Functional Bootstrapping

Aka Programmable Bootstrapping (PBS) [AKP25]

- Évaluer des LUT jusqu'à 8-bits en SIMD sur 64k éléments en ~50s (~0.7ms amorti)
- Évaluer Sign LUT multi-précision jusqu'à 32-bits (4 digits 8-bit) en ~191s (~3ms amorti)
- Pas de bench pour des LUT multi-précision quelconques…
    - Apparement juste à suivre le blueprint de [GBA21]

Références

- [SV65] Ambikeshwar Sharma and Arun K. Varma. **Trigonometric interpolation**. Duke Mathematical J., 32(2):341 – 357, 1965. doi:10.1215/S0012-7094-65-03235-7.
- [RAD79] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). **On data banks and privacy homomorphisms**. *Foundations of secure computation*, *4*(11), 169-180.
- [Gentry09] Gentry, C. (2009, May). **Fully homomorphic encryption using ideal lattices**. In *Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178).
- [DGHV10] Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. (2010, May). **Fully homomorphic encryption over the integers**. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 24-43). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [BGV11] Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). **(Leveled) fully homomorphic encryption without bootstrapping**. *ACM Transactions on Computation Theory (TOCT)*, *6*(3), 1-36.
- [BFV12] Fan, J., & Vercauteren, F. (2012). **Somewhat practical fully homomorphic encryption**. *Cryptology ePrint Archive*.
- [GSW13] Gentry, C., Sahai, A., & Waters, B. (2013, August). **Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based**. In *Annual cryptology conference* (pp. 75-92). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [DM14] Ducas, L., & Micciancio, D. (2015, April). **FHEW: bootstrapping homomorphic encryption in less than a second**. In *Annual international conference on the theory and applications of cryptographic techniques* (pp. 617-640). Berlin, Heidelberg: Springer Berlin Heidelberg.
- [CGGI16]
- [CKKS17]
- [CKKS18]
- [GBA21]
- [BCKS24]
- [DMPS24]
- [AKP24]