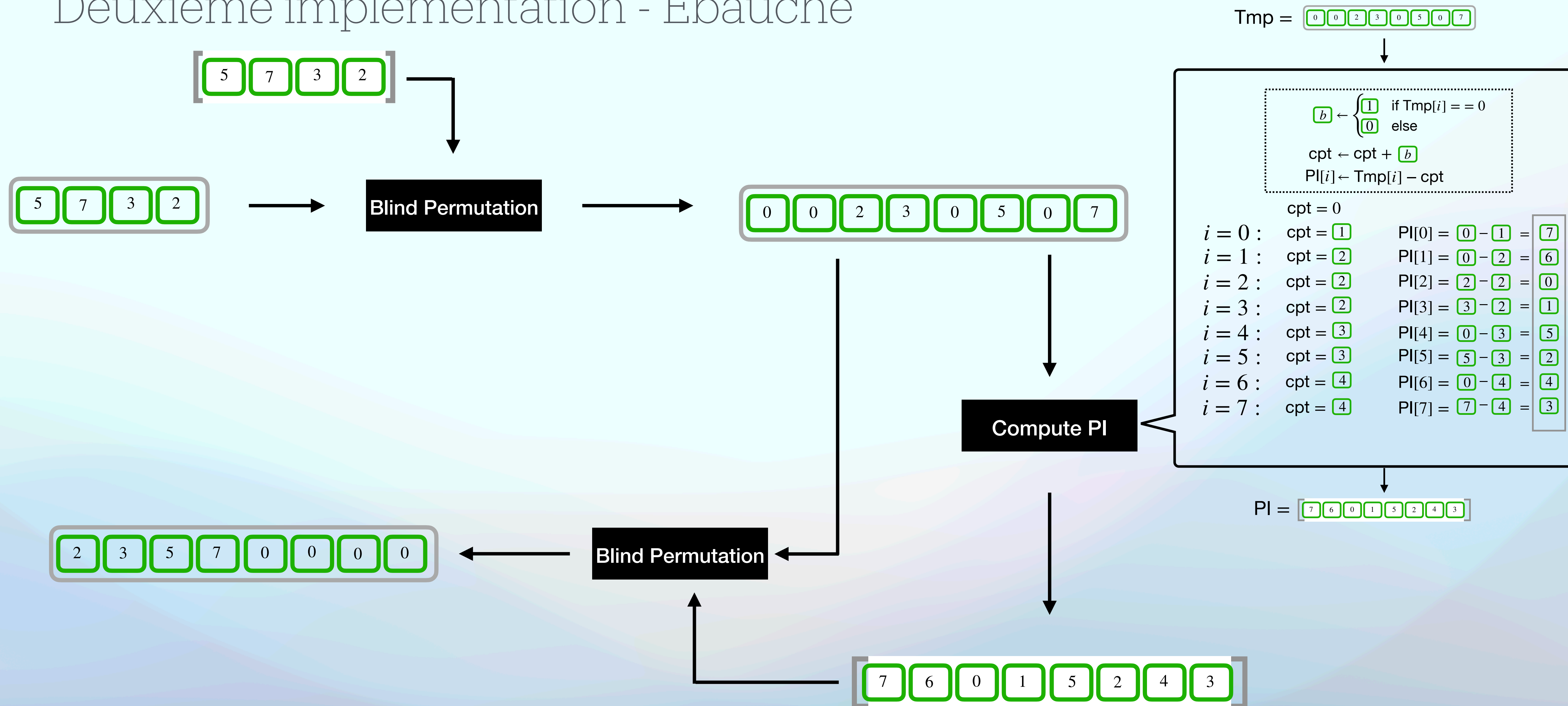


Blind Sort

Deuxième implémentation - Ébauche



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