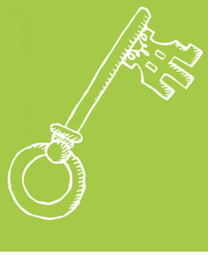

Post-Quantum Oblivious Transfer

Advisor: **Lukas Helminger**

Motivation

Oblivious transfer (OT) is a fundamental cryptographic task. It is a two-party protocol. The sender holds two messages m_0, m_1, and the receiver holds one bit b. OT allows the receiver to learn m_b, but nothing else. On the other side, the sender does not learn b, i.e., which messages the receiver learned. This functionality is widely used in secure multi-party computation (MPC), which is a subfield of cryptographic. MPC is used to create privacy-preserving applications of all kinds.

Until recently, the security of OT was based on the hardness of computing the prime factorization or computing the discrete logarithm. Both of those problems become feasible with quantum computers. In November 19, Masny and Rindal published the first-ever post-quantum secure OT. Their construction uses CRYSTALS-KYBER, which is a key encapsulation mechanism. CRYSTALS-KYBER is a lattice-based second-round candidate in NIST post-quantum cryptography standardization process.

Due to the generic nature of Masny's and Rindal's construction, one should be able to instantiate it with other NIST post-quantum candidates. It would be interesting how the different lattice-based candidates would perform when used as a building block for post-quantum OT. What is their runtime? How high his their communication complexity?

Goals and Tasks

- Get familiar with OT and post-quantum cryptography
- Implement post-quantum OT with different candidates form NIST post-quantum competition
- Evaluate the performance of the different post-quantum OT implementations and analyse the results

Literature

- D. Masny and P. Rindal
  Endemic Oblivious Transfer
  CCS
- NIST Post-Quantum-Cryptography
  https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

Schedule

- Reading related work and first steps
- Intermediate presentation or poster
- Implementing, experiments, ...
- Writing thesis
- Final presentation

Recommended if you're studying

☒ CS ☒ ICE ☒ SEM

Prerequisites

- Programming: C, C++
- Interest in Post-Quantum Cryptography

Advisor / Contact

lukas.helminger@iaik.tugraz.at