Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources

Andrea Coladangelo [*] Alex Grilo[†] Stacey Jeffery[‡] Thomas Vidick[§]

Abstract

The problem of reliably certifying the outcome of a computation performed by a quantum device is rapidly gaining relevance. We present two protocols for a classical verifier to verifiably delegate a quantum computation to two non-communicating but entangled quantum provers. Our protocols have near-optimal complexity in terms of the total resources employed by the verifier and the honest provers, with the total number of operations of each party, including the number of entangled pairs of qubits required of the honest provers, scaling as $O(g \log g)$ for delegating a circuit of size g. This is in contrast to previous protocols, whose overhead in terms of resources employed, while polynomial, is far beyond what is feasible in practice. Our first protocol requires a number of rounds that is linear in the depth of the circuit being delegated, and is blind, meaning neither prover can learn the circuit or its input. The second protocol is not blind, but requires only a constant number of rounds of interaction.

Our main technical innovation is an efficient rigidity theorem which allows a verifier to test that two entangled provers perform measurements specified by an arbitrary m-qubit tensor product of single-qubit Clifford observables on their respective halves of m shared EPR pairs, with a robustness that is independent of m. Our two-prover classical-verifier delegation protocols are obtained by combining this rigidity theorem with a single-prover quantum-verifier protocol for the verifiable delegation of a quantum computation, introduced by Broadbent.

[*]Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, USA. email: acoladan@caltech.edu. Supported by AFOSR YIP award number FA9550-16-1-0495.

[†]IRIF, CNRS/Université Paris Diderot, Paris, France. email: abgrilo@irif.fr. Supported by ERC QCC.

[‡]QuSoft and CWI, Amsterdam, the Netherlands. email: jeffery@cwi.nl. Supported by an NWO WISE Grant.

[§]Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, USA. email: vidick@cms.caltech.edu. Supported by NSF CAREER Grant CCF-1553477, AFOSR YIP award number FA9550-16-1-0495, and the IQIM, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).