TMS

$\boldsymbol{Setup(1^{\lambda}) \rightarrow (params)}$

$e: G_1 \times G_1 \rightarrow G_T, H_0: \{0,1\}^* \rightarrow G_1$

$\boldsymbol{KeyGen(params) \rightarrow (sk_i, pk_i)(n = 4, t = 3)}$

$f(x) = 5 + 2x + 3x^2$

用户 1：$(sk_1, pk_1) = (10, g^{10})$

用户 2：$(sk_2, pk_2) = (21, g^{21})$

用户 3：$(sk_3, pk_3) = (38, g^{38})$

用户 4：$(sk_4, pk_4) = (61, g^{61})$

$\boldsymbol{Enc}$

$Q = pk_1^4 \cdot pk_2^{-6} \cdot pk_3^4 \cdot pk_4^{(-1)}$

$C_1 = g^s, s \in Z_p, C_2 = e(H(W), Q)^s$

$pk_5 = g^{90}, K_5 = e(H(W), pk_5^s)$

$\boldsymbol{Trap}$

$T_1 = (H(W))^{sk_1} = (H(W))^{10},$

$T_2 = (H(W))^{sk_2} = (H(W))^{21},$

$T_3 = (H(W))^{sk_3} = (H(W))^{38},$

$T_4 = (H(W))^{sk_4} = (H(W))^{61}$

$\boldsymbol{Search}$

$K_1 = e(T_1, C_1)$

$K_2 = e(T_2, C_1)$

$K_3 = e(T_3, C_1)$

$K = e(C_1, H(W))^{sk_1 \cdot (15/4)} \cdot e(C_1, H(W))^{sk_2 \cdot (-5)} \cdot e(C_1, H(W))^{sk_3 \cdot (5/2)} \cdot e(C_1, H(W))^{sk_4 \cdot (-(\frac{1}{4}))}$

$K = e(C_1, H(W))^{10 \cdot (15/4)} \cdot e(C_1, H(W))^{21 \cdot (-5)} \cdot e(C_1, H(W))^{38 \cdot (5/2)} \cdot e(C_1, H(W))^{90 \cdot (-(\frac{1}{4}))}$

判断等式

$K = C_2$