Title: Quantum Assisted Secure Multiparty Computation

Abstract

Quantum cryptography explores quantum physics properties to enhance cryptographic methods beyond classical approaches. Quantum key distribution (QKD) has been a major focus, but advancements in two-party primitives like quantum oblivious transfer (QOT) also hold promise for quantum-safe computation. This thesis starts by reviewing the literature about QOT, covering proposed protocols, security requirements, impossibility results, and scrutinizing conditions for QOT's full quantum safety.

Oblivious transfer (OT) plays a crucial role in secure multiparty computation (SMC), promising advancements in data analysis and computation privacy. The thesis assesses quantum OT's complexity against two leading classical OT protocols, shedding light on potential benefits and limitations for SMC security and efficiency.

Expanding on the theoretical analysis of quantum and classical oblivious transfer, the thesis integrates both into a secure multiparty computation (SMC) system for genomic analysis. Using quantum cryptographic protocols, the proposed system enhances privacy in computing a phylogenetic tree from private genome sequences. Three quantum cryptographic protocols are integrated to fortify security against quantum attacks. We include a complexity analysis, a security proof, and detailed implementation insights. Evaluation against a classical-only solution shows similar execution times, with the quantum-assisted approach introducing a time overhead in the oblivious key management system.

The thesis introduces the first quantum protocol for oblivious linear evaluation, a generalized form of oblivious transfer. In this scenario, distrustful parties, Alice and Bob, collaboratively compute a linear function without disclosing their inputs. While classical methods rely on oblivious transfer, the thesis unveils a novel quantum protocol independent of quantum oblivious transfer. The protocol employs high-dimensional quantum states to compute the linear function on Galois fields, extending from semi-honest to dishonest settings using a commit-and-open strategy. Security is rigorously proven in the framework of quantum universal composability, and the protocol is generalized for vector oblivious linear evaluation, enhancing efficiency.

Key-words: quantum cryptography, quantum oblivious transfer, quantum oblivious linear evaluation, secure multiparty computation, UC security.