Apprentissage avec erreurs (Anneaux)

Établissement de clé: RLWE-KEX

- [Ding, 2012] A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem

- Comme Diffie-Hellman mais basé sur $RLWE$ plutôt que DDH

Conclusion

Résumé et ouverture

- Vraiment pas tant de lattices dans la crypto basée sur les lattices
- Les schémas sont plutôt basés sur LWE
- La sécurité dépend de la difficulté du SVP ← 🔍 lattice
- Résistance supposée même à un ordinateur quantique
- Schémas ont le bon goût d'être homomorphe
- Mais plutôt lents ← 🔍 ma recherche