1 SchemeAAIBME

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

$g \leftarrow 1_{\mathbb{G}_1}$
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 $\boldsymbol{u} \leftarrow (\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n) \in \mathbb{G}_{\nVdash}{}^{n+1}$ randomly
generate $\boldsymbol{u}' \leftarrow (\boldsymbol{u}_0', \boldsymbol{u}_1', \cdots, \boldsymbol{u}_n') \in \mathbb{G}_1^{n+1}$ randomly
$H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$
$g_1 \leftarrow g^{\alpha}$
$g_1' \leftarrow g^{\beta}$
$Y_1 \leftarrow e(g_1, g_2)^{t_1 t_2}$
$Y_2 \leftarrow e(g_3, g)^{\beta}$
$v_1 \leftarrow g^{t_1}$
$v_2 \leftarrow g^{t_2}$
$v_3 \leftarrow g^{t_3}$
$v_4 \leftarrow g^{t_4}$
$mpk \leftarrow (g_1, g_1', g_2, g_3, Y_1, Y_2, v_1, v_2, v_3, v_4, \boldsymbol{u}, \boldsymbol{T}, \boldsymbol{u}', \boldsymbol{T}', H_1)$
$msk \leftarrow (g_2^{\alpha}, \beta, t_1, t_2, t_3, t_4)$
return (mpk, msk)

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

$g \leftarrow 1_{\mathbb{G}_1}$
$H : (\boldsymbol{u} \leftarrow (\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n), ID \leftarrow (ID_1, ID_2, \cdots, ID_n)) \rightarrow \boldsymbol{u}_0 \prod_{j \in [1,n]} \boldsymbol{u}_j^{ID_j}$
generate $\vec{r} = (r_1, r_2, \cdots, r_n) \in \mathbb{Z}_r^n$ randomly
generate a $(d-1)$ degree polynominal $q(x)$ s.t. $q(0) = \beta$ randomly
$ek_{ID_{A_i}} \leftarrow (g_3^{q(i)}[H(\boldsymbol{u}', ID_A)T_i']^{r_i}, g^{r_i}), \forall i \in \{1, 2, \cdots, n\}$
generate $ek_{ID_A}(S) \subset ek_{ID_A}$ s.t. $\|ek_{ID_A}(S)\| = d$ randomly
return $ek_{ID_A}(S)$

1.3 DKGen$(\boldsymbol{id}_B) \rightarrow \boldsymbol{dk}_{\boldsymbol{ID}_B}$

$g \leftarrow 1_{\mathbb{G}_1}$
$H : (\boldsymbol{u} \leftarrow (\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n), ID \leftarrow (ID_1, ID_2, \cdots, ID_n)) \rightarrow \boldsymbol{u}_0 \prod_{j \in [1,n]} \boldsymbol{u}_j^{ID_j}$
generate $\vec{k}_1 = (k_{1,1}, k_{1,2}, \cdots, k_{1,n}) \in \mathbb{Z}_r^n$ randomly
generate $\vec{k}_2 = (k_{2,1}, k_{2,2}, \cdots, k_{2,n}) \in \mathbb{Z}_r^n$ randomly
$dk_{ID_{B_i}} \leftarrow (g^{k_{1,i} t_1 t_2 + k_{2,i} t_3 t_4} g_2^{-\alpha t_2} [H(\boldsymbol{u}, ID_B) T_i]^{k_{1,i} t_2} g_2^{-\alpha t_1} [H(\boldsymbol{u}, ID_B) T_i]^{k_{1,i} t_1} [H(\boldsymbol{u}, ID_B) T_i]^{k_{2,i} t_4} [H(\boldsymbol{u}, ID_B) T_i]^{k}$
$\{1, 2, \cdots, n\}$
generate $dk_{ID_B}(S') \subset dk_{ID_B}$ s.t. $\|dk_{ID_B}(S')\| = d$ randomly
return $dk_{ID_B}(S')$

