Def. ring signature = (KeyGen, Sign, Verify)

- KeyGen$(1^\lambda, n) \rightarrow (pk_1, sk_1), \cdots, (pk_n, sk_n)$
- Sign$(m, pk_1, \cdots, pk_n, sk_i) \rightarrow \sigma$ for some $1 \leq i \leq n$.
- Verify$(m, \sigma, pk_1, \cdots, pk_n) \rightarrow \begin{cases} 1 & \text{if } \sigma \text{ is a valid signature of } m \text{ signed by } sk_i \\ 0 & \text{otherwise.} \end{cases}$

Def. group signature = (KeyGen, Sign, Verify, Open)

- KeyGen$(1^\lambda, n) \rightarrow (pk, msk, sk_1, \cdots, sk_n)$
- Sign$(m, sk_i) \rightarrow \sigma$ for some $1 \leq i \leq n$
- Verify$(\sigma, m, pk) \rightarrow \begin{cases} 1 & \text{if } \sigma \text{ is a valid signature of } m \\ 0 & \text{otherwise} \end{cases}$
- Open$(\sigma, m, msk) \rightarrow \begin{cases} \text{a player } i \\ \perp \end{cases}$