Difficulté Entropique de Module-LWE à partir de Module-NTRU

Corentin Jeudy[1,2]
corentin.jeudy@irisa.fr

[1] Univ Rennes, CNRS, IRISA, Rennes, France
[2] Orange Labs, Applied Crypto Group, Cesson-Sévigné, France

Collaboration avec Katharina Boudgoust, Adeline Roux-Langlois et Weiqiang Wen

Le problème *Module Learning With Errors* (M-LWE) [LS15] est au coeur de la cryptographie sur les réseaux Euclidiens. Sa flexibilité entre efficacité et sécurité en fait un candidat de choix pour la construction de primitives cryptographiques efficaces. En particulier, les finalistes à la compétition de standardisation de primitives post-quantiques du NIST Kyber et Dilithium s'appuient directement sur la difficulté de M-LWE. Bien que cette difficulté ait été établie pour certains jeux de paramètres, certaines questions restent ouvertes. Nous répondons ici à l'une d'entre elles en prouvant que la version calculatoire de M-LWE reste difficile pour une distribution arbitraire sur le secret, à condition que celle-ci contienne suffisamment d'entropie. Ceci motive l'appellation de *difficulté entropique* de M-LWE, que nous basons sur la difficulté de la version décisionnelle du problème Module-NTRU (M-NTRU) [CPS+20]. Pour prouver cette difficulté entropique, nous transformons d'abord le contexte algébrique en un contexte non-algébrique, ce qui mène à des problèmes équivalents que nous appelons *Structured* LWE (S-LWE) et *Structured* NTRU (S-NTRU). Cette transformation consiste simplement à plonger les éléments algebriques dans des espaces de vecteurs et matrices à coefficients entiers ou réels. Ensuite, nous suivons la technique de preuve de Braskerski et Döttling pour R-LWE [BD20] afin de prouver que l'existence de certaines distributions, caractérisées comme *sometimes lossy pseudorandom*, implique la difficulté entropique de S-LWE. Par la suite, nous montrons que la distribution des instances S-NTRU, i.e., $\mathbf{G}\mathbf{F}^{-1} \bmod q$ pour deux matrices Gaussiennes $\mathbf{F}$ et $\mathbf{G}$, est effectivement *sometimes lossy pseudorandom* à condition que la version décisionnelle de S-NTRU soit difficile et que l'entropie de la distribution du secret soit suffisamment grande. En utilisant l'équivalence entre S-LWE et M-LWE, on obtient alors la difficulté entropique de la version calculatoire de M-LWE.

References

BD20. Z. Brakerski and N. Döttling. Lossiness and entropic hardness for ring-lwe. In *TCC (1)*, volume 12550 of *Lecture Notes in Computer Science*, pages 1–27. Springer, 2020.

CPS+20. C. Chuengsatiansup, T. Prest, D. Stehlé, A. Wallet, and K. Xagawa. Modfalcon: Compact signatures based on module-ntru lattices. In *AsiaCCS*, pages 853–866. ACM, 2020.

LS15. A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 75(3):565–599, 2015.