

1 SchemeHIBME

This scheme is applicable to symmetric and asymmetric groups of prime orders.

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

generate $g \in \mathbb{G}_1$ randomly
generate $\alpha, b_1, b_2 \in \mathbb{Z}_p^*$ randomly
generate $s_1, s_2, \dots, s_l, a_1, a_2, \dots, a_l \in \mathbb{Z}_p^*$ 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)
 $H_1 : \mathbb{Z}_p^* \rightarrow \mathbb{G}_1$
 $H_2 : \mathbb{Z}_p^* \rightarrow \mathbb{G}_2$
 $\hat{H} : \{0, 1\}^* \rightarrow \{0, 1\}^\lambda$
 $g_1 \leftarrow g^\alpha$
 $A \leftarrow e(g_1, g_2)$
 $\bar{g} \leftarrow g^{b_1}$
 $\tilde{g} \leftarrow g^{b_2}$
 $\bar{g}_3 \leftarrow g_3^{\frac{1}{b_1}}$
 $\tilde{g}_3 \leftarrow g_3^{\frac{1}{b_2}}$
 $mpk \leftarrow (g, g_1, g_2, g_3, \bar{g}, \tilde{g}, \bar{g}_3, \tilde{g}_3, h_1, h_2, \dots, h_l, H_1, H_2, \hat{H}, A)$
 $msk \leftarrow (g_2^\alpha, b_1, b_2, s_1, s_2, \dots, s_l, a_1, a_2, \dots, a_l)$
return (mpk, msk)

1.2 EKGen(ID_k) $\rightarrow ek_{ID_k}$

$A_k \leftarrow \prod_{j=1}^k a_j$
 $ek_{1,i} \leftarrow H_1(I_i)^{s_i A_k}, \forall i \in \{1, 2, \dots, k\}$
 $ek_{2,i} \leftarrow s_{k+i} A_k, \forall i \in \{1, 2, \dots, l-k\}$
 $ek_3 \leftarrow (a_{k+1}, a_{k+2}, \dots, a_l)$
 $ek_{ID_k} \leftarrow (ek_1, ek_2, ek_3)$
return ek_{ID_k}

1.3 DerivedEKGen($ek_{ID_{k-1}}, ID_k$) $\rightarrow ek_{ID_k}$

$ek'_{1,i} \leftarrow ek_{1,i}^{a_k}, \forall i \in \{1, 2, \dots, k-1\}$
 $ek'_{1,k} \leftarrow H_1(I_k)^{ek_{2,1}}$
 $ek'_1 \leftarrow ek'_1 || \langle ek'_{1,k} \rangle$
 $ek'_{2,i} \leftarrow ek_{2,i} \cdot a_k, \forall i \in \{2, 3, \dots, l-k+1\}$
 $ek'_3 \leftarrow (a_{k+1}, a_{k+2}, \dots, a_l)$
 $ek_{ID_k} \leftarrow (ek'_1, ek'_2, ek'_3)$
return ek_{ID_k}

1.4 DKGen(ID_k) $\rightarrow dk_{ID_k}$

generate $r \in \mathbb{Z}_p^*$ randomly

$$HI \leftarrow h_1^{I_1} h_2^{I_2} \cdots h_k^{I_k}$$

$$a_0 \leftarrow g_2^{\frac{\alpha}{b_1}} \cdot HI^{\frac{r}{b_1}} \cdot \bar{g}_3^r$$

$$a_1 \leftarrow g_2^{\frac{\alpha}{b_2}} \cdot HI^{\frac{r}{b_2}} \cdot \tilde{g}_3^r$$

$$A_k \leftarrow \prod_{j=1}^k a_j$$

$$dk_1 \leftarrow (a_0, a_1, g^r, h_{k+1}^{\frac{r}{b_1}}, h_{k+2}^{\frac{r}{b_1}}, \dots, h_l^{\frac{r}{b_1}}, h_{k+1}^{\frac{r}{b_2}}, h_{k+2}^{\frac{r}{b_2}}, \dots, h_l^{\frac{r}{b_2}}, h_{k+1}^{b_1^{-1}}, h_{k+2}^{b_1^{-1}}, \dots, h_l^{b_1^{-1}}, h_{k+1}^{b_2^{-1}}, h_{k+2}^{b_2^{-1}}, \dots, h_l^{b_2^{-1}}, HI^{\frac{1}{b_1}}, HI^{\frac{1}{b_2}})$$

$$dk_{2,i} \leftarrow H_2(I_i)^{s_i A_k}, \forall i \in \{1, 2, \dots, k\}$$

$$dk_{3,i} \leftarrow s_{k+i} A_k, \forall i \in \{1, 2, \dots, l-k\}$$

$$dk_4 \leftarrow (a_{k+1}, a_{k+2}, \dots, a_l)$$

$$dk_{ID_k} \leftarrow (dk_1, dk_2, dk_3, dk_4)$$

return dk_{ID_k}

1.5 DerivedDKGen($dk_{ID_{k-1}}, ID_k$) $\rightarrow dk_{ID_k}$

generate $t \in \mathbb{Z}_p^*$ randomly

$$a'_0 \leftarrow a_0 \cdot c_{0,k}^{I_k} \cdot (f_0 \cdot d_{0,k}^{I_k} \cdot \bar{g}_3)^t$$

