Conception et implémentation de cryptographie à base de réseaux

Tancrède Lepoint [1]

Prix de thèse Gilles Kahn 2014

Tancrède Lepoint a soutenu sa thèse [2] en juin 2014. Celle-ci a été préparée au LIENS (École Normale Supérieure, France) et à la Faculty of Sciences, Technology and Communication (Université du Luxembourg), sous la direction de David Pointcheval et Jean-Sébastien Coron, et a été financée dans le cadre d'un contrat CIFRE par la société CryptoExperts.

La cryptographie à base de réseaux Euclidiens est aujourd'hui un domaine scientifique en pleine expansion. Son attractivité est plurielle : les opérations sont élémentaires, sa complexité asymptotique quasi-optimale, elle résiste aux ordinateurs quantiques (contrairement aux algorithmes actuels qui seront obsolètes dès l'existence de calculateurs quantiques suffisamment performants), mais surtout rend possible de nouvelles applications qui pourraient permettre à terme d'obtenir un *Cloud* complètement sécurisé et respectueux de la vie privée. Exemple frappant : vous pourriez effectuer une requête sur un moteur de recherche *sans que celui-ci ait connaissance* de ce que vous avez recherché (voir Figure 1).

1. https://www.cryptoexperts.com/tlepoint
2. Consultable à l'adresse https://tel.archives-ouvertes.fr/tel-01069864

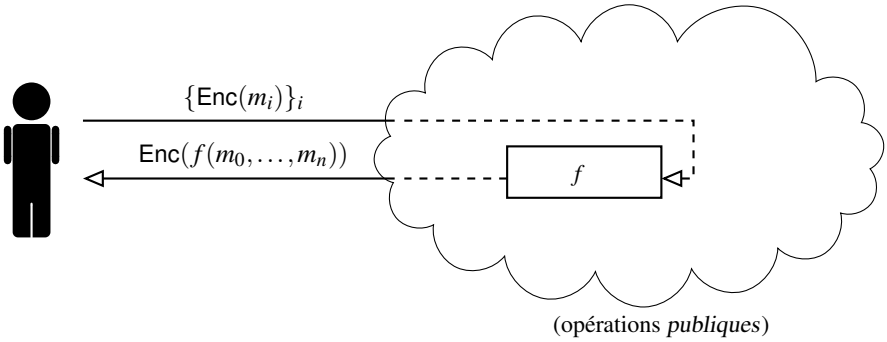

FIGURE 1. Avec un schéma de chiffrement complètement homomorphe Enc, une personne peut envoyer ses données $\{m_i\}_i$ au Cloud sous forme chiffrée. Celui-ci peut alors les manipuler publiquement (sans les connaître) et renvoyer l'évaluation de *n'importe quel algorithme* f sur ces dernières.

Considéré comme le Saint Graal de la cryptographie [14], l'existence d'un tel chiffrement n'a été prouvée possible qu'en 2009 [12] et utilise les réseaux Euclidiens. Il s'agit du *chiffrement complètement homomorphe*. Plus généralement, la richesse mathématique des réseaux Euclidiens apparaît être un composant clé pour permettre la manipulation publique de données secrètes, mais les constructions cryptographiques à visée pratique pour un niveau de sécurité fixé se révèlent être particulièrement inefficaces. L'objectif de la thèse est donc de réduire l'écart entre la théorie et la pratique de la cryptographie à base de réseaux.

Dans [10], nous proposons un nouveau schéma de signature compact (avec des signatures de l'ordre de 5000 bits), performant, sûr et adapté aux environnements contraints. Signer numériquement des données permet d'en garantir l'intégrité et l'authenticité, et est nécessaire à toute communication numérique sécurisée. Des améliorations théoriques et optimisations pratiques ont permis d'obtenir une signature numérique basée sur les réseaux aussi efficace (voire plus efficace) que celles actuellement utilisées. Moins de 18 mois après publication, notre signature digitale a été intégrée à *strongSwan* (une solution VPN open source) [15] et permet de s'authentifier de manière sécurisée et pérenne, indépendamment des avancées en physique quantique.

