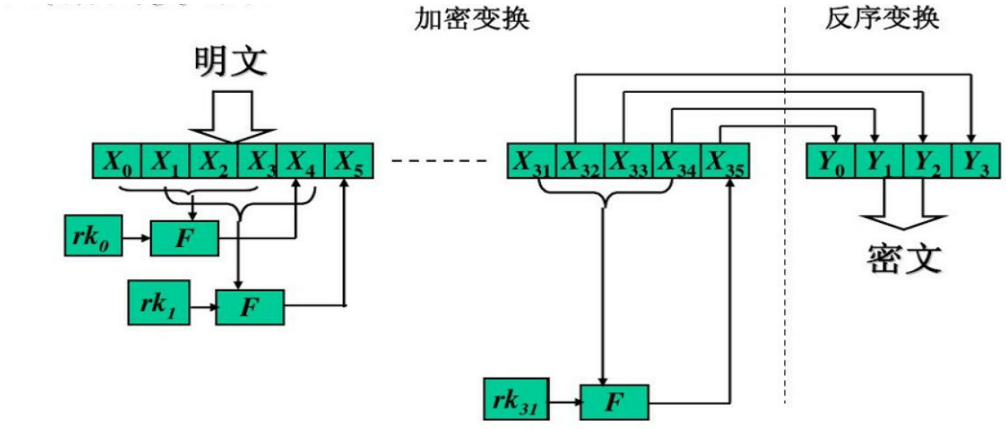
非线性变换由 4 个平行的 S 盒构成，S 盒的数据均采用 16 进制。

线性变换公式如下，其中 B 为非线性变换得到的字

$$C=L(B)=B\oplus(B<<2)\oplus(B<<10)\oplus(B<<18)\oplus(B<<24)$$

3.加密过程

- 输入明文:$(M_0, M_1, M_2, M_3)=(X_0, X_1, X_2, X_3)$, 128位，四个字。
- 输入轮密钥：rk_i，i=0,1,…,31，共32个轮密钥。
- 输出密文：（Y_0，Y_1，Y_2，Y_3），128位，四个字。
- 算法结构：轮函数32轮迭代，每轮使用一个轮密钥。
- 加密算法：
  - ① 加密变换：$X_{i+4}=F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$
    $=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)$，$i=0,1\ldots31$
  - ② 反序变换：$(Y_0, Y_1, Y_2, Y_3)=(X_{35}, X_{34}, X_{33}, X_{32})$

