abstract

SPECIAL COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Using ideas from computational learning theory, I'll show that "for most practical purposes," one can learn a quantum state using a number of measurements that grows only linearly with the number of qubits n. By contrast, traditional quantum state tomography requires a number of measurements that grows exponentially with n. Besides possible applications in experimental physics, this learning theorem has two implications for quantum computing: first, the use of trusted classical advice to verify untrusted quantum advice, and second, a new simulation of quantum one-way protocols.

Even if one can "learn" a quantum state using a linear number of measurements, one might need an exponential amount of computation. As time permits, I'll discuss a result on how one might exploit that fact to copy-protect quantum software.