Nos contributions principales au chiffrement homomorphe consistent à en améliorer l'efficacité au travers du parallélisme (SIMD), d'optimisations algorithmiques

théoriques et pratiques [4, 8] et à la réduction de problèmes d'optimisation au problème SAT [13]. Il s'agit de notre sujet de recherche principal : nous sommes impliqués dans plusieurs projets européens visant à déployer la cryptographie homomorphe dans les produits d'ici l'horizon 2020 [1], et travaillons tant sur des aspects théoriques (complexité APX [3]) que pratiques (bibliothèque efficace en C++ [2]).

Finalement, nous construisons et implémentons des applications multilinéaires cryptographiques dans [7]. Cette primitive très récente (la première construction datant également de 2013) a de nombreuses conséquences inattendues et à très fort potentiel, comme par exemple l'existence de réelle *obfuscation*[3] logicielle [11]. Cette nouvelle primitive vit en ce moment même un véritable naufrage à cause de nombreuses attaques (auxquelles nous avons aussi participé) [5, 6]. Récemment, nous avons amélioré notre schéma dans [9] : ce dernier se révèle être l'*unique* construction rendant possible de nombreuses constructions cryptographiques théoriques.

Références

[1] Homomorphic encryption applications and technology, 2015. https://heat-project.eu/.

[2] Carlos Aguilar-Melchor, Joris Barrier, Serge Guelton, Adrien Guinet, Marc-Olivier Killijian, and Tancrède Lepoint. NFLlib : NTT-based fast lattice library, 2015.

[3] Fabrice Benhamouda, Tancrède Lepoint, and Hang Zhou. Optimization of bootstrapping in circuits. 2015.

[4] Jung Hee Cheon, Jean-Sébastien Coron, Jinsu Kim, Moon Sung Lee, Tancrède Lepoint, Mehdi Tibouchi, and Aaram Yun. Batch fully homomorphic encryption over the integers. In Thomas Johansson and Phong Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 315–335. Springer, 2013.

[5] Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé. Cryptanalysis of the multilinear map over the integers. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 3–12. Springer, 2015.

[6] Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrède Lepoint, Hemanta K. Maji, Eric Miles, Mariana Raykova, Amit Sahai, and Mehdi Tibouchi. Zeroizing without low-level zeroes : New attacks on multilinear maps and their limitations. 2015. To appear at CRYPTO 2015.

[7] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Practical multilinear maps over the integers. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 476–493. Springer, 2013.

[8] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. Scale-invariant fully homomorphic encryption over the integers. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 311–328. Springer, 2014.

[9] Jean-Sébastien Coron, Tancrède Lepoint, and Mehdi Tibouchi. New multilinear maps over the integers. 2015. To appear at CRYPTO 2015.

[10] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal Gaussians. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 40–56. Springer, 2013.

3. Technique d'obscurcissement de code, rendant celui-ci particulièrement difficile à comprendre.

[11] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *FOCS 2013*, pages 40–49. IEEE Computer Society, 2013.

[12] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *STOC 2009*, pages 169–178. ACM, 2009.

[13] Tancrède Lepoint and Pascal Paillier. On the minimal number of bootstrappings in homomorphic circuits. In Andrew A. Adams, Michael Brenner, and Matthew Smith, editors, *FC 2013 Workshops, USEC and WAHC 2013*, volume 7862 of *LNCS*, pages 189–200. Springer, 2013.

[14] Daniele Micciancio. A first glimpse of cryptography's Holy Grail. *Commun. ACM*, 53(3) :96, 2010.

[15] Andreas Steffen et al. *strongSwan (Version 5.2.2)*, 2015. `https://www.strongswan.org/`.