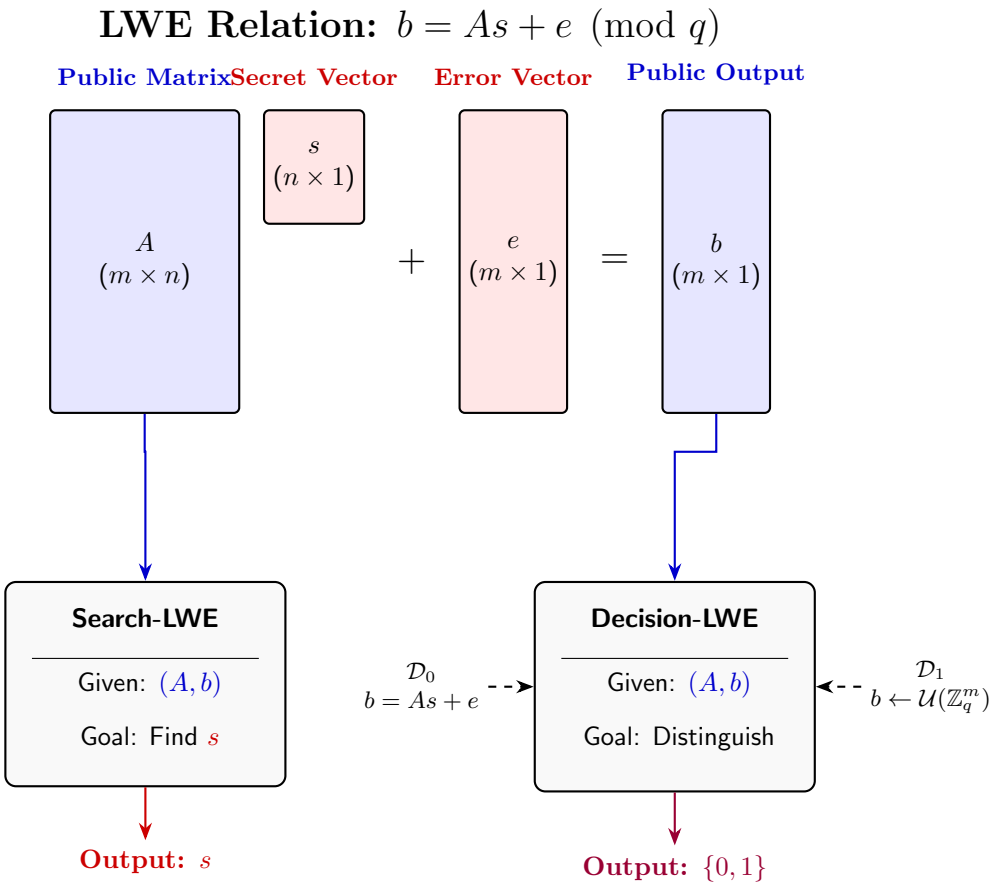
LWE Relation: $b = As + e \pmod{q}$
Public Matrix
Secret Vector
Error Vector
Public Output
A $(m \times n)$
s $(n \times 1)$
$+$
e $(m \times 1)$
$=$
b $(m \times 1)$
Search-LWE
Given: (A, b)
Goal: Find s
Output: s
$\mathcal{D}_0$ $b = As + e$
Decision-LWE
Given: (A, b)
Goal: Distinguish
$\mathcal{D}_1$ $b \leftarrow \mathcal{U}(\mathbb{Z}_q^m)$
Output: $\{0, 1\}$