Benchmarks

Avec Criterion

	Array Size			
	4	**8**	**16**	**32**
Direct Sort (Cetin)	500ms	5s	50s	7m
Direct Sort (Iliashenko)	80ms	700ms	6s	50s
Direct Sort (RevoLUT)	2s	20s	2m	-
Direct Sort (TFHE-rs)	2s	10s	40s	2m
Naive Blind Permutation	1s	4s	16s	1m
RevoLUT Blind Permutation	400ms	800ms	3.6s	10s
2BP (THFE-rs)	3s	9s	33s	2m
2BP (RevoLUT)	1s	2s	5s	21s

Conclusion

Remarques

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