Motivation

Cryptographie post-quantique et chiffrement homomorphe

- La cryptographie moderne repose sur l'hypothèse de difficulté de certains problèmes
- Cette hypothèse ne tient pas face à des ordinateurs quantique
- Il faut donc d'autres problèmes, considérés plus difficiles
- Le Shortest Vector Problem (SVP) est un tel problème

- Les crypto-systèmes basés sur les réseaux ont aussi le bon gout d'être totalement homomorphes

Plan de l'exposé

- **Définition**
  - Réseau d'espace vectoriel euclidien
  - Problème du plus court vecteur
  - Algorithme d'énumération naïf
- **Optimisation**
  - Coupure de l'espace en deux
  - Coupure par mise à jour des bornes (B&B)
  - Traitement par lots
  - Approximation par réduction de base (**LLL**)
- **Benchmarks**
  - Réseau arbitraire
  - Instance difficile
- **Ressources**
  - Code
  - Références