**MICHELE MOSCA**, Institute for Quantum Computing (UW) and Perimeter Institute
*Self-testing Quantum Apparatus*

In order to execute any quantum cryptographic protocol in practice, one must somehow trust that their quantum apparatus is faithfully executing the protocol.

Quantum self-testing defines a framework for testing quantum apparatus. I will show how a quantum circuit together with measurement apparatuses and EPR sources can be fully verified without any reference to some other trusted set of quantum devices (joint work with Magniez, Mayers and Ollivier). Our main assumption is that the physical system we are working with consists of several identifiable sub-systems, on which we can apply some given gates locally. We design a test for any quantum circuit whose complexity is linear in the number of gates and qubits, and polynomial in the required precision.

This self-testing procedure applies to protocols that only require states and operations with real-valued coefficients. The reason for this restriction was an intuition that computations with complex amplitudes can be simulated using only real amplitudes, and the simulation would not be unitarily equivalent to the desired complex amplitude computation. Recent work (with Matthew McKague) gives a simulation of general quantum circuits using states and unitaries with real coefficients only.