Peter Shor

=============

Quantum Money

We discuss a new cryptographic task which we believe may be possible with quantum information, but which is impossible with classical information. This is the creation of unforgeable states, or quantum money. Public-key quantum money is a cryptographic protocol in which a mint can create quantum states that anyone with a quantum computer can verify but no one, except possibly the mint, can clone or forge. With quantum computers, these states could be useful as identification cards or as money. We present a general blueprint for a quantum money protocol as well as a concrete example of this blueprint based on knot invariants.