

On algebraic variants of the LWE problem.

Damien Stehlé, ENS de Lyon

The Learning With Errors problem (LWE) captures the asymptotic hardness of some standard lattice problems, and enables the design of cryptographic schemes. However, these LWE-based schemes are relatively inefficient. To address this issue, algebraic variants of LWE have been introduced, such as Polynomial-LWE, Ring-LWE and Middle-Product-LWE, whose definitions involve polynomial rings and number fields. In this talk, I will describe these problems and their relationships.

The talk will be based on joint works with Miruna Rosca, Amin Sakzad, Ron Steinfeld and Alexandre Wallet: IACR eprint 2017/628 and 2018/170.