

RevoLUT

Boite à outils

- Blind Permutation:
 - Étant donné une LUT T et un tableau d'indices chiffrés σ , retourne $\sigma(T)$
- Blind Array Add:
 - Étant donné une LUT T , un indice chiffré i et une valeur chiffrée x , ajoute x à l'indice i de T

RevoLUT

Algorithme de tri aveugle: Double Blind Permutation

- Idée principale: voir un tableau comme sa propre permutation de tri

$$T = [5, 0, 1, 0, 4, 0, 0, 3]$$

$$\sigma_1 = [5, 0, 1, 0, 4, 0, 0, 3]$$

$$\sigma_1(T) = [0, 1, 0, 3, 4, 5, 0, 0] \xrightarrow{\sigma_2} [1, 3, 4, 5, 0, 0, 0, 0]$$