Contribution ID: **39**

Type: **not specified**

Parallel self-testing of EPR pairs under computational assumptions

Tuesday, July 11, 2023 4:45 PM (20 minutes)

Honghao Fu, Daochen Wang and Qi Zhao

Abstract: Self-testing is a fundamental feature of quantum mechanics that allows a classical verifier to force untrusted quantum devices to prepare certain states and perform certain measurements on them. The standard approach assumes at least two spatially separated devices. Recently, Metger and Vidick [Quantum, 2021] showed that a single EPR pair of a single quantum device can be self-tested under computational assumptions. In this work, we generalize their results to give the first parallel self-test of N EPR pairs and measurements on them in the single-device setting under the same computational assumptions. We show that our protocol can be passed with probability negligibly close to 1 by an honest quantum device using poly(N) resources. Moreover, we show that any quantum device that fails our protocol with probability at most eps must be poly(N,eps)-close to being honest in the appropriate sense. In particular, our protocol can test any distribution over tensor products of computational or Hadamard basis measurements, making it suitable for applications such as device-independent quantum key distribution under computational assumptions. Moreover, a simplified version of our protocol is the first that can efficiently certify an arbitrary number of qubits of a single cloud quantum computer using only classical communication.

Presenter: FU, Honghao

Session Classification: Track A-2