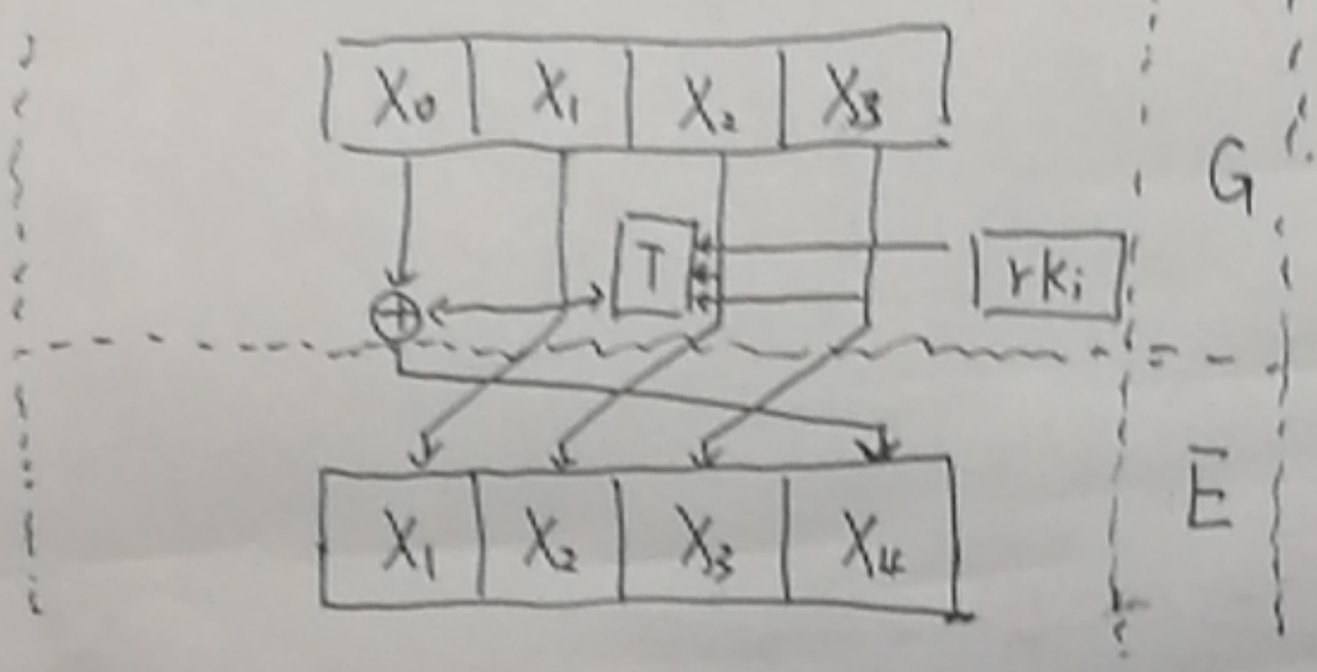
SM4加密可逆性证明：

① SM4加密变换：

$$X_{i+4} = F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i)$$

$$= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), \quad i = 0, 1 \ldots 31.$$

加密变换图：



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

$$= (X_i \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \oplus T(X_{i+1}, X_{i+2}, X_{i+3}, rk_i), X_{i+1}, X_{i+2}, X_{i+3})$$

$$= (X_1, X_{i+1}, X_{i+2}, X_{i+3}, rk_i).$$

根据加密变换图，SM4的加密过程的数据变化：

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

$$\longrightarrow (X_{35}, X_{34}, X_{33}, X_{32}) = (Y_0, Y_1, Y_2, Y_3)$$

反所以：$(X_{35}, X_{34}, X_{33}, X_{32}) \rightarrow (X_{34}, X_{33}, X_{32}, X_{31}) \rightarrow \cdots \rightarrow (X_3, X_2, X_1, X_0) \rightarrow (X_0, X_1, X_2, X_3)$

因此SM_4是可逆。