Post-Quantum Secure Accumulators

Advisor(s): Daniel Slamanig and Sebastian Ramacher

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

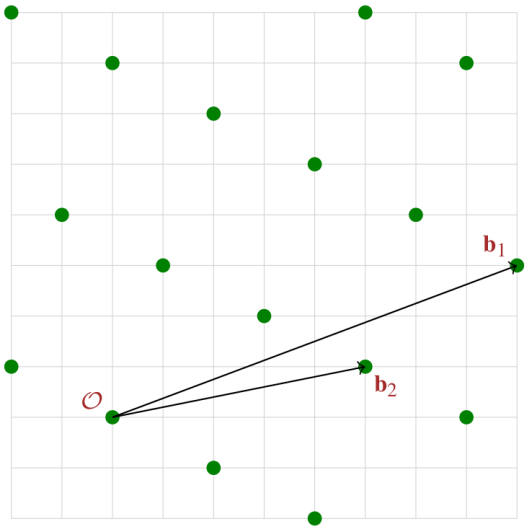
Motivation

Cryptographic accumulators allow to accumulate a finite set of values into a single succinct accumulator. For every accumulated value, one can efficiently compute a witness of membership, but it is computationally infeasible to find a witness for any non-accumulated value.

Accumulators have proven to be important building blocks in numerous cryptographic schemes such group signatures, redactable signatures etc. To be able to use aforementioned primitives in the presence of a quantum computer, one needs to rely on accumulators based on quantum immune problems (such as those related to lattices). Only recently suitable lattice-based candidates have been proposed. However, it is still unclear if they perform reasonably well in practice.

Goals and Tasks

- Getting familiar with the concept of lattice-based cryptography
- Proof-of-concept implementation of a lattice based accumulator
- Performance evaluation



Literature

- B. Libert et al.
  Zero-Knowledge Arguments for Lattice-Based Accumulators: Logarithmic-Size Ring Signatures and Group Signatures Without Trapdoors
  Advances in Cryptology - EUROCRYPT 2016
- D. Derler, C. Hanser, and D. Slamanig
  Revisiting Cryptographic Accumulators, Additional Properties and Relations to Other Primitives
  Topics in Cryptology - CT-RSA 2015

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

Prerequisites

- Basic cryptographic background
- Java programming

Advisor / Contact

daniel.slamanig@iaik.tugraz.at