Geometry Seminar
Tuesday, November 16, 2010
Room 201 WWH at 6:00 P.M.

Quantum Money from Knots

Peter Shor
MIT.

The no-cloning theory of quantum mechanics says that an unknown quantum state cannot be copied. One might think that this would immediately lead to forgery-proof quantum states. However, to be useful, a copy-proof quantum state must also have some method to verify that it is the correct state, and for many possible schemes this verification method gives enough extra information to permit an adversary to copy the state.

Quantum money is a cryptographic protocol in which a mint can produce a quantum state, no one else can copy the state, and anyone (with a quantum computer) can verify that the state came from the mint. We present a concrete quantum money scheme based on superpositions of knot diagrams that encode oriented links with the same Alexander polynomial. We expect our scheme to be secure against computationally bounded adversaries.

For more information please visit the seminar website at:
`http://www.math.nyu.edu/seminars/geometry_seminar.html`.