

# 1 SchemeAnonymousME

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

$g \leftarrow 1_{\mathbb{G}_1}$   
 generate  $\alpha, b_1, b_2 \in \mathbb{Z}_r$  randomly  
 generate  $g_2, g_3 \in \mathbb{G}_2$  randomly  
 generate  $h_1, h_2, \dots, h_l \in \mathbb{G}_2$  randomly (Note that the indexes in implementations are 1 smaller than those in theory)  
 $g_1 \leftarrow g^\alpha$   
 $\bar{g} \leftarrow g^{b_1}$   
 $\tilde{g} \leftarrow g^{b_2}$   
 $\bar{g}_3 \leftarrow g_3^{\frac{1}{b_1}}$   
 $\tilde{g}_3 \leftarrow g_3^{\frac{1}{b_2}}$   
 $mpk \leftarrow (g, g_1, g_2, g_3, \bar{g}, \tilde{g}, \bar{g}_3, \tilde{g}_3, h_1, h_2, \dots, h_l)$   
 $msk \leftarrow (g_2^\alpha, b_1, b_2)$   
**return** ( $mpk, msk$ )

## 1.2 KGen( $ID_k$ ) $\rightarrow sk_{ID_k}$

generate  $r \in \mathbb{Z}_r$  randomly  
 $HI \leftarrow h_1^{I_1} h_2^{I_2} \dots h_k^{I_k}$   
 $sk_{ID_k} \leftarrow (g_2^{\frac{r}{b_1}} \cdot HI^{\frac{r}{b_1}} \cdot \bar{g}_3^r, g_2^{\frac{r}{b_2}} \cdot HI^{\frac{r}{b_2}} \cdot \tilde{g}_3^r, g^r, h_{k+1}^{\frac{r}{b_1}}, h_{k+2}^{\frac{r}{b_1}}, \dots, h_l^{\frac{r}{b_1}}, h_{k+1}^{\frac{r}{b_2}}, h_{k+2}^{\frac{r}{b_2}}, \dots, h_l^{\frac{r}{b_2}}, h_{k+1}^{b_1^{-1}}, h_{k+2}^{b_1^{-1}}, \dots, h_l^{b_1^{-1}}, h_{k+1}^{b_2^{-1}}, h_{k+2}^{b_2^{-1}}, \dots, h_l^{b_2^{-1}}, h_{k+1}^{b_1^{-1}}, h_{k+2}^{b_1^{-1}}, \dots, h_l^{b_1^{-1}}, h_{k+1}^{b_2^{-1}}, h_{k+2}^{b_2^{-1}}, \dots, h_l^{b_2^{-1}})$   
**return**  $sk_{ID_k}$

## 1.3 DerivedKGen( $sk_{ID_{k-1}}, ID_k$ ) $\rightarrow sk_{ID_k}$

generate  $t \in \mathbb{Z}_r$  randomly  
 $sk_{ID_k} \leftarrow (a_0 \cdot c_{0,k}^{I_k} \cdot (f_0 \cdot d_{0,k}^{I_k} \cdot \bar{g}_3)^t, a_1 \cdot c_{1,k}^{I_k} \cdot (f_1 \cdot d_{1,k}^{I_k} \cdot \tilde{g}_3)^t, b \cdot g^t, c_{0,k+1} \cdot d_{0,k+1}^t, c_{0,k+2} \cdot d_{0,k+2}^t, \dots, c_{0,l} \cdot d_{0,l}^t, c_{1,k+1} \cdot d_{1,k+1}^t, c_{1,k+2} \cdot d_{1,k+2}^t, \dots, c_{1,l} \cdot d_{1,l}^t, d_{0,k+1}, d_{0,k+2}, \dots, d_{0,l}, d_{1,k+1}, d_{1,k+2}, \dots, d_{1,l}, f_0 \cdot c_{0,k}^{I_k}, f_1 \cdot c_{1,k}^{I_k})$   
**return**  $sk_{ID_k}$

## 1.4 Enc( $ID_k, M$ ) $\rightarrow CT$

generate  $s_1, s_2 \in \mathbb{Z}_r$  randomly  
 $CT \leftarrow (e(g_1, g_2)^{s_1+s_2} \cdot M, \bar{g}^{s_1}, \tilde{g}^{s_2}, (h_1^{I_1} h_2^{I_2} \dots h_k^{I_k} \cdot g_3)^{s_1+s_2})$   
**return**  $CT$

## 1.5 Dec( $CT, sk_{ID_k}$ ) $\rightarrow M$

$M \leftarrow \frac{e(b, D) \cdot A}{e(B, a_0) \cdot e(C, a_1)}$   
**return**  $M$