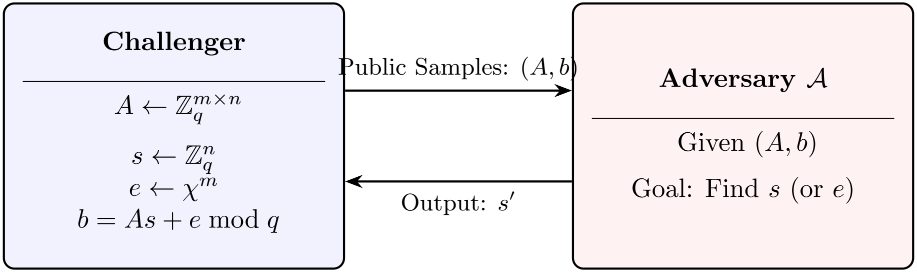
Definition: Search-LWE



Challenger

$A \leftarrow \mathbb{Z}_q^{m\times n}$

$s \leftarrow \mathbb{Z}_q^n$

$e \leftarrow \chi^m$

$b = As + e \bmod q$

Public Samples: (A, b)

Output: s'

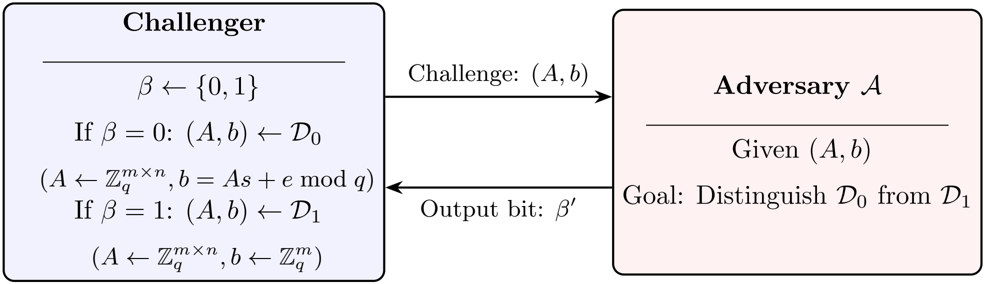
Adversary $\mathcal{A}$

Given (A, b)

Goal: Find s (or e)

Win condition: $s' = s$

Definition: Decision-LWE



Challenger

$\beta \leftarrow \{0,1\}$

If $\beta = 0$: $(A, b) \leftarrow \mathcal{D}_0$

$(A \leftarrow \mathbb{Z}_q^{m\times n}, b = As + e \bmod q)$

If $\beta = 1$: $(A, b) \leftarrow \mathcal{D}_1$

$(A \leftarrow \mathbb{Z}_q^{m\times n}, b \leftarrow \mathbb{Z}_q^m)$

Challenge: (A, b)

Output bit: β'

Adversary $\mathcal{A}$

Given (A, b)

Goal: Distinguish $\mathcal{D}_0$ from $\mathcal{D}_1$

Advantage: $|\Pr[\beta' = 1 \mid \beta = 0] - \Pr[\beta' = 1 \mid \beta = 1]|$