Lattice-Based Cryptography in Java

Advisor(s): Sebastian Ramacher

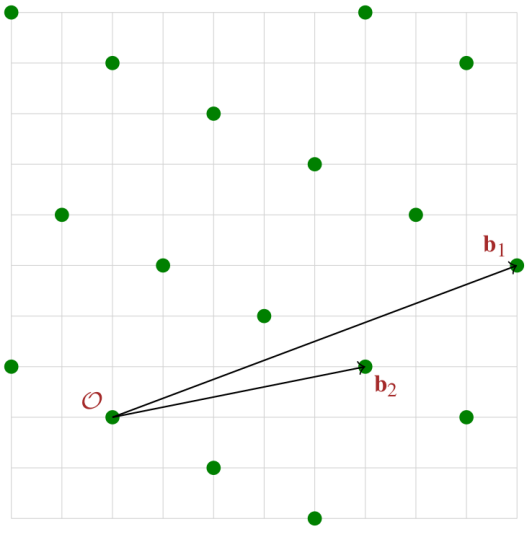
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Lattice-based cryptography is subfield of modern cryptography, which is gaining increasing popularity. Besides enabling efficient cryptographic constructions and offering resistance against quantum computer attacks, lattices are an important foundation for a plethora of recent cryptographic concepts, such as fully-homomorphic encryption, multilinear maps, attribute-based encryption and so on.

Goals and Tasks

- Getting familiar with the concept of lattice-based cryptography
- Lattice implementation in Java
- Proof-of-concept implementation of a cryptographic lattice scheme
- Performance evaluations



Literature

- D. Micciancio and O. Regev
  Lattice-based Cryptography
  Manuscript 2008
- T. Güneysu et al.
  Software speed records for lattice-based signatures
  Post-Quantum Cryptography 2013

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW ☒ TM

Prerequisites

- Basic cryptographic background
- Java

Advisor / Contact

sebastian.ramacher@iaik.tugraz.at