Direct Sort (TFHE)

Permutation Aveugle

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

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

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

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

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

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

Direct Sort (TFHE)

Permutation Aveugle

$R = [0,\ldots,0]$

Pour i de 0 à n:

  Pour j de 0 à n:

    $R_i = R_i + Eq(\sigma_j, i) \times T_j$

Retourner R