Crypto refresher

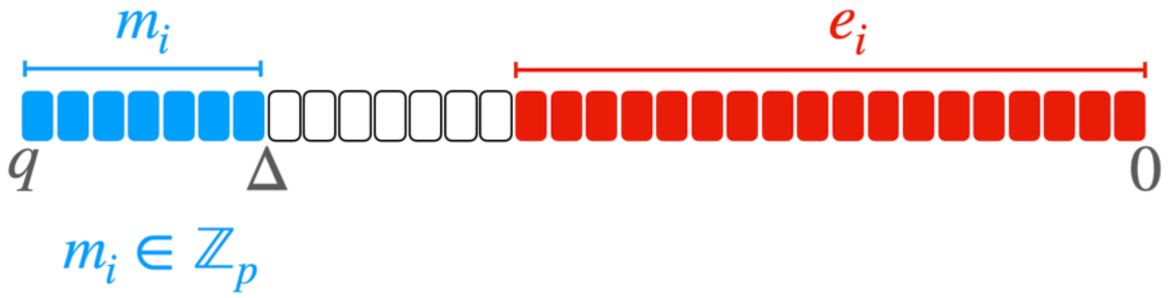
Learning with Error (LWE)

- LWE is a cornerstone of lattice based cryptography
- Allows us to build cryptosystems similar to (under an n-bit secret key $\vec{s} \in \mathbb{B}^n$)

$$LWE = \begin{cases} Enc_s(m) = (\vec{a}, \langle \vec{a}, \vec{s} \rangle + \Delta m + e) \\ Dec_s(\vec{a}, b) = \frac{b - \vec{a} \cdot \vec{s}}{\Delta} \end{cases}$$

Random mask $\vec{a} \in \mathbb{Z}_q^n$

Random noise $e < \Delta$



https://www.zama.ai/post/tfhe-deep-dive-part-1

Crypto refresher

Secrecy of noise for IND-CPA security

- $\mathcal{A}$ obtains n linearly independent encryptions $(\overrightarrow{a_i}, b_i = \langle \overrightarrow{a_i}, \vec{s} \rangle + \Delta m_i + e_i)$ from $\mathcal{O}$
- Let $\overrightarrow{a_i} = (a_{i,1}, \ldots a_{i,n})$ and $\vec{s} = (s_1, \ldots, s_n)$, we can form the following system of equations

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ & \vdots & \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \times \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} + \Delta \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} + \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

- Since $\overrightarrow{a_i}$, b_i, Δ and m_i are already public, revealing e_i allows us to re-write the system as

$$As = b - \Delta m - e$$

- This system can be solved in s using e.g. Gaussian elimination, compromising the secret key