System Initialization

$e: G_1 \times G_1 \rightarrow G_T$

$H_1: G_T \rightarrow Z_p^*, H_2: \{0,1\}^* \rightarrow Z_p^*, H_3: \{0,1\}^* \rightarrow G_1$

$sk_S \in Z_p^*, V \in G_T, pk_S = (V, g^{sk_S})$

$sk_R \in Z_p^*, pk_R = g^{sk_R}$

$x \in Z_p^*, X = g^x$

Key Decryption

Step 1. $\rho \in \{0,1\}^*, r \in Z_p^*, K \in G_T$

$EK = K \cdot e(pk_S, H_3(\rho))^r$

Step 2. $\tau = e(g^{sk_S \cdot sk_R \cdot r}, H_3(\rho))$

Step 3. $K = EK/(\tau)^{(1/sk_R)}$

Enc

$r \in Z_p^*, s \in Z_p^*$

$C_1 = (pk_R)^r,\ \ t = e(X,V)^s,\ \ C_2 = H_1\big(e\big(g, g^{H_2(W)}\big)^r \cdot t\big),\ \ C_3 = g^s$

Trap

$\tau \in Z_p^*$

$T_1 = (g^{H_2(W)})^{(1/sk_R)} \cdot X^{\tau},\ \ T_2 = g^{\tau}$

Match

$H_1(e(C_1, T_1/(T_2)^x) \cdot t) = C_2$