Réseaux Euclidiens

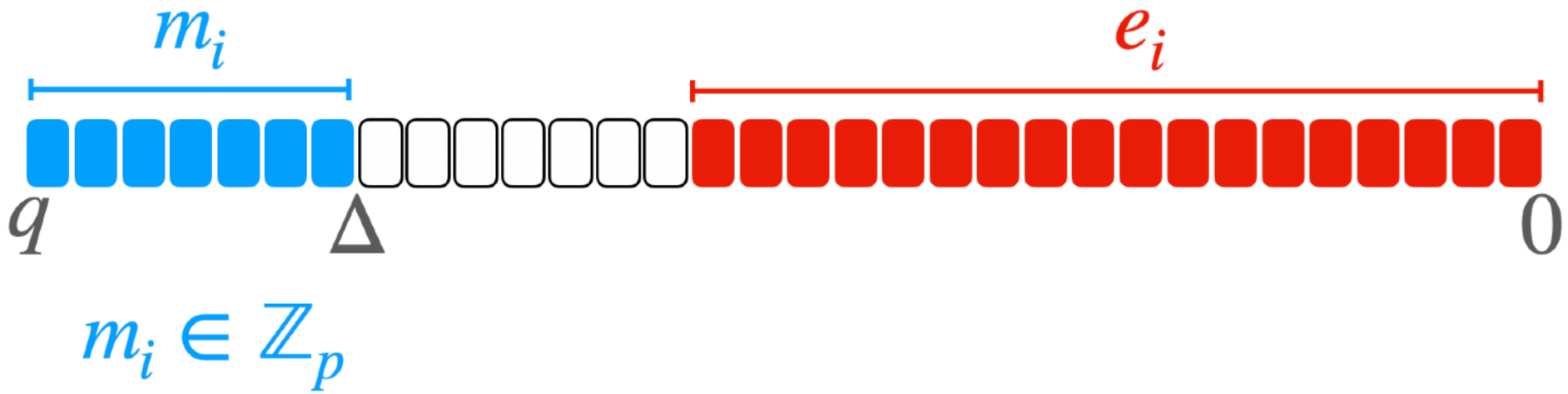
Algorithme de Lenstra–Lenstra–Lovász

- Soit $B = b_1, \ldots, b_n \in \mathbb{R}^n$ la base d'un réseau $L(B)$ et $0.25 < \delta < 1$
- [Lenstra, 1982] $B*$ une base δ-LLL réduite de $L(B)$ est telle que

$$\|b_1^*\| \leq \left(\frac{2}{\sqrt{4\delta - 1}}\right)^{n-1} \lambda$$

- Résout SVP_γ pour γ exponentiel en temps polynomial

Apprentissage avec erreurs



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