

## Quantum Money

Andrew Lutomirski (joint work with E. Farhi, D. Gosset, A. Hassidim and P. W. Shor)

Quantum money is a cryptographic protocol that is meant to work like paper money. A mint can produce a quantum state (the banknote), no one else can copy the state, and anyone can verify that the state came from the mint. All previous known implementations are either insecure, require an oracle with no known realization, or require that the mint be involved in the verification process. I'll describe some prior work in the field and why designing quantum money is hard. Then I'll present a concrete quantum money scheme based on superpositions of diagrams that encode oriented links with the same Alexander polynomial (and tell you what that means, for those of you who aren't knot theorists). Finally, I'll explain why my collaborators and I expect the scheme to be secure against computationally bounded adversaries.