Autour de la difficulté du problème « Learning with Errors »

Adeline LANGLOIS (LIP, ENS Lyon),

Travaux en commun avec Damien Stehlé (CNRS, LIP, ENS Lyon).

Née en 1996 avec les travaux d'Ajtai [Ajt96], la cryptographie reposant sur les réseaux euclidiens connaît aujourd'hui un essor rapide. Elle a de nombreux attraits tels que sa simplicité, son efficacité potentielle, sa résistance apparente aux attaques quantiques et surtout ses preuves de sécurité sous des hypothèses de difficulté algorithmique de problèmes bien compris.

L'un de ces problèmes, introduit par Regev en 2005 [Reg09], est le problème moyen-cas *Learning With Errors* (LWE). La version décisionnelle de ce problème est la suivante :

Definition. Soient n et q des entiers positifs, et χ une distribution de probabilité. Étant donné une suite de paires $(\vec{a}, b)$ qui sont soit que des échantillons de la forme $(\vec{a}, \frac{1}{q}\langle\vec{a}, \vec{s}\rangle + e)$ où chaque vecteur $\vec{a} \in \mathbb{Z}_q^n$ est uniforme et $e \in \mathbb{Z}_q$ est choisi selon χ, soit que des échantillons uniformes dans $\mathbb{Z}_q^{n+1}$, l'objectif est de distinguer entre les deux cas.

Les problèmes LWE et RLWE (sa variante structurée) sont connus pour être au moins aussi difficiles à résoudre que des problèmes pires-cas portant sur les réseaux [Reg09, LPR10]. De nombreuses primitives cryptographiques sont construites à partir de ces deux problèmes.

Les preuves de difficulté sont des réductions pire-cas moyens-cas qui dépendent de plusieurs paramètres : le plus important d'entre eux est l'entier q qui définit l'anneau dans lequel nous travaillons ($\mathbb{Z}/q\mathbb{Z}$ dans le cas de LWE et $(\mathbb{Z}/q\mathbb{Z}[x])/\langle x^n+1\rangle$ dans le cas de RLWE). Les réductions existantes [Reg09, LPR10, MP12] prouvent la difficulté du problème LWE (respectivement RLWE) sous des restrictions sur q bien précises : l'entier q doit être premier pour LWE, et il doit être premier tel que $q = 1 \bmod 2n$ pour RLWE. Ces conditions (en particulier pour RLWE) sont très restrictives et empêchent des adaptations à RLWE (donc plus efficaces) de constructions cryptographiques basées sur LWE.

Cet exposé portera tout d'abord sur le problème LWE et son lien avec la cryptographie reposant sur les réseaux euclidiens. Puis nous présenterons notre résultat [LS12] : la difficulté du problème (R)LWE sans contrainte sur la forme arithmétique du modulo q. Notre méthode pour obtenir ce résultat est de combiner les résultats existants (la difficulté de (R)LWE pour un certain q) avec une réduction d'un problème (R)LWE pour un modulo q à un problème (R)LWE de même dimension pour un autre modulo p de forme arithmétique quelconque, sous certaines conditions (faibles) concernant la distribution d'entrée du problème LWE.

Bibliographie.

[Ajt96] M. Ajtai. Generating Hard Instances of Lattice Problems (Extended Abstract). Proc. of STOC, pages 99–108, 1996.

[LPR10] V. Lyubashevsky, C. Peikert and O. Regev. On ideal lattices and learning with errors over rings. Proc. of EUROCRYPT, pages 1-23, 2010.

[LS12] A. Langlois and D. Stehlé. Hardness of decision (R)LWE for any modulus. Cryptology ePrint Archive, report 2012/091, *http://eprint.iacr.org/2012/091*.

[MP12] D. Micciancio and C. Peikert. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. Proc. of EUROCRYPT, Springer LNCS 7237, pages 700-718, 2012.

[Reg09] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. J. ACM 56(6), 2009.