Mingrui Zou

zmr0920@gmail.com Mingrui Zou wangbard.github.io/about/ wangbard

Education

The University of Edinburgh 09/2023 - 11/2024

Master of Science in Cybersecurity, Privacy and Trust *MSc With Distinction*

- **Relevant modules and grades:** Introduction to Quantum Programming and Semantics (70), Honours Algebra (66), Blockchains and Distributed Ledgers (76), Algorithmic Game Theory and its Applications (76).
- **Thesis title**: *Multiparty Computation Combiners.*

The University of Edinburgh 09/2018 - 07/2023

Bachelor of Science with Honours in Artificial Intelligence and Computer Science *Upper Second-Class Honours*

- **Relevant modules and grades:** Introduction to Quantum Computing (82), Quantum Cyber Security (93), Introduction to Modern Cryptography (95).
- **Thesis title**: *Helping Yuppies on Quantum Information Effects.*

Thesis Projects

Multiparty Computation Combiners 2024/04-2024/08

- In my Master's thesis, supervised by Dr. Michele Ciampi and awarded the Cyber Security, Privacy and Trust MSc Dissertation Prize, I investigated the construction of cryptographic combiners for secure multiparty computation (MPC). Given that Oblivious Transfer (OT) is a fundamental building block in many MPC protocols—and that previous research has shown the impossibility of transparent black-box construction for 1-out-of-2 OT combiners—the design of secure MPC combiners poses unique challenges. In this research, I introduce the first formal definition of black-box MPC combiners, which ensure that secure computation can still be achieved even if some underlying protocols fail, as long as a subset of the candidates remains reliable. A key contribution is the design and analysis of a 1-out-of-2 MPC combiner that securely computes a function for two parties under semi-honest setting using two candidate MPC protocols, under the assumption that at least one remains secure. Through rigorous cryptographic analysis, employing simulation-based security proofs and theorems, the combiner's design was validated to ensure security for at least one party. I also discussed the inherent limitations in achieving full two-party security under two protocols. Building on the this, I developed a 2-out-of-3 MPC combiner that requires at least two out of three candidate protocols to remain secure. I examined the vulnerabilities of this approach and proposed an alternative construction that, while less efficient, provides robust security guarantees.

Helping Yuppies on Quantum Information Effects 2022/09-2023/04

- This undergraduate thesis, supervised by Prof. Chris Heunen, focused on analyzing the type-and-effect interpretation of measurement as introduced in his paper *"Quantum Information Effects"*. The study formulated measurement as a computational effect, involving both the introduction of ancilla systems (allocation) and the selective reduction of information (hiding) to exploit the purification of quantum states. In my thesis, a Haskell program was developed based on the proposed categorical semantics to calculate the minimum number of ancilla (auxiliary qubits) required for measurement as a quantum information effect, demonstrating the practical application of these theoretical concepts. Additionally, a mathematical proof was formulated to elucidate the relationship between the minimum number of ancilla qubits needed and the von Neumann entropy of the system.

Skills

Programming Skills: Python, Java, Haskell, C, LaTeX, Linux, Solidity
Languages: English, Mandarin Chinese
Interests: Cryptography, Quantum Algorithm, Quantum Information, Multiparty Computation, Algebra, Blockchain

Academic Awards

- **Cyber Security, Privacy and Trust MSc Dissertation Prize** 11/2024