1 Scheme

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

generate $g_1 \in \mathbb{G}_1$ randomly
generate $g_2 \in \mathbb{G}_2$ randomly
$q \leftarrow \|\mathbb{G}\|$
generate $\alpha, \eta \in \mathbb{Z}_p^*$ randomly
generate $\mathbf{0}_{\mathbb{Z}_p^*}, \mathbf{1}_{\mathbb{Z}_p^*} \in \mathbb{Z}_p^*$ randomly
generate $\boldsymbol{B} \leftarrow (\mathbb{Z}_p^*)^{8\times 8}$ randomly
$\mathbb{D}_{i,j} \leftarrow g_1^{\boldsymbol{B}_{i,j}}, \forall i \in \{1,2,3,4\}, \forall j \in \{1,2,\cdots,8\}$
$\mathbb{D}_i^* \leftarrow \mathit{GaussEliminationinGroups}(\boldsymbol{B}||[1=i, 2=i, \cdots, 8=i]^{\mathrm{T}}), \forall i \in \{1,2,3,4\}$
$g_T \leftarrow e(g_1, g_2)$
$mpk \leftarrow (g_T^{\alpha\times\mathbf{1}_{\mathbb{Z}_p^*}}, g_T^{\eta\times\mathbf{1}_{\mathbb{Z}_p^*}}, D_1, D_2)$
$msk \leftarrow (\alpha, \eta, g_1, g_2, \boldsymbol{d}_3, \boldsymbol{d}_4, \boldsymbol{d}_1^*, \boldsymbol{d}_2^*, \boldsymbol{d}_3^*, \boldsymbol{d}_4^*)$ **return** (mpk, msk)

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

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