abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Suppose we have n players who wish to jointly perform a quantum computation, but some of them are faulty and are trying to learn privileged information and/or sabotage the computation. How many cheaters can we tolerate and still have a secure protocol? Secure multiparty classical computation is possible with fewer than n/3 cheaters, or fewer than n/2 when a secure broadcast channel is available. It turns out the same bounds hold in the quantum case.
In this talk I will sketch the construction, which owes a great deal to the classical solutions, but requires a number of new components as well.

This talk describes joint work with Crepeau, Gottesman, Hassidim, and Smith.