GlobalSetup

$gp = (g, G_1, G_T, e, H, H_1, H_2, sk_{KGC}, sk_{svr}, pk_{svr})$

$sk_{KGC} = x \in Z_p^*, sk_{svr} = l \in Z_p^*, pk_{svr} = L = g^l$

$H: Z_p^* \to G_1, H_1: G_T \to Z_p^*, H_2: \{0,1\}^* \to Z_p^*$

KeyGen$_o$

$ID_o, s \in Z_p^*, V \in G_1$

$sk_o = (sk_{co}, sk_{ao}) = (s, H(ID_o)^x)$ [x在 GlobalSetup 里]

$pk_o = (V, pk_{co}, pk_{ao}) = (V, g^s, H(ID_o))$

KeyGen$_u$

$ID_u, t \in Z_p^*$

$sk_u = (sk_{tu}, sk_{au}) = (t, H(ID_u)^x)$

$pk_u = (pk_{tu}, pk_{au}) = (g^t, H(ID_u))$

Ciphertext

$r \in Z_p^*$

$T = e(L, V)^{sk_{co}}$

$C_w = (C_{w1}, C_{w2}) = ((pk_{co})^r, e(g, g^{H_2(w)})^r \cdot T)$

$C_{ID_o} = H_1(e(H(ID_o)^x, H(ID_u)))$

Re-enc

$C'_w = (C'_{w1}, C'_{w2}) = ((C_{w1})^{(sk_{tu}/sk_{co})}, C_{w2})$

Trapdoor

$k \in Z_p^*$

$T_q = \left(T_{q1}, T_{q2}\right) = ((g^{H_2(q)})^{1/sk_{tu}} \cdot L^k, g^k)$

$C_{ID_u} = H_1(e(H(ID_o), H(ID_u)^x))$

Test

$T = e(V, pk_{co})^{sk_{svr}}$

$e(C'_{w1}, T_{q1}/(T_{q2})^{sk_{svr}}) \cdot T = C'_{w2}$