Quantum Computing Seminar

How to Verify a Quantum Computation

By

Joshua Nevin
(University of Ottawa)

Abstract: In this talk, we present a protocol introduced by Broadbent in [2] for verifying quantum computations on encrypted data, building on Selman's talk on the paper [1], also by Broadbent. In the protocol of [2], a verifier with limited quantum resources enables a remote (untrusted) quantum server to perform quantum computations on the verifier's encrypted input data. Analogous to [1], even a malicious prover deviating arbitrarily from the protocol cannot gain information about the client's secret input data, but also, in [2], we can upper-bound the probability that the malicious server, arbitrarily deviating from the protocol, can convince the verifier to accept the wrong output.

[1] Broadbent, Anne. "Delegating private quantum computations." Canadian Journal of Physics 93.9 (2015): 941-946.

[2] Broadbent, Anne. "How to Verify a Quantum Computation." Theory OF Computing 14.11 (2018): 1-37.

Date: May 13, Tuesday
Time: 17:30 UTC+3
Place: ZOOM

To request the event link, please send a message to cihan.okay@bilkent.edu.tr