Blind Sort

Première implémentation

Soit $A = [a_1, ..., a_n]_{RLWE}$ une LUT des messages clairs $a_i \in Z_p$

On calcule la matrice de comparaisons (chiffrée)

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

$$1 - LT(a_j, a_i) \quad \text{sii} > j$$

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 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