$$a'_1 \leftarrow a_1 \cdot c_{1,k}^{I_k} \cdot (f_1 \cdot d_{1,k}^{I_k} \cdot \tilde{g}_3)^t$$

$$dk'_1 \leftarrow (a'_0, a'_1, b \cdot g^t, c_{0,k+1} \cdot d_{0,k+1}^t, c_{0,k+2} \cdot d_{0,k+2}^t, \dots, c_{0,l} \cdot d_{0,l}^t, c_{1,k+1} \cdot d_{1,k+1}^t, c_{1,k+2} \cdot d_{1,k+2}^t, \dots, c_{1,l} \cdot d_{1,l}^t, d_{0,k+1}, d_{0,k+2}, \dots, d_{0,l}, d_{1,k+1}, d_{1,k+2}, \dots, d_{1,l}, f_0 \cdot c_{0,k}^{I_k}, f_1 \cdot c_{1,k}^{I_k})$$

$$dk'_{2,i} \leftarrow dk_{2,i}^{a_k}, \forall i \in \{1, 2, \dots, k-1\}$$

$$dk'_{2,k} \leftarrow H_2(I_k)^{dk_{3,1}}$$

$$dk'_2 \leftarrow dk'_2 || \langle dk'_{2,k} \rangle$$

$$dk'_{3,i} \leftarrow dk_{3,i} \cdot a_k, \forall i \in \{2, 3, \dots, l-k+1\}$$

$$dk'_4 \leftarrow (a_{k+1}, a_{k+2}, \dots, a_l)$$

$$dk_{ID_k} \leftarrow (dk'_1, dk'_2, dk'_3, dk'_4)$$

return dk_{ID_k}

1.6 Enc(ek_{ID_S}, ID_{Rev}, M) $\rightarrow CT$

generate $s_1, s_2, \eta \in \mathbb{Z}_p^*$ randomly

$$T \leftarrow A^{s_1+s_2}$$

If $m = n$:

$$K \leftarrow \prod_{i=1}^n e(g^\eta \cdot ek_{1,i}, H_2(I'_i))$$

If $m > n$:

$$A_n \leftarrow \prod_{i=1}^n a_i$$

$$B_n^m \leftarrow \prod_{i=n+1}^m a_i$$

$$K \leftarrow \left(\prod_{i=1}^n e(ek_{1,i}, H_2(I'_i)) \cdot \prod_{i=n+1}^m e(H_1(I_n), H_2(I'_i))^{\alpha_i A_n} B_n^m \right) \cdot e(g^\eta, \prod_{i=1}^m H_2(I'_i))$$

If $m < n$

$K \leftarrow \prod_{i=1}^m e(ek_{1,i}, H_2(I'_i)) \prod_{i=m+1}^n e(ek_{1,i}, H_2(I'_m)) e(g^\eta, \prod_{i=1}^m H_2(I'_i))$
 $C_1 \leftarrow M \oplus \hat{H}(T) \oplus \hat{H}(K)$
 $C_2 \leftarrow \bar{g}^{s_1}$
 $C_3 \leftarrow \hat{g}^{s_2}$
 $C_4 \leftarrow (h_1^{I_1} h_2^{I_2} \cdots h_n^{I_n} \cdot g_3)^{s_1+s_2}$
 $C_5 \leftarrow g^\eta$
 $CT \leftarrow (C_1, C_2, C_3, C_4, C_5)$
return CT

1.7 Dec($dk_{ID_R}, ID_{Rev}, ID_{Snd}, CT$) $\rightarrow M$

$T' = \frac{e(C_2, dk_{1,1})e(C_3, dk_{1,2})}{e(dk_{1,3}, C_4)}$
 If $m = n$:
 $K' \leftarrow \prod_{i=1}^n e(H_1(I_i), dk_{2,i}) \cdot e(C_5, \prod_{i=1}^n H_2(I'_i))$
 If $m > n$:
 $K' \leftarrow \prod_{i=1}^n e(H_1(I_i), dk_{2,i}) \cdot \prod_{i=n+1}^m e(H_1(I_n), dk_{2,i}) \cdot e(C_5, \prod_{i=1}^m H_2(I'_i))$
 If $m < n$:
 $A_m \leftarrow \prod_{i=1}^m a_i$
 $B_n^m \leftarrow \prod_{i=m+1}^n a_i$
 $K' \leftarrow (\prod_{i=1}^m e(H_1(I_i), dk_{2,i}) \cdot \prod_{i=m+1}^n e(H_1(I_i), H_2(I'_m))^{\alpha_i A_m} B_m^n) \cdot e(C_5, \prod_{i=1}^m H_2(I'_i))$
 $M \leftarrow C_1 \oplus \hat{H}(T') \oplus \hat{H}(K')$
return M