

# Conclusion

## Remarques

- La permutation aveugle de RevoLUT est plus rapide
  - Mais la comparaison avec BlindMatrixAccess dans RevoLUT est trop lente
  - Optimisation pas encore faite: MultiValue Bootstrapping
- L'algorithme Double Blind Permutation performe beaucoup mieux
  - Mais limité pour l'instant aux LUT sans doublons

# Code & Références

- <https://github.com/sofianeazogagh/revoLUT>
- <https://github.com/filedesless/BlindSort>
- [Regev, 2005] [On Lattices, Learning with Errors, Random Linear Codes, and Cryptography](#)
- [Gentry, 2009] [Fully homomorphic encryption using ideal lattices](#)
- [Çetin et al., 2015] [Depth Optimized Efficient Homomorphic Sorting](#)
- [Chillotti et al., 2020] [TFHE: Fast Fully Homomorphic Encryption Over the Torus](#)