

1 SchemeIBME

This scheme is only applicable to symmetric groups of prime orders.

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

generate $r, s \in \mathbb{Z}_p^*$ randomly
generate $P \in \mathbb{G}_1$ randomly
 $P_0 \leftarrow r \cdot P$
 $H_1 : \mathbb{Z}_p^* \rightarrow \mathbb{G}_1$
generate *mask*, $\|mask\| \leftarrow \|e\|, e \in \mathbb{Z}_p^*$ randomly
 $H' : \mathbb{Z}_p^* \oplus mask \rightarrow \mathbb{G}_1$
 $mpk \leftarrow (P, P_0, H, H')$
 $msk \leftarrow (r, s)$
return (*mpk*, *msk*)

1.2 SKGen(*S*) \rightarrow *ek_S*

$ek_S \leftarrow s \cdot H'(S)$
return *ek_S*

1.3 RKGen(*S*) \rightarrow *dk_R*

$H_R \leftarrow H(R)$
 $dk_1 \leftarrow r \cdot H_R$
 $dk_2 \leftarrow s \cdot H_R$
 $dk_3 \leftarrow H_R$
 $dk_R \leftarrow (dk_1, dk_2, dk_3)$
return *dk_R*

1.4 Enc(*ek_S*, *R*, *M*) \rightarrow *C*

generate $u, t \in \mathbb{Z}_p^*$ randomly
 $T \leftarrow t \cdot P$
 $U \leftarrow u \cdot P$
 $H_R \leftarrow H(R)$
 $k_R \leftarrow e(H_R, u \cdot P_0)$
 $k_S \leftarrow e(H_R, T + ek_S)$
 $V \leftarrow M \oplus k_R \oplus k_S$
 $C \leftarrow (T, U, V)$
return *C*

1.5 Dec(*dk_R*, *S*, *C*) \rightarrow *M*

$k_R \leftarrow e(dk_1, U)$
 $H'_S \leftarrow H'(S)$
 $k_S \leftarrow e(dk_3, T)$
 $M \leftarrow V \oplus k_R \oplus k_S$
return *M*