Diploma-/Master-Thesis

Estimation of the hardness of LWE given a fixed number of samples

1. General Information

Lattice-based cryptography is a very promising candidate for the future when potential quantum computers might exist. Many of the proposals for lattice-based cryptosystems are based on the hardness of instantiations of the Learning with Errors Problem (LWE). Recently Albrecht et al. published an online tool (“LWE-Estimator”) to easily choose secure instantiations of LWE. During the estimation, the optimal number of LWE-samples is computed and used, which is not always given in reality. Hence, in most cases the choice of parameters is very conservative.

2. Goals

Extension of the “LWE-Estimator” such that the number of samples is taken into account. To this end, algorithms to solve LWE have to be understood, analyzed, changed such that they take the number of samples into account, and implemented as part of the “LWE-Estimator”.

3. Required Skills

The required skills are:

- Good Code programming skills (preferable but not restricted to sage and python)
- Knowledge about lattice-based cryptography (or post-quantum crypto)
- Knowledge in linear algebra

The Thesis should be written in English using LateX.

4. Contact

If you are interested, please contact Nina Bindel (Room S2/B212), eMail: nbindel@cdc.informatik.tu-darmstadt.de

5. Material

The material for this project includes but is not restricted to the following paper:


The source code of the “LWE-Estimator” can be found at https://bitbucket.org/malb/lwe-estimator/src

17.03.2016