1 SchemeIBPME

This scheme is applicable to symmetric and asymmetric groups of prime orders.

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

$q \leftarrow \|\mathbb{G}\|$
$g \leftarrow 1_{\mathbb{G}_1}$
$\hat{g} \leftarrow 1_{\mathbb{G}_2}$
generate $s, \alpha, \beta_0, \beta_1 \in \mathbb{Z}_r$ randomly
$g_1 \leftarrow g^{\alpha}$
$f \leftarrow g^{\beta_0}$
$\hat{f} \leftarrow \hat{g}^{\beta_0}$
$h \leftarrow g^{\beta_1}$
$\hat{h} \leftarrow \hat{g}^{\beta_1}$
$H : \mathbb{G}_T \rightarrow \mathbb{Z}_r$
$H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$
$H_2 : \{0,1\}^* \rightarrow \mathbb{G}_2$
$H_3 : \mathbb{G}_T \rightarrow \mathbb{Z}_r$
$H_4 : \{0,1\}^{\lambda} \times \mathbb{G}_T^2 \times \mathbb{G}_1^2 \rightarrow \{0,1\}^{\lambda}$
$H_5 : \{0,1\}^{\lambda} \times \mathbb{G}_T^2 \times \mathbb{G}_1^2 \rightarrow \{0,1\}^{\lambda}$
$H_6 : \mathbb{G}_T \rightarrow \{0,1\}^{3\lambda}$
$H_7 : \mathbb{G}_T \rightarrow \{0,1\}^{2\lambda}$
$mpk \leftarrow (g, \hat{g}, g_1, f, h, \hat{f}, \hat{h}, H, H_1, H_2, H_3, H_4, H_5, H_6, H_7)$
$msk \leftarrow (s, \alpha)$
return (mpk, msk)

1.2 SKGen(σ) → $\boldsymbol{ek}_\sigma$

$ek_\sigma \leftarrow H_1(\sigma)^s$
return ek_σ

1.3 RKGen(ρ) → $\boldsymbol{dk}_\rho$

$d_1 \leftarrow H_2(\rho)^s$
$d_2 \leftarrow H_2(\rho)^{\alpha}$
$dk_\rho \leftarrow (d_1, d_2)$
return dk_ρ

1.4 PKGen($\boldsymbol{dk}_\rho, \sigma$) → $\boldsymbol{pdk}_{\rho,\sigma}$

generate $y \leftarrow \mathbb{Z}_r$ randomly
$\eta \leftarrow e(H_1(\sigma), d_1)$
$y_1 \leftarrow d_2^{H_3(\eta)}(\hat{f}\hat{h}^{H(\eta)})^y$
$y_2 \leftarrow \hat{g}^y$
$pdk_{(\rho,\sigma)} \leftarrow (y_1, y_2)$
return $pdk_{(\rho,\sigma)}$

1.5 $\mathbf{Enc}(\boldsymbol{ek}_\sigma, \boldsymbol{id}_2, m) \to \boldsymbol{ct}$

generate $r \in \mathbb{Z}_r$ randomly
$\eta \leftarrow e(ek_\sigma, H_2(\rho))$
$K_R \leftarrow e(g_1, H_2(\rho))^{r \cdot H_3(\eta)}$
$C_1 \leftarrow g^r$
$C_2 \leftarrow (fh^{H(\eta)})^r$
$K_C \leftarrow H_4(m, \eta, K_R)$
$Y \leftarrow H_5(m, K_C, K_R, C_1, C_2)$
$C_3 \leftarrow (m||K_C||Y) \oplus H_6(K_R)$
$C \leftarrow (C_1, C_2, C_3)$
return C

1.6 $\mathbf{ProxyDec}(\boldsymbol{pdk}, C) \to \boldsymbol{CT}$

$K_R \leftarrow e(C_1, y_1)/e(C_2, y_2)$
$m||K_C||Y \leftarrow C_3 \oplus H_6(K_R)$
if $Y = H_5(m, K_C, K_R, C_1, C_2)$**then**
$CT_1 \leftarrow C_1$
$CT_2 \leftarrow (m||K_C) \oplus H_7(K_R)$
$CT \leftarrow (CT_1, CT_2)$
else
  $CT \leftarrow \perp$
end if
return CT

1.7 $\mathbf{Dec}_1(\boldsymbol{dk}_\rho, \sigma, C) \to m$

$\eta \leftarrow e(H_1(\sigma), d_1)$
$K_R \leftarrow e(C_1, d_2^{H_3(\eta)})$
$m||K_C||Y \leftarrow C_3 \oplus H_6(K_R)$
if $K_C \neq H_4(m, \eta, K_R) \vee Y \neq H_5(m, K_C, K_R, C_1, C_2)$**then**
  $m \leftarrow \perp$
end if
return m

1.8 $\mathbf{Dec}_1(\boldsymbol{dk}_\rho, \sigma, \boldsymbol{CT}) \to m'$

$\eta \leftarrow e(H_1(\sigma), d_1)$
$K_R \leftarrow e(C_1, d_2^{H_3(\eta)})$
$m||K_C \leftarrow CT_2 \oplus H_7(K_R)$
if $K_C \neq H_4(m, \eta, K_R)$**then**
  $m \leftarrow \perp$
end if
return m