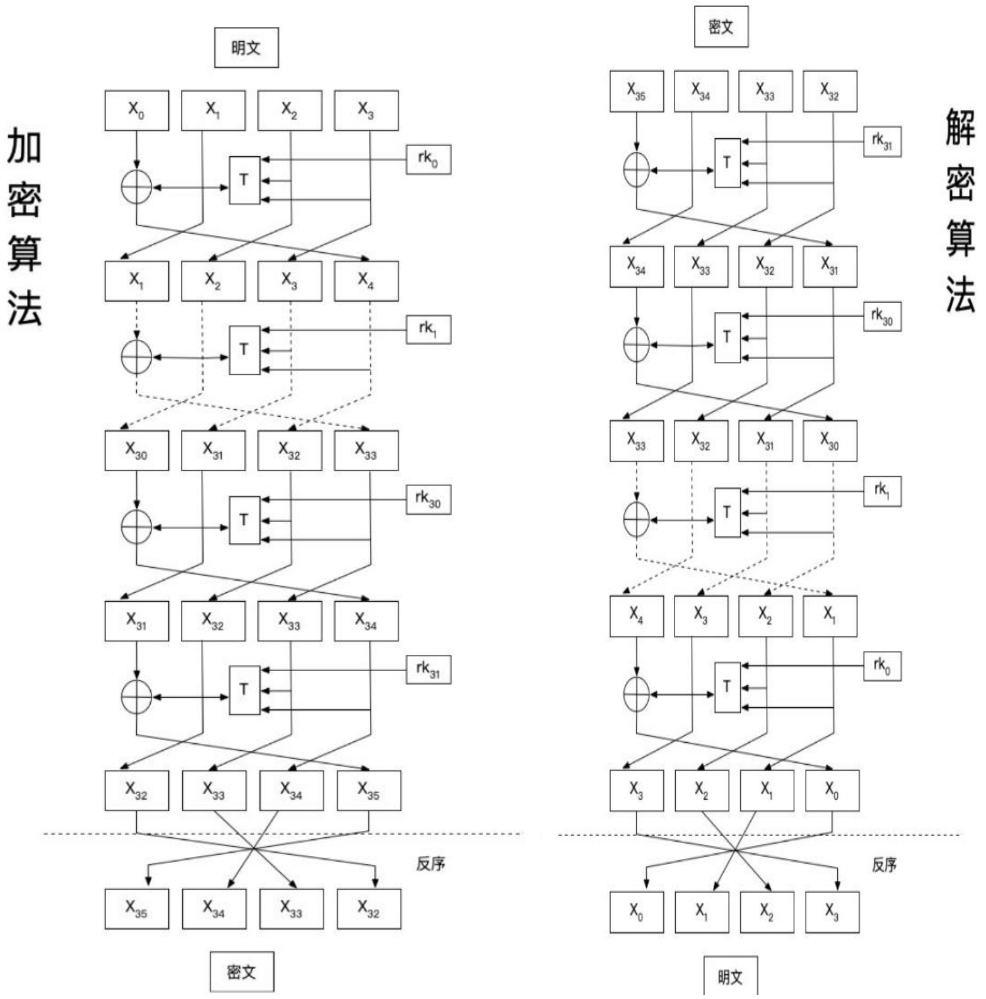
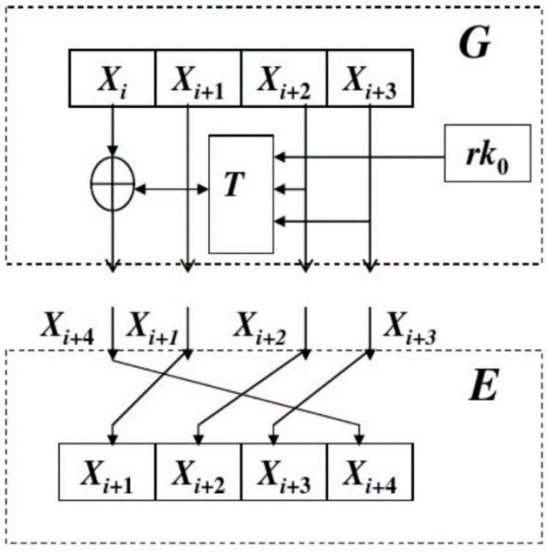
SM4 算法的加解密图示如下




如图所示，SM4 算法加密和解密均有 32 轮迭代。，加密算法和解密算法每轮迭代的算法相同，不同之处仅在于使用的密钥。每轮输入 128 比特，输出 128 比特。轮函数 F 可以分为加密函数 G 和数据交换函数 E，即轮函数 F=GE，如下图所示




其中：

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

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

对于 G 函数和 E 函数显然有

$$(G_i)^2 = G_i(X_i \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rki), X_{i+1}, X_{i+2}, X_{i+3}, rki)$$
$$= (X_i \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rki) \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rki),$$
$$X_{i+1}, X_{i+2}, X_{i+3}, rki)$$
$$= (X_i, X_{i+1}, X_{i+2}, X_{i+3}, rki)$$
$$= I$$

$$E(X_{i+4}, (X_{i+1}, X_{i+2}, X_{i+3})) = ((X_{i+1}, X_{i+2}, X_{i+3}), X_{i+4})$$
$$E^2(X_{i+4}, (X_{i+1}, X_{i+2}, X_{i+3})) = I$$

即 G 函数和 E 函数都是对合的，因此可以把 SM4 的加密过程和解密过程分别写为：

$SM4 = G_0 E G_1 E \cdots G_{29} E G_{30} R$

$SM4^{-1} = G_{31} E G_{30} E \cdots G_1 E G_0 R$

由此有 SM4 的数据加密过程中的数据变化：

$(X_0, X_1, X_2, X_3) \rightarrow (X_1, X_2, X_3, X_4) \rightarrow (X_2, X_3, X_4, X_5) \rightarrow \cdots \rightarrow (X_{32}, X_{33}, X_{34}, X_{35}) \rightarrow (X_{35}, X_{34}, X_{33}, X_{32}) = (Y_0, Y_1, Y_2, Y_3)$

其中最后一轮反序

解密过程中的数据变化：

$(X_{35}, X_{34}, X_{33}, X_{32}) \rightarrow (X_{34}, X_{33}, X_{32}, X_{31}) \rightarrow \cdots \rightarrow (X_5, X_4, X_3, X_2) \rightarrow (X_4, X_3, X_2, X_1) \rightarrow (X_3, X_2, X_1, X_0) = (X_0, X_1, X_2, X_3)$

所以有 $SM4^{-1}(SM4((X_0, X_1, X_2, X_3))) = (X_0, X_1, X_2, X_3)$