

Algorithme proposé

Blind Array Assign ($n \leq p$)

$$c_i \leftarrow x$$

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

1. $[c_i] \leftarrow \textit{BlindArrayRead}([c], [i])$ \longleftarrow Eval

2. $\uparrow \textit{BlindArrayAdd}([c], [i], [x - c_i])$ $\longleftarrow c_i \leftarrow \cancel{c_i} + (x - \cancel{c_i})$

Algorithme proposé

Blind Array Assign ($n \leq p$)

$$c_i \leftarrow x$$

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

1. $[c_i] \leftarrow \text{BlindArrayRead}([c], [i])$ \leftarrow Eval

2. $\uparrow \text{BlindArrayAdd}([c], [i], [x - c_i])$ \leftarrow $c_i \leftarrow \cancel{c_i} + (x - \cancel{c_i})$
 $c_i \leftarrow x$