

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

$$s \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$$

$$e \leftarrow \chi^m$$

$$b \in \mathbb{Z}_q^m$$

$$\underbrace{\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{bmatrix}}_{m \times n} \underbrace{\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix}}_{n \times 1} + \underbrace{\begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{bmatrix}}_{m \times 1} \equiv \underbrace{\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}}_{m \times 1} \pmod{q}$$

System of equations view:

$$\sum_{j=1}^n a_{i,j} s_j + e_i \equiv b_i \pmod{q} \quad \forall i \in \{1, \dots, m\}$$