1.4 Enc($\boldsymbol{ek_{ID_A}}(S), \boldsymbol{ID}_A, \boldsymbol{ID}_B, S, M) \rightarrow \boldsymbol{CT}$

$g \leftarrow 1_{\mathbb{G}_1}$
$H : (\boldsymbol{u} \leftarrow (\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n), ID \leftarrow (ID_1, ID_2, \cdots, ID_n)) \rightarrow \boldsymbol{u}_0 \prod_{j \in [1,n]} \boldsymbol{u}_j^{ID_j}$
generate $S'' \subset [1, n]$ s.t. $\|S''\| = d$ randomly
generate $s \in \mathbb{Z}_r$ randomly
generate $\vec{s}_1 = (s_{1,1}, s_{1,2}, \cdots, s_{1,n})$ randomly
generate $\vec{s}_2 = (s_{2,1}, s_{2,2}, \cdots, s_{2,n})$ randomly
generate a $(d-1)$ degree polynominal $q(x)$ s.t. $q(0) = s$ randomly
$K_s \leftarrow Y_1^s$
$K_l \leftarrow Y_2^s$
$C \leftarrow M \cdot K_s \cdot K_l$
$C_{1,i} \leftarrow [H(\boldsymbol{u}, ID_B)T_i]^{q(i)}, \forall i \in S''$
$C_{2,i} \leftarrow v_1^{q(i)-s_{1,i}}, \forall i \in S''$
$C_{3,i} \leftarrow v_2^{s_{1,i}}, \forall i \in S''$
$C_{4,i} \leftarrow v_3^{q(i)-s_{2,i}}, \forall i \in S''$
$C_{5,i} \leftarrow v_4^{s_{2,i}}, \forall i \in S''$
generate $\vec{z} = (z_1, z_2, \cdots, z_n) \in \mathbb{Z}_r^d$ randomly
generate $\vec{z'} = (z'_1, z'_2, \cdots, z'_n) \in \mathbb{Z}_r^d$ randomly
$C_{6,i} \leftarrow g^{z'_i}, \forall i \in S$
$C_{7,i} \leftarrow (ek_{ID_{A_{i,2}}}(S) \cdot g^{z_i})^s, \forall i \in S$
$C_{8,i} \leftarrow ek_{ID_{A_{i,1}}}(S) \cdot [H(\boldsymbol{u}', ID_A)T'_i]^{s \cdot z_i} \cdot H_1(C||C_{1,i}||C_{2,i}||C_{3,i}C_{4,i}||C_{5,i}||C_{6,i}||C_{7,i}), \forall i \in S$
$I \leftarrow S \cap S''$
if $\|I\| \leqslant d$ **then**
generate $I^* \subset I$ randomly
$CT \leftarrow (S'', I^*, C, \vec{C}_1, \vec{C}_2, \vec{C}_3, \vec{C}_4, \vec{C}_5, \vec{C}_6, \vec{C}_7, \vec{C}_8)$
return CT

1.5 Dec($\boldsymbol{dk_{ID_B}}(S'), \boldsymbol{ID}_B, \boldsymbol{ID}_A, \boldsymbol{CT}) \rightarrow M$

$CT_i \leftarrow C||C_{1,i}||C_{2,i}||C_{3,i}||C_{4,i}||C_{5,i}||C_{6,i}||C7, i, \forall i \in \{1, 2, \cdots, n\}$
$K'_l \leftarrow \prod_{i \in I^*} \left(\frac{e(C_{8,i}, g)}{e([H(\boldsymbol{u}', ID_A)T'_i]e(H_1(CT_i), C_{6,i})} \right)^{\Delta(i,I,0)}$
$K'_s \leftarrow \prod_{i \in I} ()^{\Delta(i,j,0)}$
if $|S \cap S'| \leqslant d \wedge |S' \cap S''| \leqslant d$ **then**
quad$M \leftarrow C \cdot K'_s \cdot K'_l$
else
$M \leftarrow \perp$
end if
return M