

Q2

Where $m \leq n$, if $A \in \mathbb{F}_q^{m \times n}$ is full rank, then the columns of A span \mathbb{F}_q^m . Since $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ is uniformly sampled, it naturally follows that $A\mathbf{s}$ is uniformly distributed across \mathbb{F}_q^m . As a result, $\mathbf{b} \leftarrow A\mathbf{s} + \mathbf{e}$ is uniformly distributed across \mathbb{F}_q^m regardless of the choice of distribution of $\mathbf{e} \leftarrow \chi_e^m$, and the LWE samples are identically distributed as uniform random noise. Thus, when $m \leq n$, A is full rank, \mathbf{s} is uniformly random, decisional-LWE is information-theoretically hard.

P.S. Given two independent random variables $A, B \in G$ whose support lies in some finite group, if A is uniformly random, then $A + B$ is also uniformly random regardless of the distribution of B :

$$\begin{aligned} P(A + B = c) &= \sum_{a \in G} P(A = a)P(B = c - a) \\ &= \sum_{a \in G} \frac{1}{|G|} P(B = c - a) \\ &= \frac{1}{|G|} \sum_{a \in G} P(B = c - a) \\ &= \frac{1}{|G|} \cdot 1 = \frac{1}{|G|} \end{aligned}$$