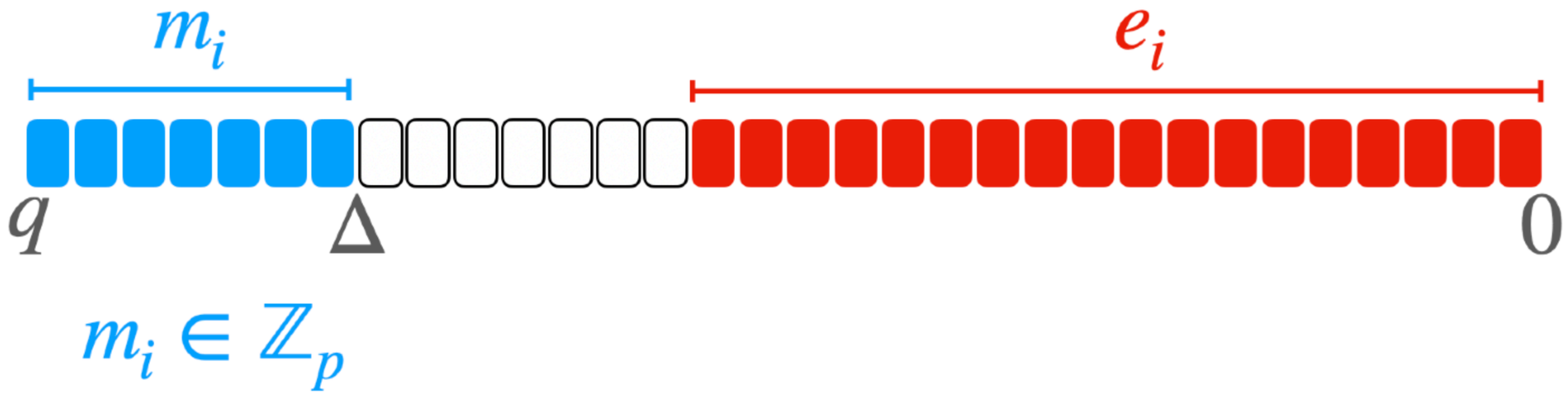
Apprentissage avec erreurs



https://www.zama.ai/post/tfhe-deep-dive-part-2

Apprentissage avec erreurs (LWE)

Usage en cryptographie

- Schémas post quantique et complètement homomorphe
- [Regev, 2005]
  - Existence d'algorithme quantique solvant SVP étant donné un oracle LWE
  - LWE au moins aussi dur que SVP
  - Cas moyen aussi dur que pire cas