1 SchemeARES

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

1.1 Setup() → (*mpk*, *msk*)

$g \leftarrow 1_{\mathbb{G}_1}$
generate $g_0, g_1 \in \mathbb{G}_1$ randomly
generate $w, t_1, t_2, t_3, t_4 \in \mathbb{Z}_r$
$\Omega \leftarrow e(g,g)^{t_1 t_2 w}$
$v \leftarrow g^{t_1}$
$v \leftarrow g^{t_2}$
$v \leftarrow g^{t_3}$
$v \leftarrow g^{t_4}$
$mpk \leftarrow (Omega, g, g_0, g_1, v_1, v_2, v_3, v_4)$
$msk \leftarrow (w, t_1, t_2, t_3, t_4)$
return (mpk, msk)

1.2 Extract(*Id*) → Pvk_{Id}

generate $r1, r2 \in \mathbb{Z}_r$ randomly
$d_0 \leftarrow g^{r_1 t_1 t_2 + r_2 t_3 t_4}$
$d_1 \leftarrow g^{-wt_2} \cdot (g_0 g_1^{Id})^{-r_1 t_2}$
$d_2 \leftarrow g^{-wt_1} \cdot (g_0 g_1^{Id})^{-r_1 t_1}$
$d_3 \leftarrow (g_0 g_1^{Id})^{-r_2 t_4}$
$d_4 \leftarrow (g_0 g_1^{Id})^{-r_2 t_3}$
$Pvk_{Id} \leftarrow (d_0, d_1, d_2, d_3, d_4)$
return Pvk_{Id}

1.3 TSK(*Id*) → Pvk_{Id}

generate $r1, r2 \in \mathbb{Z}_r$ randomly
$d_0 \leftarrow g^{r_1 t_1 t_2 + r_2 t_3 t_4}$
$d_1 \leftarrow (g_0 g_1^{Id})^{-r_1 t_2}$
$d_2 \leftarrow (g_0 g_1^{Id})^{-r_1 t_1}$
$d_3 \leftarrow (g_0 g_1^{Id})^{-r_2 t_4}$
$d_4 \leftarrow (g_0 g_1^{Id})^{-r_2 t_3}$
$Pvk_{Id} \leftarrow (d_0, d_1, d_2, d_3, d_4)$
return Pvk_{Id}

1.4 Encrypt(*Id*, m) → *CT*

generate $s, s_1, s_2 \in \mathbb{Z}_r$ randomly
$C' \leftarrow \Omega^s M$
$(g_0 g_1^{Id})^s$
$C_1 \leftarrow v_1^{s-s_1}$
$C_2 \leftarrow v_2^{s_1}$
$C_3 \leftarrow v_3^{s-s_2}$
$C_4 \leftarrow v_4^{s_2}$
$CT \leftarrow (C', C_0, C_1, C_2, C_3, C_4)$

return CT

1.5 Decrypt($\boldsymbol{Pvk_{id}}$, $\boldsymbol{CT}$) $\rightarrow M$

$M \leftarrow C' \cdot e(C_0, d_0) \cdot e(C_1, d_1) \cdot e(C_2, d_2) \cdot e(C_3, d_3) \cdot e(C_4, d_4)$
return M

1.6 TVerify($\boldsymbol{Pvk_{id}}$, $\boldsymbol{CT}$) $\rightarrow y, y \in \{0, 1\}$

return $e(C_0, d_0) \cdot e(C_1, d_1) \cdot e(C_2, d_2) \cdot e(C_3, d_3) \cdot e(C_4, d_4) = 1(\mathbb{G}_T)$