$\boldsymbol{Bilinear\ Pairing}$.

$e(aP, bH) = e(P, H)^{ab}$

$\boldsymbol{Setup}(\mathbf{1}^{\lambda})$.

$param = (G_1, G_2, P, Q, e, p, h_3, h_4, h_5)$

$P, Q \in G_1, e: G_1 \times G_1 \to G_2, h_3: G_2 \to \{0,1\}^{\lambda}, h_4: G_2 \to \{0,1\}^{2\lambda}, h_5: G_1 \to \{0,1\}^{3\lambda}$

Let G_1, G_2 be two cyclic groups with the same order p.

Let P, Q be two generators of the group G_1.

$\boldsymbol{KeyGen}(\boldsymbol{param})$.

$$PK_{do} = aP, SK_{do} = a$$
$$PK_{dr} = bP, SK_{dr} = b$$

$a, b \in Z_p^*$

$\boldsymbol{Update}(\boldsymbol{param}, \boldsymbol{PK_{dr}}, \boldsymbol{SK_{do}}, \boldsymbol{w})$

$$eh_w = h_3(e(SK_{do}PK_{dr}, h_2(w)Q)^{t_w}), t_w \in Z_p^*$$
$$uh_w = h_4(e(SK_{do}PK_{dr}, h_2(w)Q)^{t_w})$$
$$CV_w = h_5(lPK_{dr}), l \in Z_p^*$$
$$v_w = h_5(SK_{dr}lP)$$

$\boldsymbol{Trapdoor}(\boldsymbol{param}, \boldsymbol{SK_{dr}}, \boldsymbol{w}, \boldsymbol{v_w})$

$$T_w = (t_w SK_{dr} h_2(w)Q)^{t_w}$$

$\boldsymbol{Search}(\boldsymbol{param})$

$$\text{计算} pairing = e(PK_{do}, T_w)$$
$$h_4(pairing), h_3(pairing)$$