1 SchemeIBBME

This scheme is applicable to symmetric and asymmetric groups of prime orders.

1.1 Setup() $\rightarrow$ (*mpk*, *msk*)

generate $g, v \in \mathbb{G}_1$ randomly
generate $h \in \mathbb{G}_2$ randomly
generate $\vec{r_1} = (r_{1,0}, r_{1,1}, \cdots, r1, l) \in \mathbb{Z}_r^{l+1}$ randomly
generate $\vec{r_2} = (r_{2,0}, r_{2,1}, \cdots, r2, l) \in \mathbb{Z}_r^{l+1}$ randomly
generate $t_1, t_2, \beta_1, \beta_2, \alpha, \rho, b, \tau \in \mathbb{Z}_r$ randomly
$\vec{r} = (r_0, r_1, \cdots, r_l) \leftarrow \vec{r_1} + b\vec{r_2} = (r_{1,0} + br_{2,0}, r_{1,1} + br_{2,1}, \cdots, r_{1,l} + br_{2,l})$
$t \leftarrow t_1 + bt_2$
$\beta \leftarrow \beta_1 + b\beta_2$
$\vec{R} \leftarrow g^{\vec{r}} = (g^{r_0}, g^{r_1}, \cdots, g^{r_l})$
$T \leftarrow g^t$
$H_0 : \{0,1\}^* \rightarrow \mathbb{G}_2$
$H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_r$
$H_3 : \mathbb{G}_T \rightarrow \mathbb{Z}_r$
$mpk \leftarrow (v, v^\rho, g, g^b, \vec{R}, T, e(g,h)^\beta, h, h^{\vec{r_1}}, h^{\vec{r_2}}, h^{t_1}, h^{t_2}, g^{\tau\beta}, h^{\tau\beta_1}, h^{\tau\beta_2}, h^{1/\tau}, H_0, H_1, H_2, H_3)$
$msk \leftarrow (h^{\beta_1}, h^{\beta_2}, \alpha, \rho)$
return (mpk, msk)

1.2 EKGen(id^*) $\rightarrow$ ek_{id^*}

$ek_{id^*} \leftarrow H_1(id^*)^\alpha$
return ek_{id^*}

1.3 DKGen(id) $\rightarrow$ dk_{id}

generate $z \in \mathbb{Z}_r$ randomly
generate $rtags = (rtag_1, rtag_2, \cdots, rtag_l) \in \mathbb{Z}_r^l$ randomly
$dk_1 \leftarrow H_0(id)^\rho$
$dk_2 \leftarrow H_0(id)^\alpha$
$dk_3 \leftarrow H_0(id)$
$dk_4 \leftarrow h^{\beta_1}(h^{t_1})^z$
$dk_5 \leftarrow h^{\beta_2}(h^{t_2})^z$
$dk_6 \leftarrow h^z$
$dk_{7,j} \leftarrow ((h^{t_1})^{rtag_j} h^{r_{1,j}} / (h^{r_{1,0}})^{H_2(id)^j})^z, \forall j \in \{1, 2, \cdots, l\}$
$dk_{8,j} \leftarrow ((h^{t_2})^{rtag_j} h^{r_{2,j}} / (h^{r_{2,0}})^{H_2(id)^j})^z, \forall j \in \{1, 2, \cdots, l\}$
$dk_{id} \leftarrow (dk_1, dk_2, \cdots, dk_8, rtags)$
return dk_{id}

1.4 Enc(S, ek_{id^*}, m) $\rightarrow$ ct

Compute $y_0, y_1, y_2, \cdots y_n$ that satisfy $\forall x \in \mathbb{Z}_r$, we have $F(x) = \prod_{id_j \in S}(x - H_2(id_j)) = y_0 + \sum_{i=1}^{n} y_i x^i$

$\vec{y} \leftarrow (y_0, y_1, \cdots, y_n, y_{n+1}, y_{n+2}, \cdots, y_l) = (y_0, y_1, \cdots, y_n, 0, 0, \cdots, 0)$
generate $s, d_2, ctag \in \mathbb{Z}_r$ randomly
$C_0 \leftarrow m \cdot e(g,h)^{\beta s}$
$C_1 \leftarrow g^s$
$C_2 \leftarrow g^{bs}$
$C_3 \leftarrow \left(T^{ctag} \prod_{i=0}^{n} (g^{r_i})^{y_i}\right)^{d_2 s}$
$C_4 \leftarrow v^s$
$V_{id_i} \leftarrow H_3(e(H_0(id_i), ek_{id^*} \cdot g^{bs} \cdot v^{\rho s})), \forall id_i \in S$
Compute $\vec{b} \leftarrow (b_0, b_1, b_2, \cdots b_n)$ that satisfy $\forall y \in \mathbb{Z}_r$, we have $g(y) = \prod_{V_{id_k} \in V_{id}} (y - V_{id_k}) + d_2 = b_0 + \sum_{k=1}^{n} b_k y^k$
$ct \leftarrow (C_0, C_1, C_2, C_3, C_4, ctag, \vec{y}, \vec{b})$
return ct

1.5 Dec$(S, \boldsymbol{dk_{id_i}}, \boldsymbol{id^*}, \boldsymbol{ct}) \rightarrow m$

$V(id_i) \leftarrow H_3(e(dk_{i,3}, C_2)e(dk_{i,2}, H_1(id^*))e(dk_{i,1}, C_4))$
$d_2 \leftarrow g(V_{id_i}) = b_0 + \sum_{j=1}^{n} b_j V_{id_i}^j$
$rtag \leftarrow \sum_{i=1}^{l} y_i rtags_i$
if $rtag = ctag$ **then**
  $m \leftarrow \perp$
else
  $A \leftarrow e\left(C_1, \prod_{j=1}^{l} dk_{7,j}^{y_j}\right) e\left(C_2, \prod_{j=1}^{l} dk_{8,j}^{y_j}\right) / e(C_3^{1/d_2}, dk_6)$
  $B \leftarrow e(C_1, dk_4) \cdot e(C_2, dk_5)$
  $m \leftarrow C_0 \cdot A^{1/(rtag - ctag)} \cdot B^{-1}$
end if
return m