1 SchemeIBMECH

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

1.1 SKGen(σ) $\to$ $\boldsymbol{ek}_\sigma$

generate $r \in \mathbb{Z}_p^*$
$ek_\sigma \leftarrow \frac{\boldsymbol{d}_{3,i}^{\eta+r\sigma}}{\boldsymbol{d}_{4,i}^{r}}, \forall i \in \{1,2,\cdots,8\}$
return ek_σ

1.2 RKGen(ρ) $\to$ $\boldsymbol{dk}_\rho$

generate $s, s_1, s_2 \in \mathbb{Z}_p^*$ randomly
$k_1 \leftarrow \{g_2^{\boldsymbol{d}_{1,i}\cdot(\alpha+s_1\rho)-s_1\boldsymbol{d}_{2,i}+s\boldsymbol{d}_{3,i}}, \forall i \in \{1,2,\cdots,8\}\}$
$k_2 \leftarrow \{g_2^{s_2\cdot(\rho*\boldsymbol{d}_{1,i}-\boldsymbol{d}_{2,i})+s\boldsymbol{d}_{4,i}}, \forall i \in \{1,2,\cdots,8\}\}$
$k_3 \leftarrow (g_T^{\eta})^s$
$dk_\rho \leftarrow (k_1, k_2, k_3)$
return dk_ρ

1.3 Enc($\boldsymbol{ek}_\sigma, \boldsymbol{rcv}, m$) $\to$ $\boldsymbol{ct}$

generate $z \leftarrow \mathbb{Z}_p^*$ randomly
$C \leftarrow \{\boldsymbol{d}_{1,i}^{z}\boldsymbol{d}_{2,i}^{z\cdot rcv}\cdot(ek_\sigma)_i, \forall i \in \{1,2,\cdots,8\}\}$
$C_0 \leftarrow (g_T^{\alpha})^z m$
$ct \leftarrow (C, C_0)$
return ct

1.4 Dec($\boldsymbol{dk}_\rho, \boldsymbol{snd}, \boldsymbol{ct}$) $\to$ m

$m \leftarrow \frac{C_0 k_3}{\prod_{i=1}^{8} e(C_i, k_{1,i}k_{2,i}^{snd})}$
return m