1 SchemeFuzzyME

This scheme is only applicable to symmetric groups of prime orders.

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

$g \leftarrow 1_{\mathbb{G}_1}$
generate $g_2, g_3 \in \mathbb{G}_1$ randomly
generate $\vec{t} \leftarrow \{t_1, t_2, \cdots, t_{n+1}\} \in \mathbb{G}_1^{n+1}$ randomly
generate $\vec{l} \leftarrow \{l_1, l_2, \cdots, l_{n+1}\} \in \mathbb{G}_1^{n+1}$ randomly
generate $\alpha, \beta, \theta_1, \theta_2, \theta_3, \theta_4 \in \mathbb{Z}_r$ randomly
$g_1 \leftarrow g^\alpha$
$\eta_1 \leftarrow g^{\theta_1}$
$\eta_2 \leftarrow g^{\theta_2}$
$\eta_3 \leftarrow g^{\theta_3}$
$\eta_4 \leftarrow g^{\theta_4}$
$Y_1 \leftarrow \hat{e}(g_1, g_2)^{\theta_1 \theta_2}$
$Y_2 \leftarrow \hat{e}(g_3, g^\beta)^{\theta_1 \theta_2}$
$H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$
$mpk \leftarrow (g_1, g_2, g_3, Y_1, Y_2, \vec{t}, \vec{l}, \eta_1, \eta_2, \eta_3, \eta_4, H_1)$
$msk \leftarrow (\alpha, \beta, \theta_1, \theta_2, \theta_3, \theta_4)$
return (mpk, msk)

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

$g \leftarrow 1_{\mathbb{G}_1}$
$\Delta : i, S, x \rightarrow \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$
$N \leftarrow (1, 2, \cdots, n+1)$
$H : x \rightarrow g_3^{x^n} \prod_{i=1}^{n+1} l_i^{\Delta(i, N, x)}$
generate a $(d-1)$ degree polynominal $q(x)$ s.t. $q(0) = \beta$ randomly
generate $\vec{r} \leftarrow \{r_1, r_2, \cdots, r_n\} \in \mathbb{Z}_r^n$ randomly
$E_i \leftarrow g_3^{q(a_i)\theta_1\theta_2} H(a_i)^{r_i}, \forall i \in \{1, 2, \cdots, n\}$
$e_i \leftarrow g^{r_i}, \forall i \in \{1, 2, \cdots, n\}$
$ek_{S_A} \leftarrow \{E_i, e_i\}_{a_i \in S_A}$
return ek_{S_A}

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

$g \leftarrow 1_{\mathbb{G}_1}$
$\Delta : i, S, x \rightarrow \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$
$N \leftarrow (1, 2, \cdots, n+1)$
$T : x \rightarrow g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta(i, N, x)}$
$H : x \rightarrow g_3^{x^n} \prod_{i=1}^{n+1} l_i^{\Delta(i, N, x)}$
generate $\gamma \in \mathbb{Z}_r$ randomly
generate $G_{ID} \in \mathbb{G}_1$ randomly

generate a $(d-1)$ degree polynominal $f(x)$ s.t. $f(0)=\alpha$ randomly
generate a $(d-1)$ degree polynominal $h(x)$ s.t. $h(0)=\gamma$ randomly
generate a $(d-1)$ degree polynominal $q'(x)$ s.t. $q'(0)=\beta$ randomly
generate $\vec{k}_1 \leftarrow \{k_{1,1}, k_{1,2}, \cdots, k_{1,n}\} \in \mathbb{Z}_r^n$ randomly
generate $\vec{k}_2 \leftarrow \{k_{2,1}, k_{2,2}, \cdots, k_{2,n}\} \in \mathbb{Z}_r^n$ randomly
generate $\vec{r'_1} \leftarrow \{r'_{1,1}, r'_{1,2}, \cdots, r'_{1,n}\} \in \mathbb{Z}_r^n$ randomly
generate $\vec{r'_2} \leftarrow \{r'_{2,1}, r'_{2,2}, \cdots, r'_{2,n}\} \in \mathbb{Z}_r^n$ randomly
$dk_{S_{B_{0,i}}} \leftarrow g^{k_{1,i}\theta_1\theta_2 + k_{2,i}\theta_3\theta_4}, \forall i \in \{1,2,\cdots,n\}$
$dk_{S_{B_{1,i}}} \leftarrow g_2^{-f(b_i)\theta_2}(G_{ID})^{-h(b_i)\theta_2}[T(b_i)]^{-k_{1,i}\theta_2}, \forall i \in \{1,2,\cdots,n\}$
$dk_{S_{B_{2,i}}} \leftarrow g_2^{-f(b_i)\theta_1}(G_{ID})^{-h(b_i)\theta_1}[T(b_i)]^{-k_{1,i}\theta_1}, \forall i \in \{1,2,\cdots,n\}$
$dk_{S_{B_{3,i}}} \leftarrow [T(b_i)]^{-k_{2,i}\theta_4}, \forall i \in \{1,2,\cdots,n\}$
$dk_{S_{B_{4,i}}} \leftarrow [T(b_i)]^{-k_{2,i}\theta_3}, \forall i \in \{1,2,\cdots,n\}$
$dk_{S_B} \leftarrow (dk_{S_{B_0}}, dk_{S_{B_1}}, dk_{S_{B_2}}, dk_{S_{B_3}}, dk_{S_{B_4}})$
$dk_{P_{A_{0,i}}} \leftarrow g^{r'_{i,1}\theta_1\theta_2 + r'_{i,2}\theta_3\theta_4}, \forall i \in \{1,2,\cdots,n\}$
$dk_{P_{A_{1,i}}} \leftarrow g_2^{-2q'(a_i)\theta_2}(G_{ID})^{h(a_i\theta_2)}H(a_i)^{-r'_{1,i}\theta_2}, \forall i \in \{1,2,\cdots,n\}$
$dk_{P_{A_{2,i}}} \leftarrow g_2^{-2q'(a_i)\theta_1}(G_{ID})^{h(a_i\theta_1)}H(a_i)^{-r'_{1,i}\theta_1}, \forall i \in \{1,2,\cdots,n\}$
$dk_{P_{A_{3,i}}} \leftarrow [H(a_i)]^{-r'_{2,i}\theta_4}, \forall i \in \{1,2,\cdots,n\}$
$dk_{P_{A_{3,i}}} \leftarrow [H(a_i)]^{-r'_{2,i}\theta_3}, \forall i \in \{1,2,\cdots,n\}$
$dk_{P_A} \leftarrow (dk_{P_{A_0}}, dk_{P_{A_1}}, dk_{P_{A_2}}, dk_{P_{A_3}}, dk_{P_{A_4}})$
$dk_{S_B,P_A} \leftarrow (dk_{S_B}, dk_{P_A})$
return dk_{S_B,P_A}

