KEM with Subset cover

Assume we are given a KEM scheme defined by the 3 algorithms, $\mathsf{KEM.KeyGen}$, $\mathsf{KEM.Encaps}$ and $\mathsf{KEM.Decaps}$, the broadcast encryption scheme based on subset cover techniques will be defined as follows :

- Setup : $\lambda \rightarrow (\mathsf{msk}, \mathsf{mpk})$
  takes the security parameter (number of security bits we would like to reach). It first defines the partition of subsets S_i that covers the set S with respect to the target users' rights.
  And for each S_i, it invokes ($\mathsf{KEM.KeyGen}$ which outputs $(\mathsf{pk}_i, \mathsf{sk}_i)$ and defines $\mathsf{mpk} = (\mathsf{pk}_i)_i$ and $\mathsf{msk} = (\mathsf{sk}_i)_i$ the master public key and master secret key.

- Join : $(\mathsf{msk}, U) \rightarrow \mathsf{sk}_U$
  For a user U, define sk_U as the set of secret keys sk_i for each i such that $U \in S_i$ (meaning U has rights associated to set S_i).

- Encaps : $(\mathsf{mpk}, T) \rightarrow C = (K, C_i = (K_i \oplus K, E_i)_{i \in A})$
  takes as input mpk and target set T. It first samples a random key K and express T as set of covering subsets, i.e $T = \cup_{i \in A} S_i$.
  Then for each $i \in A$, it invokes $\mathsf{KEM.Encaps}$ which $C_i = (K_i, E_i)_{i \in A}$. It finally returns $(K, C = (K_i \oplus K, E_i)_{i \in A})$.

- Decaps: $(\mathsf{sk}_U, C) \rightarrow K$
  Let $T = \cup_{i \in B} S_i$ for some integers set B and A the indices of sets associated to C.
  if user U is in T, and there exists an index $i \in A$ such that U is in $S_i \subseteq T$, it invokes $\mathsf{KEM.Decaps}(\mathsf{sk}_i, E_i)$ which gives K_i. Then using the corresponding C_i parsed as K_i', E_i, it obtains $K = K_i' \oplus K_i$.