Conclusion

Résumé et ouverture

- Réseaux Euclidiens pas directement utilisés dans les schémas
- Mais la sécurité dépend de la difficulté du SVP
- Il existe plusieurs autres schémas basés sur LWE (et donc SVP)
  - Chiffrement asymétrique (encryptions de zéro comme clé publique)
  - Échange de clés (schéma RLWE-KEX)
  - Signatures basées sur $RLWE$ (schéma GLYPH)
  - Chiffrement complètement homomorphe (schéma TFHE)

Merci!