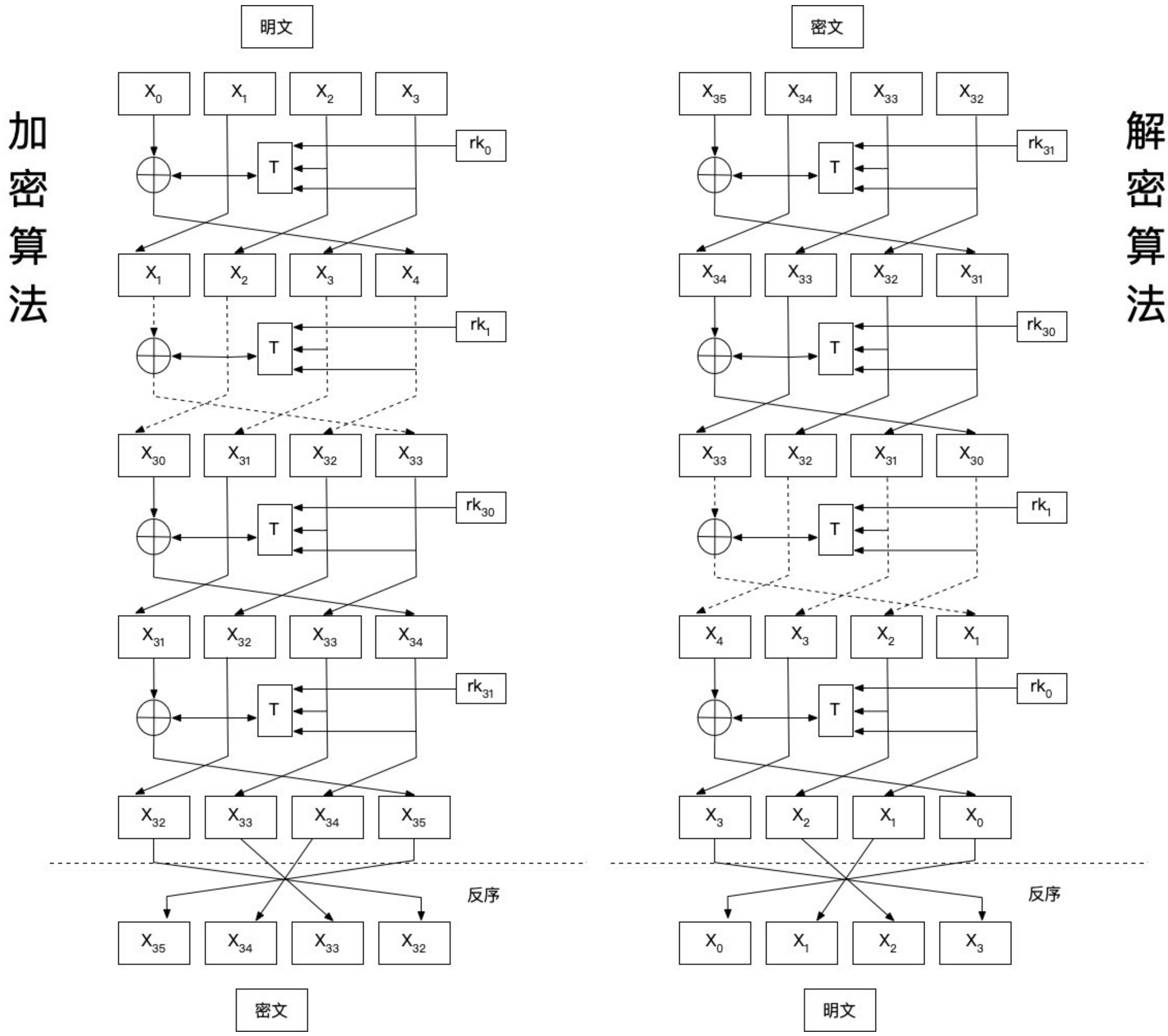
# SM4的可逆性证明

1901210403 胡兆杰

SM4算法总共有32次迭代运算和1次反序运算。加密和解密的框图如下。




**符号规定**

输入数据为$(X_0, X_1, X_2, X_3)$，四个32位的字，则输入数据的总长为128位。

