1901210488 时绍森

SM4 的加密轮函数分成加密函数 **G** 和数据交换 **E**，加密函数 **G** 进行加密处理，数据交换 **E** 进行数据顺序交换

轮函数 **F = G E**

Gi=Gi(Xi, Xi+1, Xi+2, Xi+3, rki)

=(Xi ⊕T(Xi +1，Xi+2，Xi +3, rki), Xi+1，Xi+2，Xi +3)

E(Xi+4, (Xi +1, Xi+2, Xi+3))=((Xi+1, Xi+2, Xi+3), Xi+4)

(Gi)2= Gi (Xi⊕T(Xi+1，Xi+2，Xi+3, rki)，Xi+1，Xi+2，Xi+3，rki)

= (Xi⊕T(Xi+1，Xi+2，Xi+3, rki)⊕T(Xi+1，Xi+2，Xi+3，rki)，Xi+1，Xi+2，Xi+3，rki)

=(Xi，Xi+1，Xi+2，Xi+3，rki)

=I

这说明加密函数 **G** 是对合的。因为，**E** 变换为:

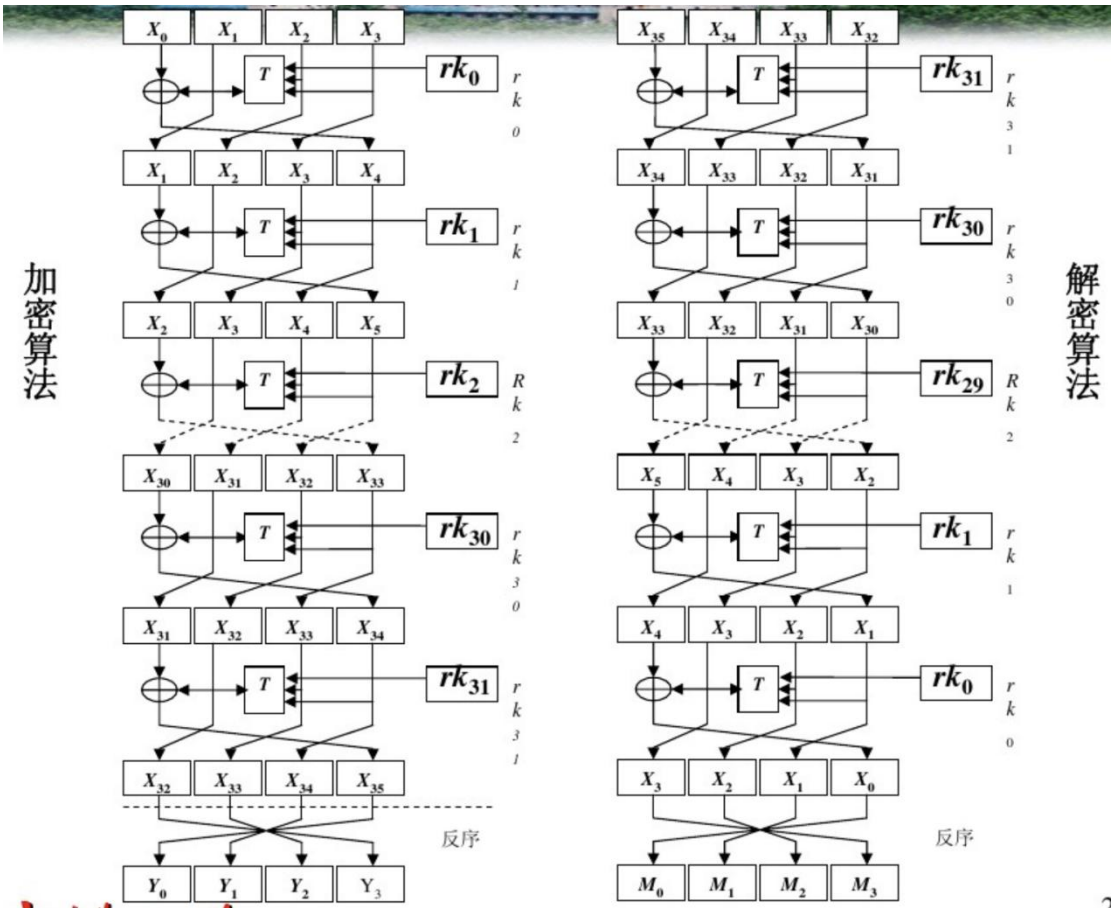
E(Xi+4，(Xi+1，Xi+2，Xi+3)) = ((Xi+1，Xi+2，Xi+3)，Xi+4) E2(Xi+4，(Xi+1，Xi+2，Xi+3)) = I

显然，**E** 是对合运算。

综上，轮函数是对合的。

Sm4 算法的加解密过程为:

明文　　密文



密文　　明文

根据加密框图，可把 **SM4** 的加密过程写成:

SM4 =G0 EG1 E…G30 EG31 R
根据解密框图，把 **SM4** 的解密过程写成: **SM4-1=G31 EG30 E…G1 EG0 R**
比较 **SM4** 与 **SM4-1** 可知，运算相同，只有密钥的使用顺序不同。
所以 **SM4** 是对合的。

根据加密框图，**SM4** 的加密过程的数据变化：
(X0,X1,X2,X3)->(X1,X2,X3,X4)->(X2,X3,X4,X5)->…->(X32,X33,X34,X35)->(X35,X34,X33,X32)=(Y0,Y1,Y2,Y3)
其中最后一步变换为反序

根据解密框图，密文**(Y0,Y1,Y2,Y3)**解密过程数据的变化：
(Y0,Y1,Y2,Y3)=(X35,X34,X33,X32)->(X34,X33,X32,X31)->(X33,X32,X31,X30)->…->(X3,X2,X1,X0)->(X0,X1,X2,X3)
其中最后一步变换为反序
由于 **SM4** 是对合的，所以 **$SM4^{-1}$=SM4**

$SM4^{-1}$(SM4(X0,X1,X2,X3))=(X0,X1,X2,X3)
所以 **SM4** 是可逆的