

Blind Sort

Première implémentation

Soit $A = [a_1, \dots, a_n]_{RLWE}$ une LUT des messages clairs $a_i \in \mathbb{Z}_p$

On calcule la matrice de comparaisons (chiffrée)

$$L_{i,j} = \begin{cases} LT(a_i, a_j) & \text{si } i < j \\ 0 & \text{si } i = j \\ 1 - LT(a_j, a_i) & \text{si } i > j \end{cases} \quad \forall i, j \in [1..n]$$

Avec $LT(x, y) = BMA(C, x, y)$ où C est telle que $C_{i,j} = [i < j]$

On calcule la permutation $\sigma \in S_n$ les somme des colonnes de L

On retourne $\sigma(A)$ grâce à Blind Permutation

Exemple

$$A = [5, 4, 6, 3]_{RLWE}$$

$$L = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\sigma = (2, 1, 3, 0)$$

$$\sigma(A) = [3, 4, 5, 6]_{RLWE}$$

Blind Sort

Deuxième implémentation - Ébauche

