Problème du plus court vecteur

Optimisation combinatoire sur les réseaux

Félix Larose-Gervais

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