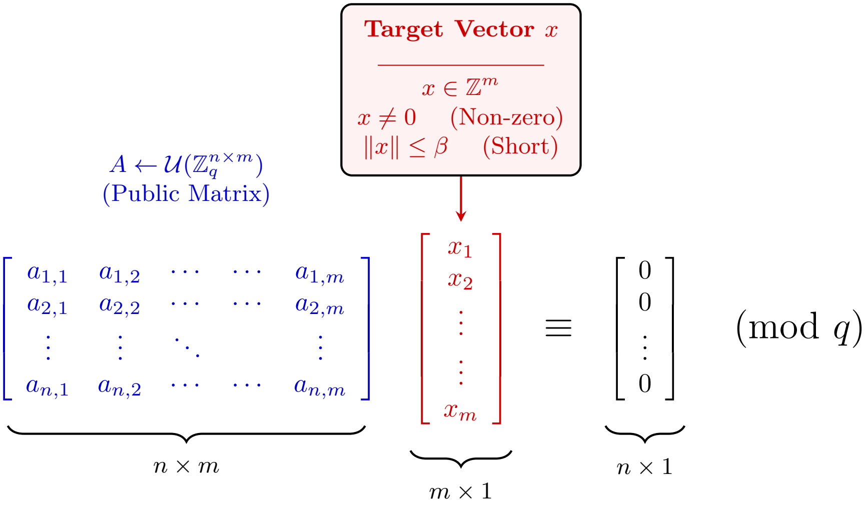

Target Vector x

$x \in \mathbb{Z}^m$

$x \neq 0$ (Non-zero)

$\|x\| \leq \beta$ (Short)

$A \leftarrow \mathcal{U}(\mathbb{Z}_q^{n \times m})$

(Public Matrix)

$$\underbrace{\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & & \vdots \\ a_{n,1} & a_{n,2} & \cdots & \cdots & a_{n,m} \end{bmatrix}}_{n \times m} \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ \vdots \\ x_m \end{bmatrix}}_{m \times 1} \equiv \underbrace{\begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}}_{n \times 1} \pmod{q}$$

System of equations view: $\sum_{j=1}^{m} a_{i,j} x_j \equiv 0 \pmod{q} \quad \forall i \in \{1, \ldots, n\}$