A Gaussian Leftover Hash Lemma for Modules over Number Fields

Joël Felderhoff*[1]

[1]Department of Informatics [King's College London] – Royaume-Uni

Résumé

Given a Gaussian matrix X, a Gaussian Leftover Hash Lemma (LHL) states that X*v for a Gaussian v is an essentially independent Gaussian sample. It has seen numerous applications in cryptography for hiding sensitive distributions of v. We generalise the Gaussian LHL initially stated over ZZ by Agrawal, Gentry, Halevi, and Sahai (2013) to modules over number fields. Our results have a sub-linear dependency on the degree of the number field and require only polynomial norm growth: ——v——/——X——. To this end, we also proof when X is surjective (assuming the Generalised Riemann Hypothesis) and give bounds on the smoothing parameter of the kernel of X. We also establish when the resulting distribution is independent of the geometry of X and establish the hardness of the k-SIS and k-LWE problems over modules based on the hardness of SIS and LWE over modules, which was assumed without proof in prior works.

*Intervenant