轮密钥为$rk$，是一个32位的字。

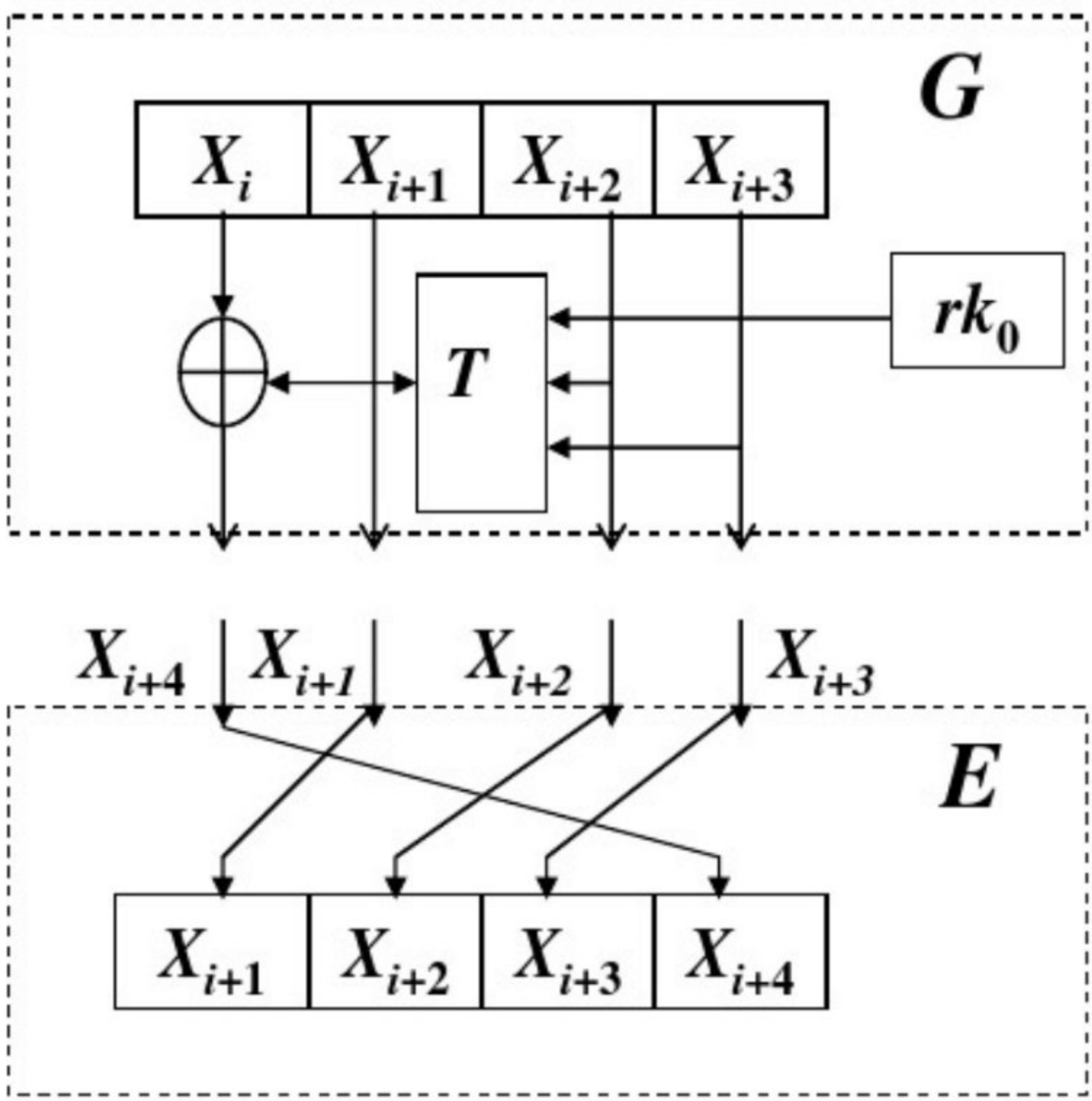
轮函数F。$F(X_0, X_1, X_2, X_3, rk) = X_0 \bigoplus T(X_1 \bigoplus X_2 \bigoplus X_3 \bigoplus rk)$

