Quantum Computing Seminar

Delegating Private Quantum Computations

By

Selman Ipek
(Bilkent University)

Abstract: In this talk, we present a protocol introduced by Broadbent [1] for delegating quantum computations on encrypted data. The protocol is intended for a client with limited quantum resources and enables a remote quantum server to execute a publicly known quantum circuit while the client's sensitive input data remains perfectly encrypted via the quantum one-time pad. In our scheme, all Clifford group operations are performed non-interactively on the encrypted data, while non-Clifford gates requires only minimal interaction—specifically, the client prepares and sends a single random auxiliary qubit and exchanges a couple of classical bits with the server. We also discuss the security proof, which guarantees that even a malicious server deviating arbitrarily from the protocol cannot gain any information about the client's data.
[1] A. Broadbent. Delegating private quantum computations. Canadian Journal of Physics. DOI: 10.1139/cjp-2015-0030.

Date: Apr 15, Tuesday
Time: 17:30 UTC+3
Place: ZOOM

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