$$CPA \subset CCA$$

FHE schemes are malleable and by definition not CCA secure

Crypto refresher

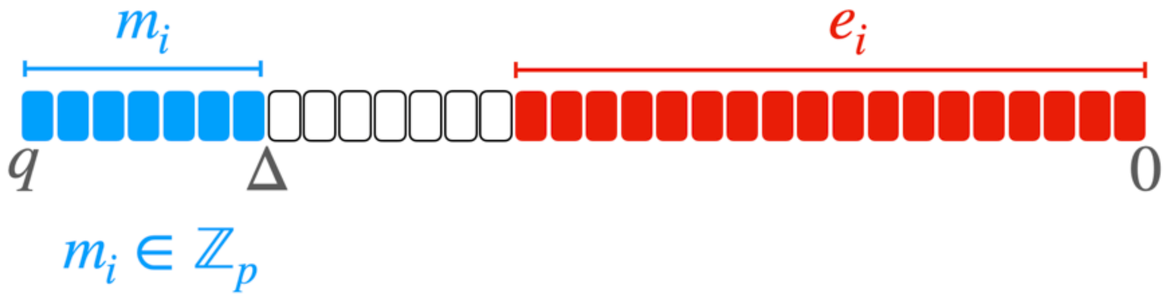
Learning with Error (LWE)

- 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