1 SchemePBAC

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

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

$q \leftarrow \|\mathbb{G}\|$
$g \leftarrow 1_{\mathbb{G}_1}$
generate $s, \alpha \in \mathbb{Z}_r$ randomly
$H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$H_2 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$H_3 : \mathbb{G}_T^2 \times \{0,1\}^\lambda \rightarrow \mathbb{Z}_r$
$H_4 : \{0,1\}^* \rightarrow \{0,1\}^\lambda$
$H_5 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$H_6 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$\hat{g} \leftarrow g^s$
$mpk \leftarrow (g, \hat{g}, H_1, H_2, H_3, H_4, H_5, H_6)$
$msk \leftarrow (s, \alpha)$
return (mpk, msk)

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

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

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

$dk_{id_R,1} \leftarrow H_2(id_R)^\alpha$
$dk_{id_R,2} \leftarrow H_2(id_R)^s$
$dk_{id_R} \leftarrow (dk_{id_R,1}, dk_{id_R,2})$
return dk_{id_R}

1.4 $\mathbf{Enc}(\boldsymbol{ek}_{\boldsymbol{id}_1}, \boldsymbol{id}_2, m) \rightarrow C$

generate $\eta_1, \eta_2 \in \mathbb{G}_T$ randomly
$r \leftarrow H_3(\eta_1, \eta_2, m)$
$C_1 \leftarrow g^r$
$C_2 \leftarrow \eta_1 \cdot e(\hat{g}, H_2(id_2)^r)$
$C_3 \leftarrow \eta_2 \cdot e(ek_{id_1}, H_2(id_2))$
$C_4 \leftarrow m \oplus H_4(\eta_1) \oplus H_4(\eta_2)$
$S \leftarrow H_5(id_2 || C_1 || C_2 || C_3 || C_4)^r$
$C \leftarrow (C_1, C_2, C_3, C_4, S)$
return C

1.5 $\mathbf{PKGen}(\boldsymbol{ek}_{\boldsymbol{id}_2}, \boldsymbol{dk}_{\boldsymbol{id}_2}, \boldsymbol{id}_1, \boldsymbol{id}_2, \boldsymbol{id}_3) \rightarrow \boldsymbol{rk}$

generate $N_1 \in \{0,1\}^\lambda$ randomly
generate $N_2 \in \{0,1\}^\lambda$ randomly
$K_1 \leftarrow e(dk_{id_2,2}, H_2(id_3))$
$K_2 \leftarrow e(ek_{id_2}, H_2(id_3))$

$rk_1 \leftarrow (N_1, H_6(K_1||id_2||id_3||N_1) \cdot dk_{id_2,2})$
$rk_2 \leftarrow (N_2, H_6(K_2||id_2||id_3||N_2) \cdot dk_{id_2,1})$
$rk \leftarrow (id_1, id_2, rk_1, rk_2)$
return rk

1.6 ProxyEnc($\boldsymbol{ct}, \boldsymbol{rk}$) $\rightarrow \boldsymbol{CT}$

$h \leftarrow H_5(id_2||C_1||C_2||C_3||C_4)$
if $e(h, C_1) = e(g, S)$**then**
generate $t \in \mathbb{Z}_r$ randomly
$C_2' \leftarrow C_2 / \dfrac{e(C_1, rk_{1,2} \cdot h^t)}{e(g^t, S)}$
$C_3' \leftarrow C_3 / e(H_1(id_1), rk_{2,2})$
$CT \leftarrow (id_1, C_1, C_2', C_3', C_4, rk_{1,1}, rk_{2,1})$
else
$CT \leftarrow \perp$
end if
return CT

1.7 $\mathbf{Dec}_1(\boldsymbol{dk_{id_2}}, \boldsymbol{id}_2, \boldsymbol{id}_1, \boldsymbol{ct}) \rightarrow m$

$h \leftarrow H_5(id_2||C_1||C_2||C_3||C_4)$
generate $t \in \mathbb{Z}_r$ randomly
$\eta_1 \leftarrow C_2 / \dfrac{e(C_1, dk_{id_2,2} \cdot h^t)}{e(g^t, S)}$
$\eta_2 \leftarrow C_3 / e(dk_{id_2,1}, H_1(id_1))$
$m \leftarrow C_4 \oplus H_4(\eta_1) \oplus H_4(\eta_2)$
$r \leftarrow H_3(\eta_1, \eta_2, m)$
if $S \neq h^r \vee C_1 \neq g^r$ **then**
$m \leftarrow \perp$
end if
return m

1.8 $\mathbf{Dec}_2(\boldsymbol{dk_{id_3}}, \boldsymbol{id}_3, \boldsymbol{id}_2, \boldsymbol{CT}) \rightarrow m'$

$K_1' \leftarrow e(dk_{id_3,2}, H_2(id_2))$
$K_2' \leftarrow e(dk_{id_3,1}, H_1(id_2))$
$\eta_1' \leftarrow C_2' \cdot e(C_1, H_6(K_1'||id_2||id_3||N_1))$
$\eta_2' \leftarrow C_3' \cdot e(H_6(K_2'||id_2||id_3||N_2), H_1(id_1))$
$m' \leftarrow C_4 \oplus H_4(\eta_1') \oplus H_4(\eta_2')$
$r' \leftarrow H_3(\eta_1', \eta_2', m')$
if $C_1 \neq g^{r'}$ **then**
$m' \leftarrow \perp$
end if
return m'