Blind Sort

Deuxième implémentation - Ébauche Tmp = 002305075 7 3 2 $b \leftarrow \begin{cases} 1 & \text{if Tmp}[i] = 0 \\ 0 & \text{else} \end{cases}$ $cpt \leftarrow cpt + b$ $PI[i] \leftarrow Tmp[i] - cpt$ **Blind Permutation** cpt = 0PI[0] = 0 - 1 = 7cpt = 1cpt = 2PI[1] = 0 - 2 = 6PI[2] = 2 - 2 = 0cpt = 2PI[3] = 3 - 2 = 1cpt = 2i = 4: cpt = 3 PI[4] = 0 - 3 = 5cpt = 3PI[5] = 5 - 3 = 2PI[6] = 0 - 4 = 4i = 6: cpt = 4 PI[7] = 7 - 4 = 3cpt = 4**Compute PI** PI = [76015243] Blind Permutation 7 6 0 1 5 2 4 3

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