

Algorithme proposé

Notation $LUT_{M,N}$

- LUT ou $LUT_{1,1}$ contient p éléments de \mathbb{Z}_p
- M indique le nombre de dimensions
- N indique le nombre de copies

Algorithme proposé

Notation $LUT_{M,N}$

- LUT ou $LUT_{1,1}$ contient p éléments de \mathbb{Z}_p
- M indique le nombre de dimensions
- N indique le nombre de copies
- $LUT_{M,N}$ contient p^M éléments de \mathbb{Z}_p^N