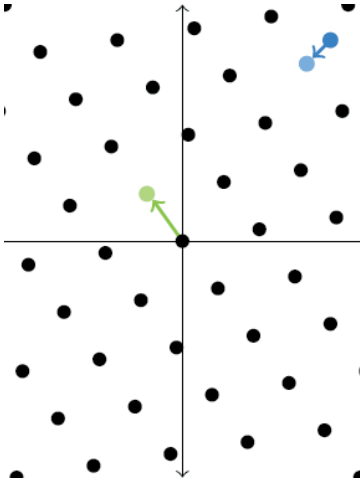
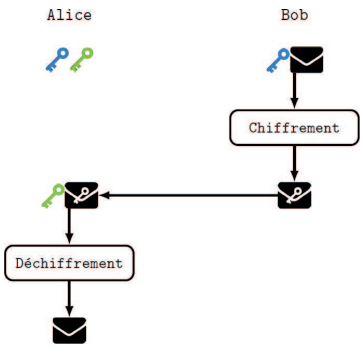
CRYPTOGRAPHIE SUR LES RÉSEAUX EUCLIDIENS

Des mathématiques au service de la protection des données !





Objectifs / Enjeux du projet

- Construire de nouvelles primitives cryptographiques post-quantiques basées sur des problèmes sur les réseaux euclidiens
- Affiner les preuves sur lesquelles reposent ces primitives
- Réduire l'écart entre les constructions théoriques et la pratique

Innovations / Atouts majeurs

- Etudier une nouvelle manière efficace de faire de la cryptographie à clé publique
- Anticiper l'apparition d'un ordinateur quantique capable de casser la cryptographie actuelle
- Développer des primitives cryptographiques avancées

Application militaire ou civile du projet

- Sécuriser les communications à l'aide de chiffrement à clé publique et d'échange de clé
- Assurer l'intégrité et l'authenticité des données à l'aide de signature numérique
- Faire des calculs sur des données chiffrées à l'aide du chiffrement complètement homomorphe

AGENCE INNOVATION DÉFENSE · UMR IRISA · cnrs · EMSEC · UNIVERSITÉ DE RENNES 1 · DGA · Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE MINISTÈRE DES ARMÉES