Conclusion

Points clés, trivia, ouverture

- Le chiffrement homomorphe permet le calcul privé
- Les schémas basé sur le problème LWE ont le bon goût d'être Quantum Resistant
- Beaucoup de place à l'amélioration en terme de performance

Références

- RevoLUT: http://github.com/sofianeazogagh/revoLUT
- TFHE-rs: https://github.com/zama-ai/tfhe-rs
- TFHE blogpost: https://www.zama.ai/post/tfhe-deep-dive-part-1
- TFHE paper: https://link.springer.com/article/10.1007/s00145-019-09319-x