1077-68-2759 **Peter W. Shor*** (shor@math.mit.edu), Room 2-369, 77 Mass. Ave., Cambridge, MA 02139.

Quantum Money from Knots.

Quantum money is a cryptographic protocol in which a mint can produce a quantum state, anyone (with a quantum computer) can verify that the state came from the mint, and nobody, even knowing the verification procedure, can copy the quantum state. We present a concrete quantum money scheme based on quantum superpositions of knot diagrams that encode oriented links having the same polynomial-time computable knot invariant (such as the Alexander polynomial). We will try to distill what kinds of classical algorithms for manipulating knots and knot diagrams would permit the breaking of this protocol for quantum money. This is joint work with Edward Farhi, David Gosset, Avinatan Hassidim and Andrew Lutomirski. (Received September 22, 2011)