Delegating Private Quantum Computations

Anne Broadbent

Abstract

Given the technological challenge in building quantum computers, it is likely that their initial availability will be in a client-server configuration. We address the question of privacy in this scenario, by showing that an almost-classical client can delegate the execution of any quantum computation, where the data uploaded to the server is encrypted via the one-time pad. In order to do this, the quantum power required of the client is limited to being able to prepare random BB84 states. We give a simulation-based security definition and a rigorous proof of security using a transformation to an entanglement-based protocol.