Direct Sort (RevoLUT)

Matrice de comparaison

Soit le tableau de chiffré $T = [1,3,2,2]$

On construit M telle que $M_{x,y} = \begin{cases} BlindLt(T_x, T_y) & \text{si } x < y \\ 1 - M_{y,x} & \text{sinon} \end{cases}$

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

On calcule la somme des lignes $\sigma = (0,3,2,1)$

Direct Sort (TFHE)

Permutation Aveugle

- Soient les chiffrés de $T = [1,3,2,2]$ et $\sigma = (0,3,2,1)$

$$S_0 = [1,0,0,0] \implies R_0 = T \cdot S_0 = 1$$

$$S_1 = [0,0,0,1] \implies R_1 = T \cdot S_1 = 2$$

$$S_2 = [0,0,1,0] \implies R_2 = T \cdot S_2 = 2$$

$$S_3 = [0,1,0,0] \implies R_3 = T \cdot S_3 = 3$$

$$R = [1,2,2,3]$$