

Double Blind Permutation

Exemple

- Soit le tableau de chiffres $T = [5, 7, 3, 2, 0, 0, 0, 0]$
- On parse T comme une permutation $\sigma_1 = (5, 7, 3, 2, 0, 0, 0, 0)$
- On applique T à lui-même:

$$\sigma_1(T) = [0, 0, 2, 3, 0, 5, 0, 7]$$

- On construit une deuxième permutation pour ré-arranger:

$$\sigma_2 = (7, 6, 0, 1, 5, 2, 4, 3)$$

- On retourne $\sigma_2(\sigma_1(T)) = [2, 3, 5, 7, 0, 0, 0, 0]$

Double Blind Permutation

Seconde permutation

- Étant donné un tableau de chiffré partiellement ordonné

$$T = [0,0,2,3,0,5,0,7]$$

- Pour chaque position, on compte le nombre de zéros vus

$$Z = [1,2,2,2,3,3,4,4]$$

- On construit $\sigma = T - Z \pmod{n}$

$$\sigma = (7,6,0,1,5,2,4,3)$$