PREKS

Setup. $pp = (e, G_1, G_T, g, h, H_1); e: G_1 \times G_1 \to G_T; g, h \in G_1; H_1: \{0,1\}^* \to G_1$

KeyGen. $pk_1 = g^{x_1}, sk_1 = x_1 \in Z_p^*; pk_2 = g^{x_2}, sk_2 = x_2 \in Z_p^*;$

Trapdoor 是一组

Trapdoor. $T_w = H_1(w)^{1/sk_1}$

Enc 是一组

Enc. $A \in \{0,1\}^*;\ B = pk_1^r; C = e(g, H_1(A))^r \cdot m, m \in G_T; D = H_1(A)^r; E = h^r;$
$t = e(g, H_1(w))^r, F = H_1(t)$

ReEnc 和 Test 是一组

ReEnc. $e\big(B, H_1(A)\big) = e(pk_1, D);\ e(B, h) = e(pk_1, E);\ B' = B^{sk_2/sk_1}$

Test. $F = H_1(e(B, T_w))$