1 SchemePBAC

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

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

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

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

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

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

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

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

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($\boldsymbol{ct}, \boldsymbol{rk}$) $\rightarrow$ $\boldsymbol{ct'}$

If $e(ct_1, g) = e(h, ct_2) \wedge e(ct_1, H_5(ct_1||ct_2||ct_3||ct_4)) = e(h, ct_5)$ **then**
$ct'_4 \leftarrow \frac{ct_4}{rk_3}$
$ct_6 \leftarrow rk_1$
$ct_7 \leftarrow \frac{e(rk_2, ct_2)}{e(ct_1, rk_1)}$
$ct' \leftarrow (ct_2, ct_3, ct'_4, ct_6, ct_7, N)$
else
$ct' \leftarrow \perp$
return ct'

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

If $e(ct_1, g) = e(h, ct_2) \wedge e(ct_1, H_5(ct_1||ct_2||ct_3||ct_4)) = e(h, ct_5)$:
$V \leftarrow e(dk_{id_2,2}, H_2(id_1))$
$\eta' \leftarrow \frac{ct_4}{V}$
$r \leftarrow H_3((ct_3 \oplus H_4(e(dk_{id_2,1})) \oplus H_4(\eta'))||\eta')$
If $g^r = ct_2$:
return m

1.8 $\text{Dec}_2(\boldsymbol{dk_{id_3}}, \boldsymbol{id}_1, \boldsymbol{id}_2, \boldsymbol{id}_3, \boldsymbol{ct'})$ $\rightarrow m$

$V \leftarrow e(dk_{id_3,2}, H_2(id_2))$
$\eta' \leftarrow ct'_4 \cdot e(H_2(id_1), H_7(V||id_2||id_3||N))$
$R \leftarrow \frac{ct_7}{e(H_6(e(dk_{id_3,1}, ct_6), ct_2)}$
$r \leftarrow H_3((ct_3 \oplus H_4(R) \oplus H_4(\eta'))||\eta')$
If $g^r = ct_2$:
return m