Hardness and advantages of Module-SIS and LWE.

Adeline Roux-Langlois, Univ Rennes, CNRS, IRISA

Most lattice-based cryptographic schemes are built upon the assumed hardness of the Short Integer Solution (SIS) and Learning With Errors (LWE) problems. Their efficiencies can be drastically improved by switching the hardness assumptions to the more compact Ring-SIS and Ring-LWE problems. However, this change of hardness assumptions comes along with a possible security weakening as the ring variants are only known to be as hard as their restrictions to special classes of ideal lattices. In this talk, we will discuss the hardness of the module variants of SIS and LWE, which bridge SIS with Ring-SIS, and LWE with Ring-LWE, respectively, and the advantages of those problems to build practical constructions.