

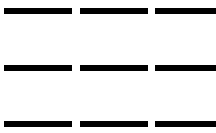








Algorithme proposé

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

M N	1	2	3
1			
2			
3			

Algorithme proposé

Applications

- Blind Counting Sort
 - Trier une $LUT_{M,N}$ avec comme tableau auxiliaire une $LUT_{N,M}$
- Private Shortest Path
 - Encoder les *next_hop* dans une $LUT_{M,N}$