1.4 Encryption($\boldsymbol{ek}_{S_A}, M$) $\rightarrow \boldsymbol{CT}$

$g \leftarrow 1_{\mathbb{G}_1}$
$\Delta : i, S, x \rightarrow \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$
$N \leftarrow (1, 2, \cdots, n+1)$
$T : x \rightarrow g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta(i,N,x)}$
$H : x \rightarrow g_3^{x^n} \prod_{i=1}^{n+1} l_i^{\Delta(i,N,x)}$
generate $s, s_1, s_2, \tau \in \mathbb{Z}_r$ randomly
$K_s \leftarrow Y_1^s$
$K_l \leftarrow Y_2^s \cdot \hat{e}(g_3, g^{-\tau})$
$C_0 \leftarrow M \cdot K_s \cdot K_l$
$C_1 \leftarrow \eta_1^{s-s_1}$
$C_2 \leftarrow \eta_2^{s_1}$
$C_3 \leftarrow \eta_3^{s-s_2}$
$C_4 \leftarrow \eta_4^{s_2}$
$C_{1,i} \leftarrow T(b_i)^s, \forall b_i \in P_B$
$C_{2,i} \leftarrow H(a_i)^s, \forall a_i \in S_A$
generate a $(d-1)$ degree polynominal $l(x)$ s.t. $l(0)=\tau$ randomly
generate $\vec{\xi} \leftarrow \{\xi_1, \xi_2, \cdots, \xi_n\} \in \mathbb{Z}_r^n$ randomly
generate $\vec{\chi} \leftarrow \{\chi_1, \chi_2, \cdots, \chi_n\} \in \mathbb{Z}_r^n$ randomly
$C_{3,i} \leftarrow e_i \cdot g^{\xi_i}, \forall i \in \{1,2,\cdots,n\}$

$C_{4,i} \leftarrow g^{\chi_i}, \forall i \in \{1, 2, \cdots, n\}$
$C_{5,i} \leftarrow E_i^s \cdot g_3^{l(a_i)} H(a_i)^{s \cdot \xi_i} \cdot H_1(C_0||C_1||C_2||C_3||C_4||C_{1,i}||C_{2,i}||C_{3,i}||C_{4,i})^{\chi_i}$
$CT \leftarrow (C_0, C_1, C_2, C_3, C_4, \vec{C}_1, \vec{C}_2, \vec{C}_3, \vec{C}_4, \vec{C}_5)$
return CT

1.5 Decryption($\boldsymbol{dk}_{S_B,P_A}, S_B, P_A, \boldsymbol{CT}$) $\rightarrow M$

$W'_A \leftarrow S_A \cap P_A$
$W'_B \leftarrow S_B \cap P_B$
if $|W'_A| \leqslant d \wedge |W'_B| \leqslant d$ **then**
  generate $W_A \subset W'_A$ s.t. $|W_A| = d$ randomly
  generate $W_B \subset W'_B$ s.t. $|W_B| = d$ randomly
  $g \leftarrow 1_{\mathbb{G}_1}$
  $\Delta : i, S, x \rightarrow \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$
  $K'_s \leftarrow \prod_{b_i \in W_B} (\hat{e}(C_{1,i}, dk_{S_{B_{0,i}}})\hat{e}(C_1, dk_{S_{B_{1,i}}})\hat{e}(C_2, dk_{S_{B_{2,i}}})\hat{e}(C_3, dk_{S_{B_{3,i}}})\hat{e}(C_4, dk_{S_{B_{4,i}}}))^{\Delta(b_i, W_B, 0)}$
  $CT_i \leftarrow C_0||C_1||C_2||C_3||C_4||C_{1,i}||C_{2,i}||C_{3,i}||C_{4,i}, \forall i \in \{1, 2, \cdots, n\}$
  $K'_l \leftarrow \prod_{a_i \in W_A} \left(\frac{\hat{e}(C_{1,i}, dk_{P_{A_{0,i}}})\hat{e}(C_1, dk_{P_{A_{1,i}}})\hat{e}(C_2, dk_{P_{A_{i,2}}})}{\hat{e}(H_1(CT_i), C_{4,i}) \cdot \hat{e}(C_{3,i}, C_{2,i})} \cdot \hat{e}(C_3, dk_{P_{A_{i,3}}})\hat{e}(C_4, dk_{P_{A_{i,4}}})\hat{e}(C_{5,i}, g) \right)^{\Delta(a_i, W_A, 0)}$
  $M \leftarrow C_0 \cdot K'_s \cdot K'_l$
else
  $M \leftarrow \perp$
end if
return M