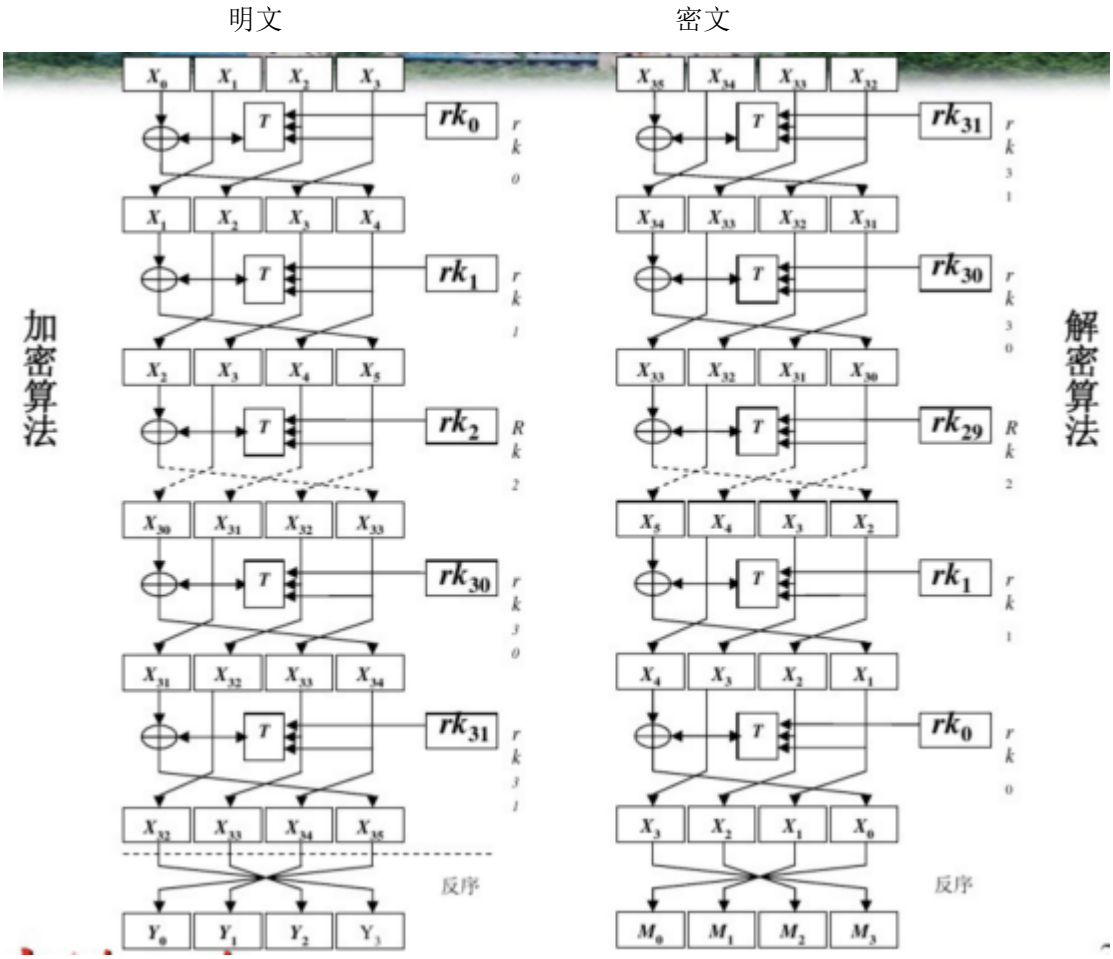
1901210488 时绍森

Sm4算法的加解密过程为：



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

$SM4^{-1}(SM4(X0,X1,X2,X3))=(X0,X1,X2,X3)$

所以SM4是可逆的