From Module-uSVP to NTRU

Joël Felderhoff, Alice Pellet–Mary, Damien Stehlé

The NTRU problem asks to find f and g two polynomials with small coefficients given $h = g/f \bmod q$, where all the polynomials are taken modulo some irreducible polynomial P defining a number field. This problem is a particular instance of a Shortest Vector Problem in a Module lattice of rank 2 in which there exists a particularly dense submodule of rank 1.

Although NTRU has first been proposed as a security assumption by Hoffstein, Pipher and Silverman in 1998 [HPS98], its relationship to other classical module lattice problems is not yet well understood. It was proven in [PS21] that ideal-SVP reduces to average-case-NTRU, and that average-case-NTRUmod (consisting in recovering the dense rank-1 submodule of the NTRU module) reduces to decision-NTRU. In this follow-up, we consider Module-uSVP, the Module version of the unique-Shortest Vector Problem. This problem asks to find a short vector in a module lattice, provided that it contains a dense submodule of rank 1. We then propose a reduction from module-uSVP to NTRU.

The talk will be presented by Joël Felderhoff (PhD student) and the results are a joint work with Alice Pellet–Mary and Damien Stehlé.

References

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory*, Lecture Notes in Computer Science, pages 267–288. Springer, 1998.

[PS21] Alice Pellet-Mary and Damien Stehlé. On the hardness of the NTRU problem. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 3–35, Cham, 2021. Springer International Publishing.