STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Lac Nguyen
Degree:	Doctor of Philosophy, Interdisciplinary
School:	Charles V. Schaefer, Jr. School of Engineering and Science
Department:	Physics and Electrical & Computer Engineering
Date:	Wednesday, May 3rd, 2023
Time/Location:	2:30 PM/ Babbio Center, room 320
Title:	A practical approach for quantum cryptography with quantum authentication
Chairperson:	Dr. Yuping Huang, Department of Physics, School of Engineering and Science
Committee Members:	Dr. Cristina Comaniciu, Department of Electrical & Computer Engineering, School of Engineering and Science Dr. Kevin Lu, Department of Electrical & Computer Engineering, School of Engineering and Science Dr. Yong Meng Sua, Department of Physics, School of Engineering and Science Dr. Rupak Chatterjee, Department of Physics, School of Engineering and Science Dr. Michael Zabarankin, Department of Mathematical Sciences, School of Engineering and Science

ABSTRACT

Quantum mechanics provides a revolutionary approach to secure communication by utilizing superposition, entanglement, and measurements. Current cryptographic protocols such as data encryption, authentication, digital signatures, privacy-preserving computing, and hash functions rely on public-private key (PPK) encryption based on the prime factor problem. This method is vulnerable to quantum computers (QC) that can break PPK in almost no time. As a result, digital data, finance, and communication are at risk. Although post-quantum cryptography methods have been developed to replace PPK, they are not yet confirmed to be immune to future quantum algorithms. A defensive approach to quantum communication has been quantum key distribution (QKD). However, this technology is not a universal solution for secret and secure communication. It only provides secure encryption, assuming a pre-authenticated channel between participants, and does not address the most prominent issues of network security. In this thesis, we propose a quantum network platform that supports multiple cryptographic protocols for communication among multiple users. On this platform, we demonstrate the broadcasting of quantum random numbers (QRNs) with arbitrary probability distribution and present a use case for a trustless decentralized quantum randomness consensus protocol. Next, we demonstrate a practical QKD system with multiple parties that doesn't require complex key distillation and error correction. We then introduce two additional quantum cryptography protocols: quantum private comparison (QPC) and quantum physical unclonable functions (QPUF). By combining these protocols with QKD, we demonstrate how quantum authentication and quantum encryption can be achieved in a single communication step. This approach provides a complete replacement for PPK and opens an avenue towards fully practical quantum communication networks.