

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 $SVP \leftarrow \text{🔍 lattice}$
- Résistance supposée même à un ordinateur quantique
- Schémas ont le bon goût d'être homomorphe
- Mais plutôt lents $\leftarrow \text{🔍 ma recherche}$

Merci!
Questions?