1 SchemeAAIBME

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

generate $\alpha, \beta, t_1, t_2, t_3, t_4 \in \mathbb{Z}_r$ randomly
generate $g_2, g_3 \in \mathbb{G}_1$ randomly
generate $\boldsymbol{T} \leftarrow (\boldsymbol{T}_0, \boldsymbol{T}_1, \cdots, \boldsymbol{T}_n) \in \mathbb{G}_1^{n+1}$ randomly
generate $\boldsymbol{T}' \leftarrow (\boldsymbol{T}'_0, \boldsymbol{T}'_1, \cdots, \boldsymbol{T}'_n) \in \mathbb{G}_1^{n+1}$ randomly
generate $\boldsymbol{u} \leftarrow (\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n) \in \mathbb{G}_{\mathbb{1}}{}^{n+1}$ randomly
generate $\boldsymbol{u}' \leftarrow (\boldsymbol{u}'_0, \boldsymbol{u}'_1, \cdots, \boldsymbol{u}'_n) \in \mathbb{G}_1^{n+1}$ randomly
$g_1 \leftarrow g^{\alpha}$
$g'_1 \leftarrow g^{\beta}$
$Y_1 \leftarrow e(g_1, g_2)^{t_1 t_2}$
$Y_2 \leftarrow e(g_3, g)^{\beta}$
$v_1 \leftarrow g^{t_1}$
$v_2 \leftarrow g^{t_2}$
$v_3 \leftarrow g^{t_3}$
$v_4 \leftarrow g^{t_4}$
$H : \boldsymbol{u} \leftarrow (\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n), ID \leftarrow (ID_1, ID_2, \cdots, ID_n) \rightarrow \boldsymbol{u}_0 \prod_{j \in [1,n]} \boldsymbol{u}_j^{ID_j}$
$mpk \leftarrow (g_1, g'_1, g_2, g_3, Y_1, Y_2, v_1, v_2, v_3, v_4, \boldsymbol{u}, \boldsymbol{T}, \boldsymbol{u}', \boldsymbol{T}', H_1)$
$msk \leftarrow (g_2^{\alpha}, \beta, t_1, t_2, t_3, t_4)$
return (mpk, msk)

1.2 EKGen$(\boldsymbol{ID}_A) \rightarrow \boldsymbol{ek}_{\boldsymbol{ID}_A}$

$HI \leftarrow h_1^{I_1} h_2^{I_2} \cdots h_k^{I_k}$
$sk_{ID_k} \leftarrow (g_2^{\frac{\alpha}{b_1}} \cdot HI^{\frac{r}{b_1}} \cdot \bar{g}_3^r, g_2^{\frac{\alpha}{b_2}} \cdot HI^{\frac{r}{b_2}} \cdot \tilde{g}_3^r, g^r, h_{k+1}^{\frac{r}{b_1}}, h_{k+2}^{\frac{r}{b_1}}, \cdots, h_l^{\frac{r}{b_1}}, h_{k+1}^{\frac{r}{b_2}}, h_{k+2}^{\frac{r}{b_1}}, \cdots, h_l^{\frac{r}{b_1}}, h_{k+1}^{b_1^{-1}}, h_{k+2}^{b_1^{-1}}, \cdots, h_l^{b_1^{-1}}, h_{k+1}^{b_2^{-1}}, h$
return sk_{ID_k}

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

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

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