

The Vienna Doctoral Programme on Complex Quantum Systems
invites to a

SEMINAR TALK

by

Scott Aaronson

MIT

Quantum Money from Hidden Subspaces

(Joint work with Paul Christiano)

Forty years ago, Wiesner pointed out that quantum mechanics raises the striking possibility of money that cannot be counterfeited according to the laws of physics. We propose the first quantum money scheme that is (1) public-key---meaning that anyone can verify a banknote as genuine, not only the bank that printed it, and (2) cryptographically secure, under a "classical" hardness assumption that has nothing to do with quantum money. Our scheme is based on hidden subspaces, encoded as the zero-sets of random multivariate polynomials. A main technical advance is to show that the "black-box" version of our scheme, where the polynomials are replaced by classical oracles, is unconditionally secure. Previously, such a result had only been known relative to a quantum oracle (and even there, the proof was never published). Even in Wiesner's original setting---quantum money that can only be verified by the bank---we are able to use our techniques to patch a major security hole in Wiesner's scheme. We give the first private-key quantum money scheme that allows unlimited verifications and that remains unconditionally secure, even if the counterfeiter can interact adaptively with the bank. Our money scheme is simpler than previous public-key quantum money schemes, including a knot-based scheme of Farhi et al. The verifier needs to perform only two tests, one in the standard basis and one in the Hadamard basis---matching the original intuition for quantum money, based on the existence of complementary observables. Our security proofs use a new variant of Ambainis's quantum adversary method, and several other tools that might be of independent interest.

The seminar talk will be preceded by a CoQuS Student talk at 17:00 s.t.

"Quantum interferometric visibility as a witness of general relativistic proper time"
by Magdalena Zych / University of Vienna

Monday, January 30th, 2012
17:30 hrs s.t.

Ernst-Mach-Hörsaal, Boltzmanngasse 5, 1090 Wien