## Double Blind Permutation Exemple

- Soit le tableau de chiffrés 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:  $\sigma_1(T) = [0, 0, 2, 3, 0, 5, 0, 7]$

## Double Blind Permutation

## Exemple

- Soit le tableau de chiffrés 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:

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