Références

- [ZamaLWE] https://www.zama.ai/post/tfhe-deep-dive-part-1

- [ZamaPBS] https://docs.zama.ai/tfhe-rs/get-started/benchmarks/cpu/cpu-programmable-bootstrapping

- [SV65] Sharma, A., & Varma, A. K. (1965). **Trigonometric interpolation**

- [PS73] Paterson, M. S., & Stockmeyer, L. J. (1973). **On the number of nonscalar multiplications necessary to evaluate polynomials**. *SIAM Journal on Computing, 2*(1), 60-66.

- [GBA21] Guimarães, A., Borin, E., & Aranha, D. F. (2021). **Revisiting the functional bootstrap in TFHE**. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 229-253.

- [DMPS24] Drucker, N., Moshkowich, G., Pelleg, T., & Shaul, H. (2022). **BLEACH: cleaning errors in discrete computations over CKKS**. *Cryptology ePrint Archive*.

- [AKP25] Alexandru, A., Kim, A., & Polyakov, Y. (2025, August). **General functional bootstrapping using CKKS**. In *Annual International Cryptology Conference* (pp. 304-337). Cham: Springer Nature Switzerland.