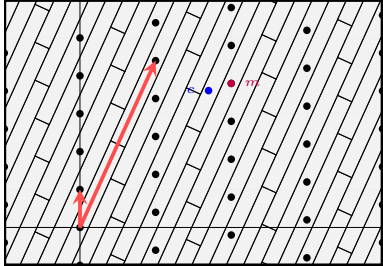


$$\text{sk} = \textcolor{green}{B}$$



$$\text{pk} = \textcolor{red}{B'}, \text{ s.t. } \mathcal{L}(\textcolor{red}{B'}) = \mathcal{L}(\textcolor{green}{B})$$