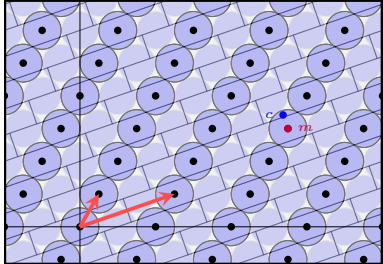


$$\text{sk} = \textcolor{blue}{B}$$



$$\text{pk} = \textcolor{red}{H}, \text{ s.t. } \mathcal{L}(\textcolor{red}{H}) \subset \mathcal{L}(\textcolor{blue}{B})$$