1 SchemeIBMEMR

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

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

$p \leftarrow \|\mathbb{G}\|$
$g \leftarrow 1_{\mathbb{G}_1}$
$H_1 : \mathbb{Z}_r \rightarrow \mathbb{G}_1$
$H_2 : \mathbb{Z}_r \rightarrow \mathbb{G}_1$
$\hat{H} : \mathbb{G}_T \rightarrow \{0,1\}^\lambda$
$H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_r$
$H_4 : \mathbb{G}_T \rightarrow \mathbb{Z}_r$
$H_5 : \{0,1\}^* \rightarrow \mathbb{G}_1$
generate $g_0, g_1 \in \mathbb{G}_1$ randomly
generate $w, \alpha, \gamma, k, t_1, t_2 \in \mathbb{Z}_r$ randomly
$\Omega \leftarrow e(g,g)^w$
$v_1 \leftarrow g^{t_1}$
$v_2 \leftarrow g^{t_2}$
$v_3 \leftarrow g^\gamma$
$v_4 \leftarrow g^k$
$mpk \leftarrow (p, g, g_0, g_1, v_1, v_2, v_3, v_4, \Omega, H_1, H_2, H_3, H_4, H_5, \hat{H})$
$msk \leftarrow (w, \alpha, \gamma, k, t_1, t_2)$
return (mpk, msk)

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

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

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

$dk_1 \leftarrow H_2(id_R)^\alpha$
$dk_2 \leftarrow g^{w/t_1}(g_0 g_1^{id_R})^{\gamma/t_1}$
$dk_3 \leftarrow g^{w/t_2}(g_0 g_1^{id_R})^{\gamma/t_2}$
$dk_{id_R} \leftarrow (dk_1, dk_2, dk_3)$
return dk_{id_R}

1.4 TDKGen$(\boldsymbol{id}_R) \rightarrow \boldsymbol{td}_{\boldsymbol{id}_R}$

$td_1 \leftarrow g^{-1/t_1}(g_0 g_1^{id_R})^{k/t_1}$
$td_2 \leftarrow g^{-1/t_2}(g_0 g_1^{id_R})^{k/t_2}$
$td_{id_R} \leftarrow (td_1, td_2)$
return td_{id_R}

1.5 $\mathbf{Enc}(\boldsymbol{ek_{id_S}}, \boldsymbol{id}_R, m) \rightarrow \boldsymbol{ct}$

generate $s_1, s_2, \beta, \sigma, K, R \in \mathbb{Z}_r$ randomly
$r \leftarrow H_3(\sigma || m)$
$ct_1 \leftarrow g^{\beta}$
$ct_2 \leftarrow v_1^{s_1}$
$ct_3 \leftarrow v_2^{s_2}$
$K_i \leftarrow e(H_2(id_i), ek_{id_S} \cdot ct_1), \forall i \in \{1, 2, \cdots, d\}$
Compute $a_0, a_1, a_2, \cdots a_d$ that satisfy $\forall x$, we have $F(x) = \prod_{i=1}^{d}(x - H_4(K_i)) + K = \sum_{i=0}^{d} a_i x^i$
$s \leftarrow s_1 + s_2$
$R_i \leftarrow e(v_3, (g_0 g_1^{id_i})^s), \forall i \in \{1, 2, \cdots, d\}$
Compute $b_0, b_1, b_2, \cdots, b_d$ that satisfy $\forall x$, we have $L(x) = \prod_{i=1}^{d}(x - H_4(R_i \cdot e(g, g)^{ws})) + R = \sum_{i=0}^{d} b_i x^i$
$ct_4 \leftarrow \hat{H}(K) \oplus \hat{H}(R) \oplus (m || \sigma)$
$V_i \leftarrow e(v_4, (g_0 g_1^{id_i})^s), \forall i \in \{1, 2, \cdots, d\}$
Compute $c_0, c_1, c_2, \cdots, c_d$ that satisfy $\forall x$, we have $G(x) = \prod_{i=1}^{d}(x - H_4(V_i \cdot e(g, g)^{-s})) = \sum_{i=0}^{d} c_i x^i$
$ct_5 \leftarrow g^r$
$ct_6 \leftarrow H_5(ct_1 || ct_2 || \cdots || ct_5 || a_0 || a_1 || \cdots || a_d || b_0 || b_1 || \cdots || b_d || c_0 || c_1 || \cdots || c_d)^r$
$ct \leftarrow (ct_1, ct_2, ct_3, ct_4, ct_5, ct_6)$
return ct

1.6 $\mathbf{Dec}(\boldsymbol{dk_{id_R}}, \boldsymbol{id}_R, \boldsymbol{id}_S, \boldsymbol{ct}) \rightarrow m$

if $e(ct_5, H_5(ct_1 || ct_2 || \cdots || ct_5 || a_0 || a_1 || \cdots || a_d || b_0 || b_1 || \cdots || b_d || c_0 || c_1 || \cdots c_d)) = e(ct_6, g)$
then
  $K'' \leftarrow H_4(e(dk_1, H_1(id_S)) \cdot e(H_2(id_R), ct_1))$
  $R'' \leftarrow H_4(e(dk_2, ct_2) \cdot e(dk_3, ct_3))$
  $K' \leftarrow \sum_{i=0}^{d} a_i K''^i$
  $R' \leftarrow \sum_{i=0}^{d} b_i R''^i$
  $m || \sigma \leftarrow ct_4 \oplus \hat{H}(K') \oplus \hat{(H)}(R')$
  $r \leftarrow H_3(\sigma || m)$
  if $ct_5 \neq g^r$ **then**
    $m \leftarrow \perp$
  end if
else
  $m \leftarrow \perp$
end if
return m

1.7 ReceiverVerify($\boldsymbol{ct}, \boldsymbol{td_{id_R}}$) $\to y, y \in \{0, 1\}$

if $e(ct_5, H_5(ct_1||ct_2||\cdots||ct_5||a_0||a_1||\cdots||a_d||b_0||b_1||\cdots||b_d||c_0||c_1||\cdots c_d)) = e(ct_6, g)$
then
  $V' \leftarrow H_4(e(td_1, ct_2) \cdot e(td_2, ct_3))$
  $y \leftarrow \sum_{i=0}^{d} c_i V'^i = 0$
else
  $y \leftarrow 0$
end if
return y