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 😮‍💨

Apprentissage avec erreurs

Définition du problème

- Soit $\mathbb{T} \cong \mathbb{R}/\mathbb{Z} \cong [0,1)$, étant donné $s \in \mathbb{Z}_q^n$, et ϕ une distribution sur $\mathbb{T}$
- On note $A_{s,\phi}$ la distribution sur $\mathbb{Z}_q^n \times \mathbb{T}$ telle que
  - On choisi $a \in \mathbb{Z}_q^n$ uniformément et $e \in \mathbb{T}$ par ϕ
  - On calcule $(a, (a \cdot s)/q + e)$
- Le problème $LWE_{q,\phi}$ demande à trouver $s \in \mathbb{Z}_q^n$ étant donné un nombre polynomial d'échantillons de $A_{s,\phi}$