Gu2CKS

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

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

$sk_C \in Z_p^*$是云服务器的私钥，$pk_c = g^{sk_c}$是云服务器的公钥

$g_1 = g^{x_1}, x_1$是随机选取的整数

$\boldsymbol{KeyGen(t = 3)}$

$(sk_1, pk_1): sk_1 \in Z_p^*, pk_1 = g^{sk_1};$

$(sk_2, pk_2): sk_1 \in Z_p^*, pk_1 = g^{sk_1};$

$(sk_3, pk_3): sk_1 \in Z_p^*, pk_1 = g^{sk_1};$

$\boldsymbol{Enc}$

$\eta_0 = 207, \eta_1 = -30, \eta_2 = 1$

$B_0 = g^{r_1 \cdot \eta_0 \cdot (7^{-1})}, B_1 = g^{r_1 \cdot \eta_1 \cdot (7^{-1})}, B_2 = g^{r_1 \cdot \eta_2 \cdot (7^{-1})}$

$C_1 = e(g_1, pk_1)^{r_1} \cdot e(g_1, pk_2)^{r_1} \cdot e(g_1, pk_3)^{r_1}$

$\boldsymbol{Trap}$

$T_{1,-1} = (pk_1)^a, T_{1,0} = g_1^{sk_1 \cdot (10^0 + 20^0) \cdot 2^{-1}} \cdot (pk_c)^{sk_1 \cdot a};$

$T_{1,1} = g_1^{sk_1 \cdot (10^1 + 20^1) \cdot 2^{-1}} \cdot (pk_c)^{sk_1 \cdot a};\ T_{1,2} = g_1^{sk_1 \cdot (10^2 + 20^2) \cdot 2^{-1}} \cdot (pk_c)^{sk_1 \cdot a},$

a是随机整数，标红是有变化的地方

$T_{2,-1} = (pk_2)^b,\ T_{2,0} = g_1^{sk_2 \cdot (10^0 + 20^0) \cdot 2^{-1}} \cdot (pk_c)^{sk_2 \cdot b};$

$T_{2,1} = g_1^{sk_2 \cdot (10^1 + 20^1) \cdot 2^{-1}} \cdot (pk_c)^{sk_2 \cdot b};\ T_{2,2} = g_1^{sk_2 \cdot (10^2 + 20^2) \cdot 2^{-1}} \cdot (pk_c)^{sk_2 \cdot b},$

b是随机整数

$T_{3,-1} = (pk_3)^d,\ T_{3,0} = g_1^{sk_3 \cdot (10^0 + 20^0) \cdot 2^{-1}} \cdot (pk_c)^{sk_3 \cdot d};$

$T_{3,1} = g_1^{sk_3 \cdot (10^1 + 20^1) \cdot 2^{-1}} \cdot (pk_c)^{sk_3 \cdot d};\ T_{3,2} = g_1^{sk_3 \cdot (10^2 + 20^2) \cdot 2^{-1}} \cdot (pk_c)^{sk_3 \cdot d},$

d是随机整数

$\boldsymbol{Search}$

$T_0 = [T_{1,0}/(T_{1,-1})^{sk_c}] \cdot [T_{2,0}/(T_{2,-1})^{sk_c}] \cdot [T_{3,0}/(T_{3,-1})^{sk_c}]$

$T_1 = [T_{1,1}/(T_{1,-1})^{sk_c}] \cdot [T_{2,1}/(T_{2,-1})^{sk_c}] \cdot [T_{3,1}/(T_{3,-1})^{sk_c}]$

$T_2 = [T_{1,2}/(T_{1,-1})^{sk_c}] \cdot [T_{2,2}/(T_{2,-1})^{sk_c}] \cdot [T_{3,2}/(T_{3,-1})^{sk_c}]$

判断等式

$e(B_0, T_0) \cdot e(B_1, T_1) \cdot e(B_2, T_2) = C_1$