Sujet de stage Master 2

Compression des chiffrés pour le chiffrement complètement homomorphe

Malika Izabachene, Laura Luzzi

Octobre 2026

Date de démarrage du stage : flexible

Lieu : Laboratoire ETIS, UMR 8051 CY Cergy Paris Université, ENSEA, CNRS

Contacts : malika.izabachene@cyu.fr ; laura.luzzi@ensea.fr

Le chiffrement complètement homomorphe (Fully Homomorphic Encryption, FHE) [Gen09] permet d'effectuer des calculs sur des données chiffrées sans les déchiffrer. Dans les constructions FHE fondées sur les réseaux euclidiens, le chiffrement introduit un bruit qui joue un rôle essentiel dans les garanties de sécurité. Les opérations homomorphes font évoluer ce bruit, dont la croissance peut, au-delà d'un certain seuil, compromettre la correction du déchiffrement.

L'utilisation du FHE soulève ainsi plusieurs défis, notamment en matière de coût des opérations et de coût de stockage. En effet, la taille des chiffrés, souvent très supérieure à celle des données en clair, entraîne des coûts importants de stockage et de communication.

Le choix des paramètres constitue en lui-même une difficulté, puisqu'il doit concilier la maîtrise de la croissance du bruit induite par les opérations homomorphes, le niveau de sécurité visé et la complexité des calculs à effectuer.

La *quantification* [CS82] constitue une approche pouvant contribuer à réduire la taille de représentation des chiffrés. Elle consiste à remplacer certaines de leurs composantes par des représentants dans un ensemble plus restreint, permettant ainsi une représentation plus compacte au prix d'une erreur supplémentaire. Cette erreur doit alors être analysée conjointement avec le bruit initial du chiffrement et, lorsque des calculs sont effectués après compression, avec son évolution au cours des opérations homomorphes. Le gain de stockage ou de communication doit donc être mis en regard de l'effet sur la correction du déchiffrement et le coût des calculs homomorphes.

Dans [MS23], Micciancio et Shultz montrent qu'il est possible de combiner un encodage compatible avec le chiffrement fondé sur les réseaux *gadgets* [MP12] et un algorithme de compression permettant d'atteindre un taux de compression proche de 1, ce taux étant défini comme le rapport entre la taille du message et celle du chiffré. Ce résultat établit ainsi des garanties de correction et de compacité pour le chiffrement considéré.

L'objectif de ce stage est d'étudier la compatibilité des méthodes de compression avec les opérations homomorphes, ainsi que les compromis entre le gain de compression, la croissance du bruit et le coût des opérations, afin d'identifier les conditions dans lesquelles la *quantification* peut être intégrée aux constructions homomorphes.

L'étude de cette compatibilité portera notamment sur le cas où le réseau de quantification est construit à partir du réseau *gadget*. Il s'agira d'examiner les contraintes qu'une telle construction impose au décodage et à la réalisation des opérations homomorphes, puis d'analyser dans quelle mesure les propriétés géométriques et algébriques de ce réseau influencent l'erreur de *quantification*, sa propagation au cours des calculs homomorphes et les conditions de correction du déchiffrement.

Ce travail permettra d'évaluer le potentiel de ces approches de compression et d'identifier les conditions dans lesquelles elles peuvent être exploitées efficacement dans le cadre du chiffrement homomorphe.

Références

[CS82] J. H. Conway and N. J. A. Sloane. Voronoi regions of lattices, second moments of polytopes, and quantization. *IEEE Transactions on Information Theory*, 28(2) :211–226, 1982.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009.

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices : Simpler, tighter, faster, smaller. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer, 2012.

[MS23] Daniele Micciancio and Mark Schultz. Error correction and ciphertext quantization in lattice cryptography. In *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*, volume 14085 of *Lecture Notes in Computer Science*, pages 648–681. Springer, 2023.