Title: Testing Quantum Devices and Quantum Mechanics

PI: Prof. Umesh V. Vazirani
University of California, Berkeley.

Abstract: The testing of quantum devices, besides being a pressing practical challenge, touches on foundational questions in quantum computational complexity, cryptography as well as the foundations of quantum mechanics. The classical verifier of such a device is necessarily at a disadvantage due to the exponential power of quantum systems, and an exciting recent development is the realization that uniquely quantum features such as entanglement can be leveraged to make such testing possible. A question of great theoretical and practical importance is whether it is possible for such testing to be carried out without relying on entanglement — i.e. for a classical verifier to test a single quantum device, rather than two spatially separated devices that share quantum entanglement. We propose to use existing postquantum cryptography to establish such a test for a quantum random number generator. We also propose to tackle the much harder challenge of classically test a claimed quantum computer. This will undoubtedly require the exploration of new cryptographic primitives for encrypting quantum states, such as quantum quantum analogs of homomorphic encryption and program obfuscation (two of the most powerful classical cryptographic primitives that have been invented over the last decade.

Another fundamental issue that we propose to explore is the efficiency and robustness of the testing protocols. Although there is a well developed theory of fault tolerance for quantum computation, it largely remains to be effectively applied in the quantum device testing setting. A closely related issue is the theory of PCPs, whose extension to the quantum setting has been a major challenge, but where recent results suggest promise of progress.

Finally, we propose to explore whether entanglement based tests of quantum devices can provide the basis of fundamentally new tests of quantum mechanics.