

1 SchemePBAC

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

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

1.2 SKGen(*id_S*) \rightarrow *ek_{id_S}*

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

1.3 RKGen(*id_R*) \rightarrow *dk_{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 Enc(*ek_{id₁}*, *id₂*, *m*) \rightarrow *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 PKGen(*ek_{id₂}*, *dk_{id₂}*, *id₁*, *id₂*, *id₃*) \rightarrow *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(ct, rk) $\rightarrow CT$

$h \leftarrow H_5(id_2 || C_1 || C_2 || C_3 || C_4)$
if $e(h, C_1) = e(g, S)$ **then**
 generate $t \in \mathbb{Z}_r$ randomly
 $C'_2 \leftarrow C_2 / \frac{e(C_1, rk_{1,2} \cdot h^t)}{e(g^t, S)}$
 $C'_3 \leftarrow C_3 / e(H_1(id_1), rk_{2,2})$
 $CT \leftarrow (id_1, C_1, C'_2, C'_3, C_4, rk_{1,1}, rk_{2,1})$
else
 $CT \leftarrow \perp$
end if
return CT

1.7 Dec₁($dk_{id_2}, id_2, id_1, ct$) $\rightarrow m$

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

1.8 Dec₂($dk_{id_3}, id_3, id_2, CT$) $\rightarrow m'$

$K'_1 \leftarrow e(dk_{id_3,2}, H_2(id_2))$
 $K'_2 \leftarrow e(dk_{id_3,1}, H_1(id_2))$
 $\eta'_1 \leftarrow C'_2 \cdot e(C_1, H_6(K'_1 || id_2 || id_3 || N_1))$
 $\eta'_2 \leftarrow C'_3 \cdot e(H_6(K'_2 || id_2 || id_3 || N_2), H_1(id_1))$
 $m' \leftarrow C_4 \oplus H_4(\eta'_1) \oplus H_4(\eta'_2)$
 $r' \leftarrow H_3(\eta'_1, \eta'_2, m')$
if $C_1 \neq g^{r'}$ **then**
 $m' \leftarrow \perp$
end if
return m'