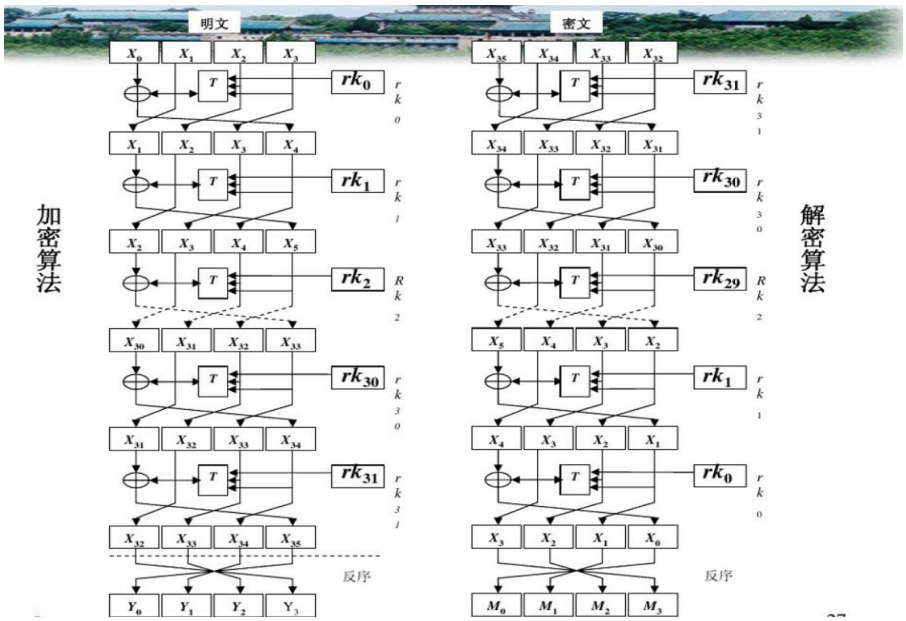


4.解密过程

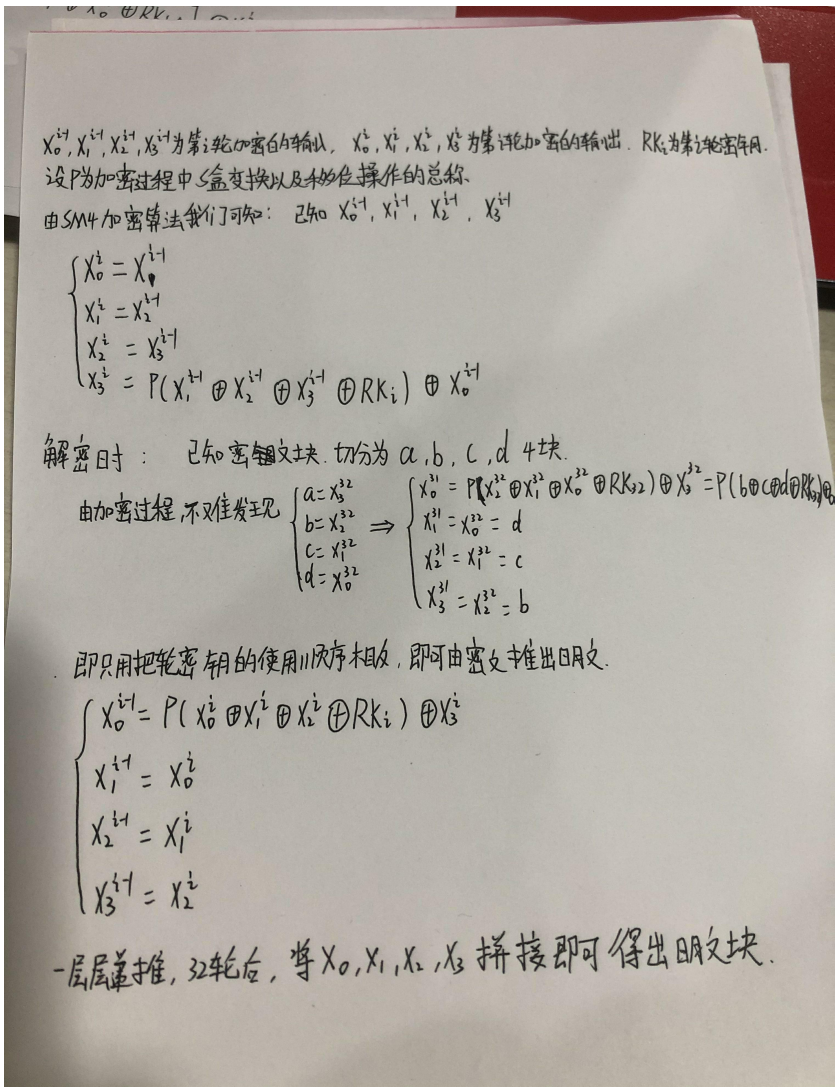
- SM4密码算法是对合的，因此解密与加密算法相同，只是轮密钥的使用顺序相反。
- 输入密文：$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32})$
- 输入轮密钥：rk_i，i =31,30，…,1，0
- 输出明文：(X_0, X_1, X_2, X_3)
- 算法：轮函数的32轮迭代，每轮使用一个轮密钥。
- 解密算法：用符号X描述
  - 解密变换：$X_i = F(X_{i+4}, X_{i+3}, X_{i+2}, X_{i+1}, rk_i)$
    $= X_{i+4} \oplus T(X_{i+3} \oplus X_{i+2} \oplus X_{i+1} \oplus rk_i), i=31,\ldots 1,0$
  - 反序变换：$(X_3, X_2, X_1, X_0) = (M_0, M_1, M_2, M_3)$

5.可逆性

- 可逆性
- 根据加密框图，SM4的加密过程的数据变化：
  $(X_0, X_1, X_2, X_3) \rightarrow (X_1, X_2, X_3, X_4) \rightarrow (X_2, X_3, X_4, X_5) \rightarrow \ldots \rightarrow (X_{32}, X_{33}, X_{34}, X_{35}) \rightarrow (X_{35}, X_{34}, X_{33}, X_{32}) = (Y_0, Y_1, Y_2, Y_3)$。
  - 其中最后一步变换为反序。
- 根据解密框图，密文(Y_0, Y_1, Y_2, Y_3)解密过程数据的变化：
  $(X_{35}, X_{34}, X_{33}, X_{32}) \rightarrow (X_{34}, X_{33}, X_{32}, X_{31}) \rightarrow (X_{33}, X_{32}, X_{31}, X_{30}) \rightarrow \ldots \rightarrow (X_3, X_2, X_1, X_0) \rightarrow (X_0, X_1, X_2, X_3)$。
  - 其中最后一步变换为反序。
- $SM4^{-1}(SM4(X_0, X_1, X_2, X_3)) = (X_0, X_1, X_2, X_3)$
- 所以SM4是可逆的。


明文
密文
加密算法
解密算法
反序
反序

手写证明如下：


$X_0^{i+1}, X_1^{i+1}, X_2^{i+1}, X_3^{i+1}$为第$i$轮加密的输入，$X_0^i, X_1^i, X_2^i, X_3^i$为第$i$轮加密的输出，$RK_i$为第$i$轮密钥。
设P为加密过程中S盒变换以及4次位操作的总称。
由SM4加密算法我们可知：已知 $X_0^{i+1}, X_1^{i+1}, X_2^{i+1}, X_3^{i+1}$
$\begin{cases} X_0^i = X_1^{i+1} \\ X_1^i = X_2^{i+1} \\ X_2^i = X_3^{i+1} \\ X_3^i = P(X_1^{i+1} \oplus X_2^{i+1} \oplus X_3^{i+1} \oplus RK_i) \oplus X_0^{i+1} \end{cases}$
解密时：已知密钥文块，切分为 a, b, c, d 4块。
由加密过程，不难发现 $\begin{cases} a = X_3^{32} \\ b = X_2^{32} \\ c = X_1^{32} \\ d = X_0^{32} \end{cases} \Rightarrow \begin{cases} X_0^{31} = P(X_2^{32} \oplus X_1^{32} \oplus X_0^{32} \oplus RK_{32}) \oplus X_3^{32} = P(b \oplus c \oplus d \oplus RK_{32}) \oplus a \\ X_1^{31} = X_0^{32} = d \\ X_2^{31} = X_1^{32} = c \\ X_3^{31} = X_2^{32} = b \end{cases}$
即只用把轮密钥的使用顺序相反，即可由密文推出明文。
$\begin{cases} X_0^{i+1} = P(X_0^i \oplus X_1^i \oplus X_2^i \oplus RK_i) \oplus X_3^i \\ X_1^{i+1} = X_0^i \\ X_2^{i+1} = X_1^i \\ X_3^{i+1} = X_2^i \end{cases}$
一层层递推，32轮后，等 X_0, X_1, X_2, X_3 拼接即可得出明文块。