

Abstract Submitted
for the DAMOP20 Meeting of
The American Physical Society

An efficiently-verifiable test of quantum advantage GREGORY D. KAHANAMOKU-MEYER¹, SOONWON CHOI, UMESH V. VAZIRANI, NORMAN Y. YAO, University of California, Berkeley — Recently, quantum hardware has started to outperform classical computers at certain computational tasks (so-called quantum supremacy). Many protocols designed to demonstrate quantum advantages in computation have the undesirable feature that they are difficult to verify—checking whether or not a quantum machine produced correct results is as difficult as solving the problem classically. We propose a new test protocol that is efficiently verifiable and provably secure: the correctness of the results can be checked quickly (in polynomial time) by a classical machine, while passing the test with a classical machine is as hard as integer factorization. Such a protocol is essential in order to verify the performance of the first large-scale quantum devices; to our knowledge this protocol requires the least quantum resources of any proposal until now. In particular, we show that the resources are much less than those needed to run Shor’s algorithm, allowing its efficient implementation in near-term devices. We present multiple ways to realize our protocols using trapped ions and Rydberg atoms systems, and explicitly analyze qubit and gate counts. Finally, we discuss the protocol’s relevance in the broader landscape of quantum algorithms.

¹Supported by the Department of Defense (DoD) through the National Defense Science Engineering Graduate Fellowship (NDSEG) Program.

Gregory D. Kahanamoku-Meyer
University of California, Berkeley

Date submitted: 31 Jan 2020

Electronic form version 1.4