Résultats expérimentaux

Implémentation dans la librairie RevoLUT [1]

Table 3.4 Temps d'exécution (en secondes) de l'assignation aveugle

(p, M, N)	n	(Trama *et al.*, 2025)	Blind Tensor Assign
$(16, 1, 2)$	16	10.832	0.08
$(16, 2, 2)$	256	173.312	1.24
$(16, 3, 2)$	4096	2,772.992	20.28

Temps estimé par Trama selon la formule $n \times (0.088 + 2 \times 0.159 + 0.271)$
pour assigner n entiers 8 bits encodés comme deux chiffrés de 4 bits

[1]: https://github.com/sofianeazogagh/revoLUT/

Références

- **[Trama, 25]** Trama, D., Boudguiga, A., Clet, P.-E., Sirdey, R., & Ye, N. (2025). **Designing a General-Purpose 8-bit (T)FHE Processor Abstraction**. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(2), 535-578. https://doi.org/10.46586/tches.v2025.i2.535-578
- **[Azogagh, 25]** Azogagh, S., Killijian, M.-O., Larose-Gervais, F. (2025). **A non-comparison oblivious sort and its application to private k-NN**. PoPETs Proceedings on Privacy Enhancing Technologies Symposium, 2025(3), 156-169. https://doi.org/10.56553/popets-2025-0093
- **[Guimarães, 21]** Guimarães, A., Borin, E., & Aranha, D. F. . (2021). **Revisiting the functional bootstrap in TFHE**. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021(2), 229-253. https://doi.org/10.46586/tches.v2021.i2.229-253