
Bachelor-Thesis

Parallelization of lattice basis reduction

One promising approach in lattice basis reduction is the usage of parallelized processes. With today's multicore-processors it is possible to split the computation into several parts and compute them parallel. We will use this technique to speed up lattice reduction algorithms.

Goals

The main goal of the bachelor thesis is to give an overview of parallelization ideas used in lattice basis reduction. There are some reduction algorithms which allow parallelization, others are not considered to. Some common literature shall be summarized here (e.g. [1]).

Subsequently, it will be investigated whether the ideas of parallelized computing can be integrated into reduction algorithms that were not considered before. A practical implementation of the examined algorithms might be possible.

Required Skills

The required skills, in order of importance, are:

- good knowledge in linear algebra
- Course '*Introduction to Cryptography*'
- Some knowledge on lattices would be helpful

The thesis will be written in \LaTeX . Clearly knowledge of the English language is required to get along with the technical literature.

Contact

If you are interested, please contact Michael Schneider.
Room: B214
EMail: mischnei@cdc.informatik.tu-darmstadt.de



Bibliography

- [1] Gilles Villard. Parallel lattice basis reduction. In *ISSAC '92: Papers from the international symposium on Symbolic and algebraic computation*, pages 269–277, New York, NY, USA, 1992. ACM.
-