

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 $[c] = [c_0], \dots, [c_{p-1}]$

5

2

1. $[x\delta_0] \leftarrow KS([x])$

2. $[x\delta_i] \leftarrow BR([-i], [x\delta_0])$

0	1	2	3
5	0	0	0
0	1	2	3
0	0	5	0

0	1	2	3
0	1	2	3



0	1	2	3
0	1	7	3

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 $[c] = [c_0], \dots, [c_{p-1}]$

5

2

1. $[x\delta_0] \leftarrow KS([x])$

2. $[x\delta_i] \leftarrow BR([-i], [x\delta_0])$

3. $\uparrow [c] + [x\delta_i]$

0	1	2	3
5	0	0	0
0	1	2	3
0	0	5	0
0	1	2	3
0	1	7	3

0	1	2	3
0	1	2	3
⇓			
0	1	2	3
0	1	7	3