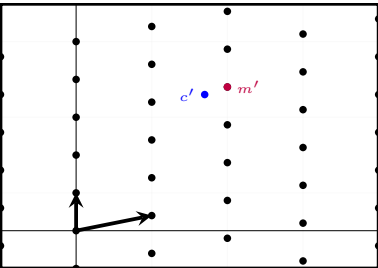
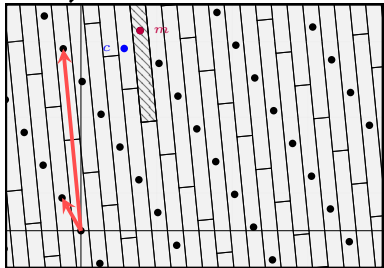


$$O \in \mathcal{O}_n$$



$$\text{sk} = O \in \mathcal{O}_n$$



$$\text{pk} = B', \text{ s.t. } \mathcal{L}(B') = O \cdot \mathcal{L}(B)$$