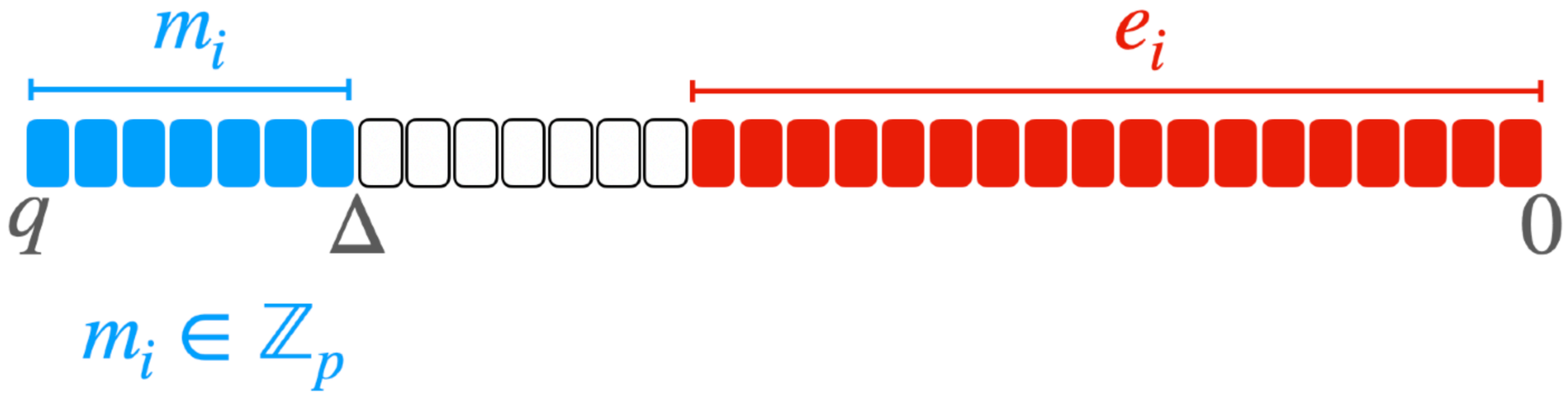
Apprentissage avec erreurs



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

Apprentissage avec erreurs (LWE)

Usage en cryptographie

- Schémas post quantique
- Chiffrement complètement homomorphe
- [Regev, 2005]
  - SVP hard $\Longrightarrow$ LWE hard
  - Cas moyen aussi dur que pire cas
- [Chen, 2024] $LWE \in QP$ 💀
  - Erreur fatale dans la preuve trouvée après une semaine 😮‍💨