Quantum Science
& Engineering Center

Quantum Computing Seminar Series

GEORGE MASON UNIVERSITY

Jiayu Zhang

California Institute and Technology

New Approaches for Quantum Delegation: Succinct Blind Quantum Computation Using a Random Oracle & Classical Verification of Quantum Computations in Linear Time

Monday, April 4, 2022 | 12–1pm | Zoom

Abstract

In the universal blind quantum computation problem [arXiv:0807.4154], a client wants to make use of a single quantum server to evaluate C|0⟩ where C is an arbitrary quantum circuit while keeping C secret. The client's goal is to use as few resources as possible. This problem has become fundamental to the study of quantum cryptography, not only because of its own importance, but also because it provides a testbed for new techniques that can be later applied to related problems (for example, quantum computation verification). Known protocols on this problem are mainly either information-theoretically (IT) secure or based on trapdoor assumptions (public key encryptions).

In the first part of this talk we study how the availability of symmetric-key primitives, modeled by a random oracle, changes the complexity of universal blind quantum computation. We give a new universal blind quantum computation protocol. Similar to previous works on IT-secure protocols (for example, BFK [FOCS09, arXiv:0807.4154]), our protocol can be divided into two phases. In the first phase the client prepares some quantum gadgets with relatively simple quantum gates and sends them to the server, and in the second phase the client is entirely classical -- it does not even need quantum storage. Crucially, the protocol's first phase is succinct, that is, its complexity is independent of the circuit size. Given the security parameter κ, its complexity is only a fixed polynomial of κ, and can be used to evaluate any circuit (or

several circuits) of size up to a subexponentially of κ. In contrast, known schemes either require the client to perform quantum computations that scale with the size of the circuit [FOCS09, arXiv:0807.4154], or require trapdoor assumptions [Mahadev, FOCS18, arXiv:1708.02130].

In the quantum computation verification problem, a quantum server wants to convince a client that the output of evaluating a quantum circuit C is some result that it claims. This problem is considered very important both theoretically and practically in quantum computation [arXiv:1709.06984], [arXiv:1704.04487], [arXiv:1209.0449]. The client is considered to be limited in computational power, and one desirable property is that the client can be completely classical, which leads to the classical verification of quantum computation (CVQC) problem. In terms of total time complexity of both the client and the server, the fastest single-server CVQC protocol so far has complexity O(poly(κ)|C|^3)where |C| is the size of the circuit to be verified, given by Mahadev [arXiv:1804.01082].

In the second part of this talk, by developing new techniques, we give a new CVQC protocol with complexity O(poly(κ)|C|), which is significantly faster than existing protocols. Our protocol is secure in the quantum random oracle model [arXiv:1008.0931] assuming the existence of noisy trapdoor claw-free functions [arXiv:1804.00640], which are both extensively used assumptions in quantum cryptography. Along the way, we also give a new classical channel remote state preparation protocol for states in {|+θ⟩=1√2(|0⟩+e^iθπ/4|1⟩):θ∈{0,1⋯7}}, another basic primitive in quantum cryptography. Our protocol allows for parallel verifiable preparation of L independently random states in this form (up to a constant overall error and a possibly unbounded server-side isometry), and runs in only O(poly(κ)L) time and constant rounds; for comparison, existing works (even for possibly simpler state families) all require very large or unestimated time and round complexities

Meeting Information

https://gmu.zoom.us/j/93426209769?pwd=TjNmaWpvMlYxRzZGUkNzeHdPV2g3QT09

About the Seminar Series

The Quantum Computing Seminar Series are a series of working seminars organized and hosted by QSEC's quantum computing subgroup on Mondays. These events are free and open to the public. More information is available on QSEC's Computing Events and Mathematical Sciences Department's Quantum Computing Seminars. For any questions, contact qsec@gmu.edu.