Breaking and making quantum money: toward a new quantum cryptographic protocol

Andrew Lutomirski, MIT
with: Scott Aaronson, Edward Farhi, David Gosset, Avinatan Hassidim, Jon Kelner, and Peter Shor
What is a quantum state?

$n$ qubits

State is in a $2^n$ dimensional Hilbert space

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$
Unknown states cannot be copied!
Properties of quantum money

- The bank can print it
- Anyone can verify it (public-key)
- No one can copy it
A single piece of quantum money

- A quantum state
- A “serial number” that encodes a circuit to verify the state
- A digital signature of the serial number
Properties of quantum money

- The bank can print it
- Anyone can verify it (public-key)
- No one can copy it
- Collision-free: *no one* can produce two states with the same serial number
Germany

Value of one gold Mark in paper Marks
Random secret description of state

- Actual copy of the state
- Obscured verification circuit

Quantum money
Postselection money

Labeling function: \( L : S \rightarrow T \) \( \|S\| \gg \|T\| \)

\[
|\psi_\ell\rangle = \frac{1}{\sqrt{\|L^{-1}(x)\|}} \sum_{x \text{ s.t. } L(x) = \ell} |x\rangle
\]
Verification

Markov chain that mixes rapidly over states with the same label

\[ M|\psi_\ell\rangle = |\psi_\ell\rangle \]

\[ M^r \approx \sum_\ell |\psi_\ell\rangle\langle\psi_\ell| \]
Verification

Markov matrix has a special form:

\[ U = \sum_i P_i \otimes |i\rangle \langle i| \]

\[
\left( I \otimes \frac{1}{\sqrt{N}} \sum_{i=1}^{N} \langle i| \right) U \left( I \otimes \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle \right) \\
= \frac{1}{N} \sum_{i=1}^{N} P_i \\
= M
\]
Breaking stabilizer money

- Secret is a description of a list of stabilizer states
- A parameter controls the strength of the verifier
- Weak verifiers accept non-stabilizer states
- Strong verifiers allow us to recover the secret