

# 1 SchemeCANIFPPCT

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

$p \leftarrow \|\mathbb{G}\|$   
 $g_1 \leftarrow 1_{\mathbb{G}_1}$   
 $g_2 \leftarrow 1_{\mathbb{G}_2}$   
 generate  $g_3 \in \mathbb{G}_1$  randomly  
 $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}_1$   
 $H_2 : \mathbb{G}_T \rightarrow \mathbb{Z}_r$   
 $H_3 : \{0, 1\}^* \rightarrow \mathbb{Z}_r$   
 $H_4 : \mathbb{G}_1 \rightarrow \mathbb{Z}_r$   
 generate  $r, s, t, \omega, t_1, t_2, t_3, t_4 \in \mathbb{Z}_r$  randomly  
 $R \leftarrow g_1^r$   
 $S \leftarrow g_2^s$   
 $T \leftarrow g_1^t$   
 $\Omega \leftarrow e(g_1, g_2)^{t_1 t_2 \omega}$   
 $v_1 \leftarrow g_2^{t_1}$   
 $v_2 \leftarrow g_2^{t_2}$   
 $v_3 \leftarrow g_2^{t_3}$   
 $v_4 \leftarrow g_2^{t_4}$   
 $mpk \leftarrow (g_1, g_2, p, g_3, H_1, H_2, H_3, H_4, R, S, T, \Omega, v_1, v_2, v_3, v_4)$   
 $msk \leftarrow (r, s, t, \omega, t_1, t_2, t_3, t_4)$   
**return** ( $mpk, msk$ )

## 1.2 KGen( $ID_i$ ) $\rightarrow$ ( $sk_{ID_i}, ek_{ID_i}$ )

generate  $k_i, x_i \in \mathbb{Z}_r$  randomly  
 $z_i \leftarrow (r - x_i)(sx_i)^{-1} \in \mathbb{Z}_r$   
 $Z_i \leftarrow g_1^{z_i} \in \mathbb{G}_1$   
 $sk_{ID_i} \leftarrow k_i$   
 $ek_{ID_i} \leftarrow (x_i, Z_i)$   
 $tag_i \leftarrow H_4(x_i \cdot Z_i)$   
**return** ( $sk_{ID_i}, ek_{ID_i}$ )

## 1.3 Encryption( $TP_S, ek_{ID_i}$ ) $\rightarrow CT_{TP_S}$

generate  $\vec{s} \leftarrow (s_1, s_2, \dots, s_n) \in \mathbb{Z}_r^n$  randomly  
 generate  $\vec{s}_1 \leftarrow (s_{1,1}, s_{1,2}, \dots, s_{1,n}) \in \mathbb{Z}_r^n$  randomly  
 generate  $\vec{s}_2 \leftarrow (s_{2,1}, s_{2,2}, \dots, s_{2,n}) \in \mathbb{Z}_r^n$  randomly  
 $V_i \leftarrow H_2(\Omega^{s_i}), \forall i \in \{1, 2, \dots, n\}$   
 $\vec{C}_{i,0} \leftarrow (g_3 H_1(TP_S))^{s_i}, \forall i \in \{1, 2, \dots, n\}$   
 $\vec{C}_{i,1} \leftarrow v_1^{s_i - s_{i,1}}$   
 $\vec{C}_{i,2} \leftarrow v_2^{s_{i,1}}$   
 $\vec{C}_{i,3} \leftarrow v_3^{s_i - s_{i,2}}$   
 $\vec{C}_{i,4} \leftarrow v_4^{s_{i,2}}$   
 $f(x) := \prod_{i=1}^n (x - V_i)$   
 generate  $\alpha \in \mathbb{Z}_r$  randomly  
 $C_1 \leftarrow g_1^\alpha$

$C_2 \leftarrow Z_i^{x_i} + T^\alpha$   
 $C_3 \leftarrow e(T, S)^\alpha$   
**return**  $CT$

#### 1.4 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**  $sk_{ID_k}$

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

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