Problème du tri aveugle

Chiffrement homomorphe

- Fonction de chiffrement préserve les opérations de calcul

$$Enc(a + b) \equiv Enc(a) + Enc(b)$$

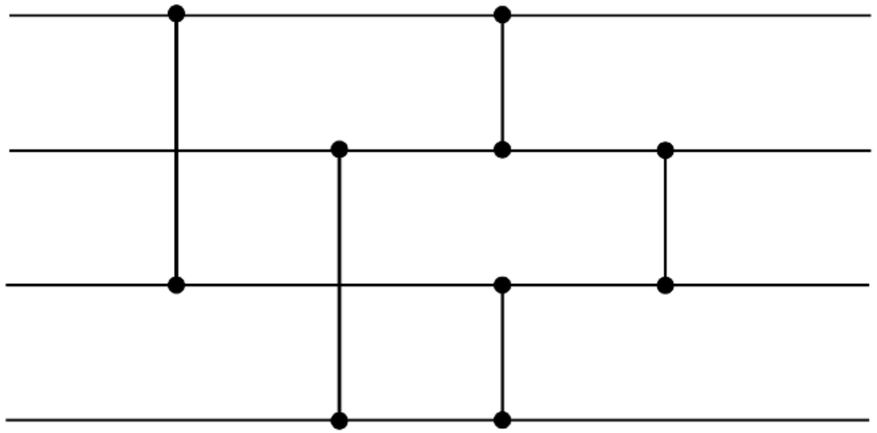
$$Enc(a \times b) \equiv Enc(a) \times Enc(b)$$

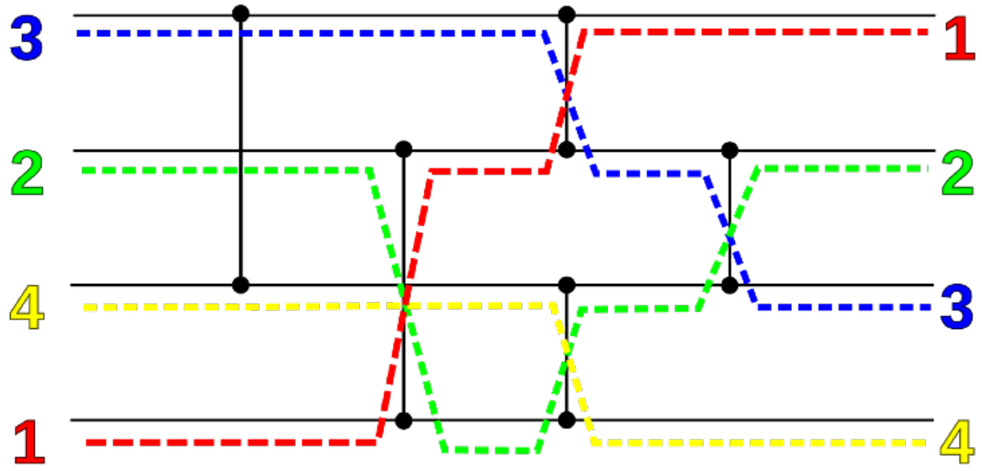
- LookUp Tables (LUT) permet d'évaluer en aveugle $f(x)$ pour un x chiffré

État de l'art

Algorithme de tri aveugle: Bitonic Sort (réseaux de tri)

- On a pas accès au branchement qui dépend des valeurs à trier
  - If p then a else b équivalent à $p \times a + (1 - p) \times b$ (pas de court-circuit)
- On construit une séquence de swap indépendante des résultats de comparaisons





https://en.wikipedia.org/wiki/Sorting_network