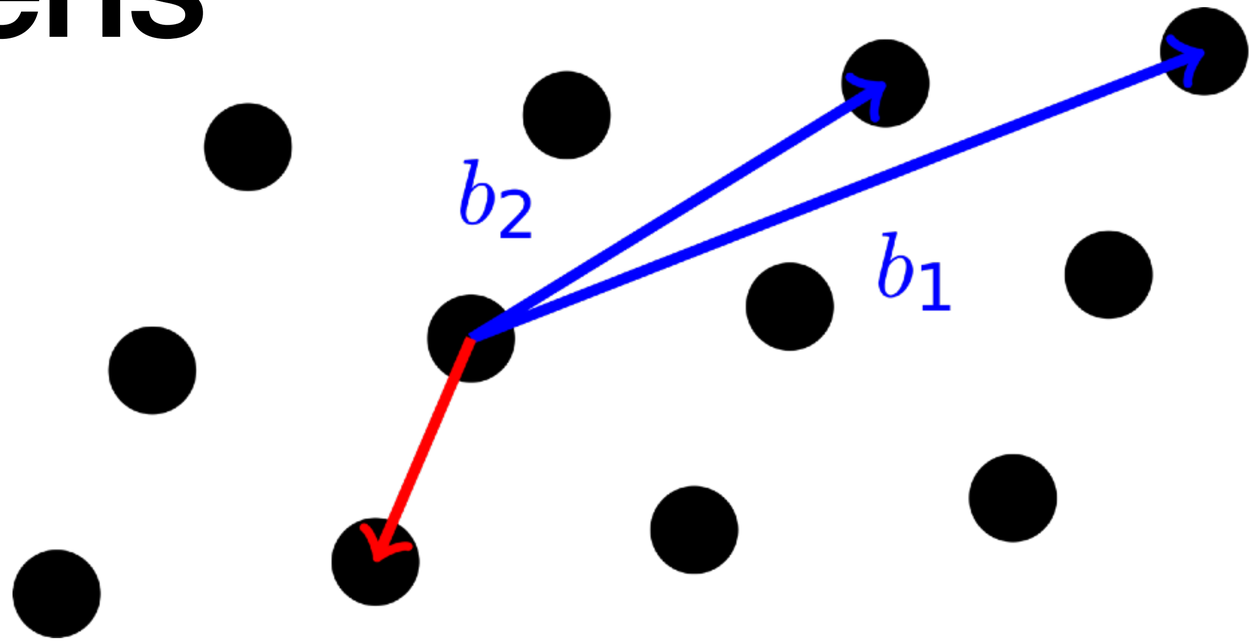
Cryptographie Moderne

Hypothèses de calcul post-quantique

- Codes linéaires 😱
  - Décodage de code aléatoire
- Courbes elliptiques supersingulières 😱
  - Recherche d’isogénies
  - Supersingular Isogeny Diffie-Hellman brisé en 2022
- Réseaux Euclidiens 😎
  - Problème du vecteur le plus court

Réseaux Euclidiens



https://en.wikipedia.org/wiki/Lattice_problem