

# 1 SchemeIBPRME

## 1.1 Setup() $\rightarrow$ ( $mpk, msk$ )

$q \leftarrow \|\mathbb{G}\|$   
 $g \leftarrow 1_{\mathbb{G}_1}$   
 generate  $h \in \mathbb{G}_1$  randomly  
 generate  $x, \alpha \in \mathbb{Z}_r$  randomly  
 $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$   
 $H_2 : \{0, 1\}^* \rightarrow \mathbb{G}_1$   
 $H_3 : \{0, 1\}^* \rightarrow \mathbb{Z}_r$   
 $H_4 : \{0, 1\}^* \rightarrow \mathbb{G}_1^2$   
 $H_5 : \{0, 1\}^* \rightarrow \mathbb{G}_1$   
 $H_6 : \{0, 1\}^* \rightarrow \mathbb{G}_1$   
 $H_7 : \{0, 1\}^* \rightarrow \mathbb{G}_1$   
 $y \leftarrow g^x$   
 $mpk \leftarrow (G, G_T, q, g, e, h, H_1, H_2, H_3, H_4, H_5, H_6, H_7, y)$   
 $msk \leftarrow (x, \alpha)$   
**return** ( $mpk, msk$ )

## 1.2 DKGen( $id_R$ ) $\rightarrow dk_{id_R}$

$dk_{id_R,1} \leftarrow H_1(id_R)^x$   
 $dk_{id_R,2} \leftarrow H_1(id_R)^\alpha$   
 $dk_{id_R} \leftarrow (dk_{id_R,1}, dk_{id_R,2})$   
**return**  $dk_{id_R}$

## 1.3 EKGen( $id_S$ ) $\rightarrow ek_{id_S}$

$ek_{id_S} \leftarrow H_2(id_S)^\alpha$   
**return**  $ek_{id_S}$

## 1.4 ReEKGen( $ek_{id_2}, dk_{id_2}, id_1, id_2, id_3$ ) $\rightarrow rk$

generate  $N \in \{0, 1\}^\lambda$  randomly  
 generate  $\bar{x} \in \mathbb{Z}_r$  randomly  
 $rk_1 \leftarrow g^{\bar{x}}$   
 $rk_2 \leftarrow dk_{id_2,1} h^{\bar{x}} H_6(e(y, H_1(id_3))^{\bar{x}})$   
 $K \leftarrow e(ek_{id_2}, H_1(id_3))$   
 $rk_3 \leftarrow e(H_2(id_1), H_7(K || id_2 || id_3 || N) \cdot dk_{id_2,2})$   
 $rk \leftarrow (N, rk_1, rk_2, rk_3)$   
**return**  $rk$

## 1.5 Enc( $ek_{id_1}, id_2, m$ ) $\rightarrow ct$

generate  $\sigma \in \mathbb{G}_1$  randomly  
 generate  $\eta \in \mathbb{G}_T$  randomly  
 $r \leftarrow H_3(m || \sigma || \eta)$   
 $ct_1 \leftarrow h^r$   
 $ct_2 \leftarrow g^r$   
 $ct_3 \leftarrow (m || \sigma) \oplus H_4(e(y, H_1(id_2))^r) \oplus H_4(\eta)$

$ct_4 \leftarrow \eta \cdot e(ek_{id_1}, H_1(id_2))$   
 $ct_5 \leftarrow H_5(ct_1 || ct_2 || ct_3 || ct_4)^r$   
 $ct \leftarrow (ct_1, ct_2, ct_3, ct_4, ct_5)$   
**return**  $ct$

### 1.6 ReEnc( $ct, rk$ ) $\rightarrow ct'$

**If**  $e(ct_1, g) = e(h, ct_2) \wedge e(ct_1, H_5(ct_1 || ct_2 || ct_3 || ct_4)) = e(h, ct_5)$  **then**  
 $ct'_4 \leftarrow \frac{ct_4}{rk_3}$   
 $ct_6 \leftarrow rk_1$   
 $ct_7 \leftarrow \frac{e(rk_2, ct_2)}{e(ct_1, rk_1)}$   
 $ct' \leftarrow (ct_2, ct_3, ct'_4, ct_6, ct_7, N)$   
**else**  
 $ct' \leftarrow \perp$   
**return**  $ct'$

### 1.7 Dec<sub>1</sub>( $dk_{id_2}, id_1, ct$ ) $\rightarrow m$

**If**  $e(ct_1, g) = e(h, ct_2) \wedge e(ct_1, H_5(ct_1 || ct_2 || ct_3 || ct_4)) = e(h, ct_5)$ :  
 $V \leftarrow e(dk_{id_2, 2}, H_2(id_1))$   
 $\eta' \leftarrow \frac{ct_4}{V}$   
 $r \leftarrow H_3((ct_3 \oplus H_4(e(dk_{id_2, 1})) \oplus H_4(\eta')) || \eta')$   
**If**  $g^r = ct_2$ :  
**return**  $m$

### 1.8 Dec<sub>2</sub>( $dk_{id_3}, id_1, id_2, id_3, ct'$ ) $\rightarrow m$

$V \leftarrow e(dk_{id_3, 2}, H_2(id_2))$   
 $\eta' \leftarrow ct'_4 \cdot e(H_2(id_1), H_7(V || id_2 || id_3 || N))$   
 $R \leftarrow \frac{ct_7}{e(H_6(e(dk_{id_3, 1}, ct_6), ct_2))}$   
 $r \leftarrow H_3((ct_3 \oplus H_4(R) \oplus H_4(\eta')) || \eta')$   
**If**  $g^r = ct_2$ :  
**return**  $m$