HARVARD UNIVERSITY
CENTER OF MATHEMATICAL
SCIENCES AND APPLICATIONS

20 Garden Street
Cambridge, MA 02138
Tel: (617) 496-5421
Fax: (617) 384-8348

CENTER OF MATHEMATICAL SCIENCES AND APPLICATIONS

# COLLOQUIUM

## Peter Shor

MIT

*will speak on:*

Quantum Money from Lattices

**Wednesday, February 19, 2020**
**4:30 pm – 5:30 pm**
**CMSA, 20 Garden St, G10**

Quantum money is a cryptographic protocol for quantum computers. A quantum money protocol consists of a quantum state which can be created (by the mint) and verified (by anybody with a quantum computer who knows what the "serial number" of the money is), but which cannot be duplicated, even by somebody with a copy of the quantum state who knows the verification protocol. Several previous proposals have been made for quantum money protocols. We will discuss the history of quantum money and give a protocol which cannot be broken unless lattice cryptosystems are insecure.