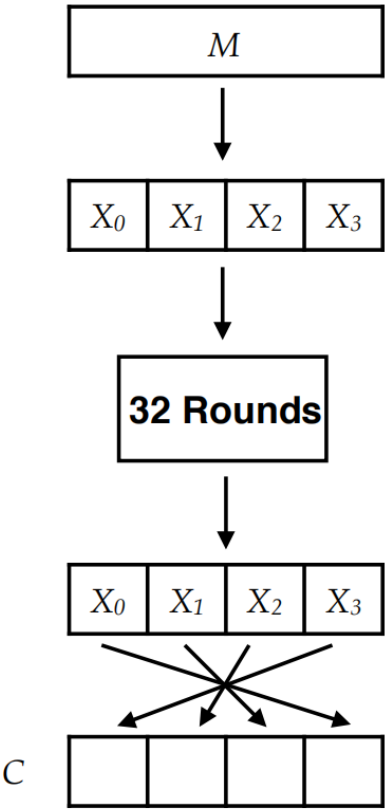
SM4 算法结构图



定义反序变换 R 为 R(A0,A1,A2,A3)=(A3,A2,A1,A0),
T 为可逆变换。

加密算法：
明文 M 为 128 比特，将它分为四段各为 32 比特，M=(X[0],X[1],X[2],X[3])。
然后用轮密钥对其进行变换。
X[i+4]=X[i]⊕T(X[i+1]⊕X[i+2]⊕X[i+3]⊕rk[i]).i=0,1,…31.
密文（Y[0], Y[1], Y[2], Y[3]）=R(X[32],X[33],X[34],X[35])=(X[35],X[34],X[33],X[32])

解密算法：
Y[i+4]=Y[i]⊕T(Y[i+1]⊕Y[i+2]⊕Y[i+3]⊕rk[i]).i=31,30,…0
X（[0], Y[1], Y[2], Y[3]）=R(Y[32],Y[33],Y[34],Y[35])=([Y35],Y[34],Y[33],Y[32])

SM4 算法所使用的变换都是可逆的，由上述算法分析可知，SM4 算法是可逆的。

.