Cryptographie Moderne

Informatique quantique

- Algorithme de Grover
  - Accélère la fouille exhaustive contre les schémas symétriques $n \rightarrow \sqrt{n}$
  - On peut doubler la taille des clés
- Algorithme de Shor
  - Efficace pour factoriser ou trouver le log discret
  - Nécessite de nouveaux schémas basés sur d’autres problèmes

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