Setup(λ):

1. PKG picks random generators $g, h_1, h_2, h_3 \in \mathbb{G}$
2. PKG picks random $\alpha \in \mathbb{Z}_p$
3. PKG calculates $g_1 = g^{\alpha}$
4. PKG chooses hash functions:
   - $H_0 : \mathbb{G} \to \{0,1\}^{\lambda}$
   - $H_1 : \{0,1\}^{*} \to \mathbb{Z}_p$
5. PKG publishes *params* $\leftarrow (g, g_1, h_1, h, h_3, H_0, H_1)$ and keeps α secret as the master key

Extract($ID \in \{0,1\}^{*}$):

1. PKG calulates $Q_{ID} \leftarrow H_1(ID)$
2. PKG generates random $r_{ID,i}$ for $i \in \{1,2,3\}$
3. PKG calulates the private key
   $d_{ID} \leftarrow \{(r_{ID,i}, h_{ID,i}) : i \in \{1,2,3\}\}$
   where $h_{ID,i} \leftarrow (h_i g^{-r_{ID,i}})^{\frac{1}{\alpha - ID}}$
4. PKG transmits d_{ID} over a secure channel to user ID

Encrypt(S, M)

1. Alice calculates $(\mathtt{vk}, \mathtt{sk}) \leftarrow \mathtt{Sig\text{-}Gen}(\lambda)$
2. Alice picks a random symmetric key K
3. Alice picks a random exponent r and calculates $T \leftarrow g^r$
4. For each $(ID, g^a) \in S$, $c_{ID} \leftarrow H_0(g^{r\alpha}) || E_{ID}$ with E_{ID}
5.