1 SchemeCANIFPPCT

1.1 Setup$(l) \rightarrow (\boldsymbol{mpk}, \boldsymbol{msk})$

$p \leftarrow \|\mathbb{G}\|$
generate $g_1, g_3 \in \mathbb{G}_1$ randomly
generate $g_2 \in \mathbb{G}_2$ randomly
generate $r, s, t, \omega, t_1, t_2, t_3, t_4 \in \mathbb{Z}_r$ randomly
$R \leftarrow g_1^r$
$S \leftarrow g_2^s$
$T \leftarrow g_1^t$
$\Omega \leftarrow e(g_1, g_2)^{t_1 t_2 \omega}$
$v_1 \leftarrow g_2^{t_1}$
$v_2 \leftarrow g_2^{t_2}$
$v_3 \leftarrow g_2^{t_3}$
$v_4 \leftarrow g_2^{t_4}$
$mpk \leftarrow (g_1, g_2, p, g_3, H_1, H_2, H_3, H_4, R, S, T, \Omega, v_1, v_2, v_3, v_4)$
$msk \leftarrow (r, s, t, \omega, t_1, t_2, t_3, t_4)$
return (mpk, msk)

1.2 KGen$(\boldsymbol{ID}_k) \rightarrow \boldsymbol{sk}_{\boldsymbol{ID}_k}$

generate $k_i, x_i \in \mathbb{Z}_r$ randomly
$z_i \leftarrow (r - x_i)(sx_i)^{-1} \in \mathbb{Z}_r$
$Z_i \leftarrow g_1^{z_i} \in \mathbb{G}_1$
$sk_{ID_i} \leftarrow k_i$
$ek_{ID_i} \leftarrow (x_i, Z_i)$
$HI \leftarrow h_1^{I_1} h_2^{I_2} \cdots h_k^{I_k}$
$sk_{ID_k} \leftarrow (g_2^{\frac{\alpha}{b_1}} \cdot HI^{\frac{r}{b_1}} \cdot \bar{g}_3^r, g_2^{\frac{\alpha}{b_2}} \cdot HI^{\frac{r}{b_2}} \cdot \tilde{g}_3^r, g^r, h_{k+1}^{\frac{r}{b_1}}, h_{k+2}^{\frac{r}{b_1}}, \cdots, h_l^{\frac{r}{b_1}}, h_{k+1}^{\frac{r}{b_2}}, h_{k+2}^{\frac{r}{b_1}}, \cdots, h_l^{\frac{r}{b_1}}, h_{k+1}^{b_1^{-1}}, h_{k+2}^{b_1^{-1}}, \cdots, h_l^{b_1^{-1}}, h_{k+1}^{b_2^{-1}}, h$
return sk_{ID_k}

1.3 DerivedKGen$(\boldsymbol{sk}_{\boldsymbol{ID}_{k-1}}, \boldsymbol{ID}_k) \rightarrow \boldsymbol{sk}_{\boldsymbol{ID}_k}$

generate $t \in \mathbb{Z}_r$ randomly
$sk_{ID_k} \leftarrow (a_0 \cdot c_{0,k}^{I_k} \cdot (f_0 \cdot d_{0,k}^{I_k} \cdot \bar{g}_3)^t, a_1 \cdot c_{1,k}^{I_k} \cdot (f_1 \cdot d_{1,k}^{I_k} \cdot \tilde{g}_3)^t, b \cdot g^t, c_{0,k+1} \cdot d_{0,k+1}^t, c_{0,k+2} \cdot$
$d_{0,k+2}^t, \cdots, c_{0,l} \cdot d_{0,l}^t, c_{1,k+1} \cdot d_{1,k+1}^t, c_{1,k+2} \cdot d_{1,k+2}^t, \cdots, c_{1,l} \cdot d_{1,l}^t, d_{0,k+1}, d_{0,k+2}, \cdots, d_{0,l}, d_{1,k+1}, d_{1,k+2}, \cdots, d_{1,l}, f_0$
$c_{0,k}^{I_k}, f_1 \cdot c_{1,k}^{I_k})$
return sk_{ID_k}

1.4 Enc$(\boldsymbol{ID}_k, M) \rightarrow \boldsymbol{CT}$

generate $s_1, s_2 \in \mathbb{Z}_r$ randomly
$CT \leftarrow (e(g_1, g_2)^{s_1 + s_2} \cdot M, \bar{g}^{s_1}, \tilde{g}^{s_2}, (h_1^{I_1} h_2^{I_2} \cdots h_k^{I_k} \cdot g_3)^{s_1 + s_2})$
return CT

1.5 Dec$(\boldsymbol{sk}_{\boldsymbol{ID}_k}, \boldsymbol{CT}) \rightarrow M$

$$M \leftarrow \frac{e(b, D) \cdot A}{e(B, a_0) \cdot e(C, a_1)}$$
return M