Algorithm 1 Setup

Input: Security parameter ε.

Output: System keys $pk, sk_1, sk_2, sk_{u_i}, sk_{s_i}$.

/*Key distribution*/

KC generates $(pk, sk) \leftarrow \mathsf{KeyGen}(1^{\varepsilon})$;

KC implements $(sk_1, sk_2) \leftarrow \mathsf{KeySplit}(sk)$;

for $\mathcal{U}_{i\in[1,n]} \in \mathcal{U}$ **do**

  KC implements $(sk_{u_i}, sk_{s_i}) \leftarrow \mathsf{KeySplit}(sk)$;

return KC broadcasts pk and distributes sk_{s_i}, sk_1 to $\mathcal{S}_1$, sk_2 to $\mathcal{S}_2$, and sk_{u_i} to $\mathcal{U}_{i\in[1,n]}$;

/*Model distribution*/

for $\mathcal{U}_{i\in[1,n]} \in \mathcal{U}$ **do**

  $\mathcal{U}_i$ downloads $[\![W^{(0)}]\!]$ and partial decryption $[W^{(0)}]_{sk_{s_i}} \leftarrow \mathsf{PartDec}_{sk_{s_i}}([\![W^{(0)}]\!])$ from $\mathcal{S}_1$;

  $\mathcal{U}_i$ decrypts and initializes $W^{(0)}$ using $\mathsf{FullDec}$.