Post-Quantum Secure Accumulators from Symmetric Key Primitives

Advisor(s): 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 value, called an 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 as ring signatures, group signatures, redactable signatures, and others. 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 symmetric key primitives). Only recently suitable 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 post-quantum accumulators
- Proof-of-concept implementation of a ring signature scheme
- Performance evaluation

Literature

- D. Derler, S. Ramacher, and D. Slamanig
  Post-Quantum Zero-Knowledge Proofs for Accumulators with Applications to Ring Signatures from Symmetric-Key Primitives
  PQCrypto 2018
- 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
- Programming (C/C++, Java or Python)

Advisor / Contact

sebastian.ramacher@iaik.tugraz.at