RevoLUT

LookUp Table avec rotation aveugle

- Une LUT est un tableau de taille fixe de n chiffrés d'entiers modulo n
- Primitives supplémentaires de RevoLUT
  - Blind Rotation
  - Blind Array Access
  - Blind Matrix Access
  - Blind Permutation

Algorithme 1 : Direct Sort