

# 1 Scheme

## 1.1 Setup( $l$ ) $\rightarrow$ ( $mpk, msk$ )

$p \leftarrow \|\mathbb{G}\|$   
 generate  $g \in \mathbb{G}_1$  randomly  
 $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$   
 $H_2 : \{0, 1\}^* \rightarrow \mathbb{G}_2$   
 $\hat{H} : \{0, 1\}^* \rightarrow \{0, 1\}^\lambda$   
 generate  $g_0, g_1 \in \mathbb{G}_1$  randomly  
 generate  $w, \alpha, t_1, t_2 \in \mathbb{Z}_p^*$   
 $\Omega \leftarrow e(g, g)^w$   
 $v \leftarrow g^{t_1}$   
 $v \leftarrow g^{t_2}$   
 $mpk \leftarrow (p, g, g_0, g_1, v_1, v_2, \Omega, H_1, H_2, \hat{H})$   
 $msk \leftarrow (w, \alpha, t_1, t_2)$   
**return** ( $mpk, msk$ )

## 1.2 EGen( $id_S$ ) $\rightarrow ek_{id_S}$

$ek_{id_S} \leftarrow H_1(id_S)$   
**return**  $ek_{id_S}$

## 1.3 DGen( $id_R$ ) $\rightarrow dk_{id_R}$

generate  $r \in \mathbb{Z}_p^*$  randomly  
 $dk_0 \leftarrow H_2(id_R)^\alpha$   
 $dk_1 \leftarrow g^r$   
 $dk_2 \leftarrow g^{-\frac{w}{t_1}} (g_0 g_1^{id_R})^{-\frac{r}{t_1}}$   
 $dk_3 \leftarrow g^{-\frac{w}{t_2}} (g_0 g_1^{id_R})^{-\frac{r}{t_2}}$   
 $dk_{ID_R} \leftarrow (dk_0, dk_1, dk_2, dk_3)$   
**return**  $dk_{id_R}$

## 1.4 TGen( $id_R$ ) $\rightarrow tk_{id_R}$

generate  $k \in \mathbb{Z}_p^*$  randomly  
 $tk_1 \leftarrow g^k$   
 $tk_2 \leftarrow g^{\frac{1}{t_1}} (g_0 g_1^{id_R})^{-\frac{k}{t_1}}$   
 $tk_3 \leftarrow g^{\frac{1}{t_2}} (g_0 g_1^{id_R})^{-\frac{k}{t_2}}$   
 $tk_{ID_R} \leftarrow (tk_1, tk_2, tk_3)$   
**return**  $tk_{id_R}$

## 1.5 Enc( $ek_{id_S}, id_{Rev}, m$ ) $\rightarrow ct$

generate  $s_1, s_2, \beta \in \mathbb{Z}_p^*$  randomly  
 $s = s_1 + s_2$   
 $R = \Omega^{-s}$   
 $T \leftarrow g^\beta$   
 $K \leftarrow e(H_2(id_{Rev}), ek_{id_S} \cdot T)$   
 $ct_0 \leftarrow \hat{H}(R) \oplus \hat{H}(K) \oplus m$

$ct_1 \leftarrow (g_0 g_1^{id_{Rev}})^s$   
 $ct_2 \leftarrow v_1^{s_1}$   
 $ct_3 \leftarrow v_2^{s_2}$   
 $e(g, g)^s$   
 $ct \leftarrow (ct_0, ct_1, ct_2, ct_3, T, V)$   
**return**  $ct$

**1.6**  $\text{Dec}(dk_{id_R}, id_{Rev}, id_{Snd}, ct) \rightarrow m$

$R' \leftarrow e(dk_1, ct_1) \cdot e(dk_2, ct_2) \cdot e(dk_3, ct_3)$   
 $K' \leftarrow e(dk_0, H_1(id_{Snd})) \cdot e(H_2(id_R), T)$   
 $m \leftarrow ct_0 \oplus \hat{H}(R') \oplus \hat{H}(K')$   
**return**  $m$

**1.7**  $\text{TVerify}(tk_{id_R}, ct) \rightarrow y, y \in \{0, 1\}$

**return**  $V = e(tk_1, ct_1) \cdot e(tk_2, ct_2) \cdot e(tk_3, ct_3)$