Algorithme proposé

Blind Array Assign $(n \leq p)$

$c_i \leftarrow x$

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

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

2. $\uparrow \mathit{BlindArrayAdd}([c], [i], [x - c_i])$ ⟵ $c_i \leftarrow \not{c}_i + (x - \not{c}_i)$

   $c_i \leftarrow x$

Algorithme proposé

Blind Array Assign $(n \leq p)$

$c_i \leftarrow x$

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

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

2. $\uparrow \mathit{BlindArrayAdd}([c], [i], [x - c_i])$ ⟵ $c_i \leftarrow \not{c}_i + (x - \not{c}_i)$

   $c_i \leftarrow x$

$$2t_{BR} + t_{KS}$$