# 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

# Apprentissage avec erreurs

## Définition du problème

- Soient $s \in \mathbb{Z}_q^n$, et $\phi$ une distribution Gaussienne sur $\mathbb{Z}_q$
- On note $A_{s,\phi}$ la distribution sur $\mathbb{Z}_q^n \times \mathbb{Z}_q$ telle que
  - On choisi $a \in \mathbb{Z}_q^n$ uniformément et $e \in \mathbb{Z}_q$ par $\phi$
  - On produit $(a, b)$ avec $b = a \cdot s + e$
- Le problème $LWE_{q,\phi}$ demande à trouver $s \in \mathbb{Z}_q^n$ étant donné un nombre polynomial d'échantillons de $A_{s,\phi}$