其中$T$为字合成变换，由非线性变换$\tau$（S盒置换）和线性变换$L$（循环左移）复合而成。

$T(X) = L(\tau(X))$

**可逆性证明**

单轮的变换图如下。




从图中可以看出，每一轮的加密经历了两个部分，一部分为加密函数($G$)，另一部分为数据交换($E$)，所以轮函数F又可以写成下面的形式。

$F_i = G_i E_i$

其中：

$$\begin{aligned} G_i &= G_i\left(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i\right) \\ &= \left(X_i \bigoplus T\left(X_{i+1} \bigoplus X_{i+2} \bigoplus X_{i+3} \bigoplus rk_i\right), X_{i+1}, X_{i+2}, X_{i+3}\right) \end{aligned}$$

$E\left(X_{i+4}, \left(X_{i+1}, X_{i+2}, X_{i+3}\right)\right) = \left(\left(X_{i+1}, X_{i+2}, X_{i+3}\right), X_{i+4}\right)$

以第0轮加密为例，输入数据为$(X_0, X_1, X_2, X_3)$，则：

$G(X_0, X_1, X_2, X_3, rk_0) = (X_0 \bigoplus T(X_1, X_2, X_3, rk_0), X_1, X_2, X_3)$

再对上式进行E变换，得到：

$E((X_0 \bigoplus T(X_1 \bigoplus X_2 \bigoplus X_3 \bigoplus rk_0), X_1, X_2, X_3)) = (X_1, X_2, X_3, X_0 \bigoplus T(X_1 \bigoplus X_2 \bigoplus X_3 \bigoplus rk_0))$

令$X_0 \bigoplus T(X_1 \bigoplus X_2 \bigoplus X_3 \bigoplus rk_0) = X_4$，就变成了图中第一轮加密之后的结果。以此类推，到第31轮时，得到输出$(X_{32}, X_{33}, X_{34}, X_{35})$，经过反序，得到输出$(X_{35}, X_{34}, X_{33}, X_{32})$

解密时，只需要将轮密钥倒过来使用即可。以解密的第0轮为例，输入为加密得到的密文$(X_{35}, X_{34}, X_{33}, X_{32})$，其中$X_{35} = X_{31} \bigoplus T(X_{32} \bigoplus X_{33} \bigoplus X_{34} \bigoplus rk_{31})$。

对输入进行G变换。

$$\begin{aligned} & G\left(X_{35}, X_{34}, X_{33}, X_{32}, rk_{31}\right) \\ & = \left(X_{31} \bigoplus T\left(X_{32} \bigoplus X_{33} \bigoplus X_{34} \bigoplus rk_{31}\right) \bigoplus T\left(X_{34} \bigoplus X_{33} \bigoplus X_{32} \bigoplus rk_{31}\right), X_{34}, X_{33}, X_{32}\right) \\ & = \left(X_{31}, X_{34}, X_{33}, X_{32}\right) \end{aligned}$$

对上式进行E变换。

$$E(X_{31}, X_{34}, X_{33}, X_{32}) = (X_{34}, X_{33}, X_{32}, X_{31})$$

该轮解密成功，以此类推，到第31轮解密时，得到的输出为$(X_3, X_2, X_1, X_0)$，再经过反序，得到最终的明文$(X_0, X_1, X_2, X_3)$。

由上面可知，SM4是可逆的。