

Algorithme proposé

Blind Array Add [Azogagh, 25]

$$c_i \leftarrow c_i + x$$

Algorithme proposé

Blind Array Add [Azogagh, 25]

$$c_i \leftarrow c_i + x$$

- Ajouter un chiffré $[x]$ à un indice chiffré $[i]$ d'un tableau $[c] = [c_0], \dots, [c_{p-1}]$