Benchmarks

Avec Criterion

	Array Size			
	4	**8**	**16**	**32**
Direct Sort (Cetin)	~0.5s	~5s	~50s	>7m
Direct Sort (RevoLUT)	~2s	~20s	>2m	-
Direct Sort (TFHE-rs)	~2s	~10s	~40s	>2m
Double Blind Permutation	~1s	~2s	~5s	~21s
Direct Blind Permutation	~1s	~4s	~16s	~62s
RevoLUT Blind Permutation	~400ms	~800ms	~3.6s	~10s

Conclusion

Remarques

- La permutation aveugle de RevoLUT est plus rapide
  - Mais la comparaison avec BlindMatrixAccess dans RevoLUT est trop lente
  - Optimisation pas encore faite: MultiValue Bootstrapping
- L’algorithme Double Blind Permutation performe beaucoup mieux
  - Mais limité pour l’instant aux LUT sans doublons