Bombs that don't explode!
Undetectable forgery!

An adaptive attack on Wiesner's quantum money.

Daniel Nagaj — Slovak Academy of Sciences
Or Sattath — UC Berkeley
Aharon Brodutch — IQC Waterloo
Dominique Unruh — University of Tartu, Estonia

Classical money is hard to forge practically (watermarks, special paper), while quantum money is attractive because its security relies no-cloning. The first quantum money scheme was introduced by Wiesner around 1970. Today, we have more sophisticated quantum money, but Wiesner's idea remains appealing because of its clean concept and simple implementation.

We show an efficient adaptive attack on Wiesner's quantum money in a strict testing scenario, when valid money is accepted and returned, while handing in invalid money is highly discouraged. Our approach is inspired by the Elitzur-Vaidman bomb testing problem. We break the protocol with 4 hidden states, and then present general single-qubit tomography under strict testing.

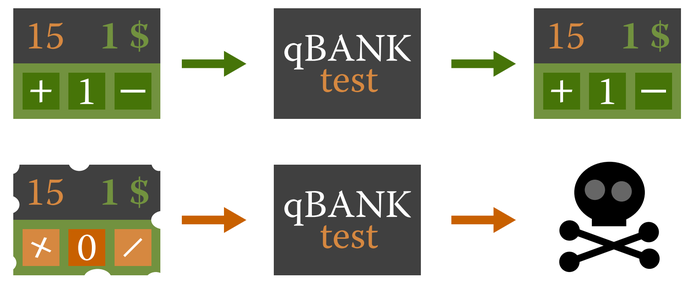
1 Wiesner's quantum money

- A classical serial # and a secret quantum state.

- Security: no cloning for non-OG states.

2 Strict testing

- When you pass the test, you get your money (state) back.
- You *don't* want to fail a test.

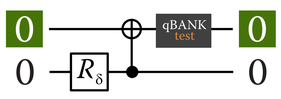


3 Finding the secret state without failing the test

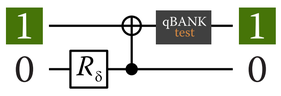
- Elitzur & Vaidman can test bombs using the quantum Zeno effect.

  We run a similar test on the four secret states used in Wiesner's money.

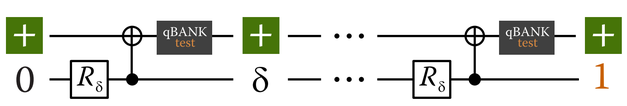
  R_δ is a rotation by $\delta=\pi/2N$ for large N.

- 

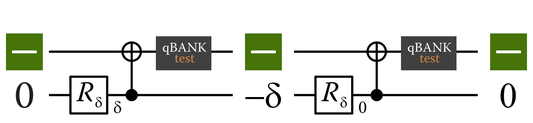
  Failure probability of one test $\sim\delta^2$.
  Repeat N times, reusing the ancilla.
  The ancilla remains in the state 0.
  Total probability of detection $p_\text{☠}\sim 1/N$.

- 

  Just as for 0, the ancilla stays 0.
  Total probability of detection $p_\text{☠}\sim 1/N$.

- 

  When reusing the ancilla over N rounds, it slowly rotates to the state 1!
  The state always passes the bank's test.

- 

  Do N tests. In even rounds, the ancilla is 0.
  The state always passes the bank's test.

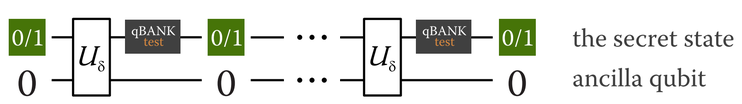
- This way we can identify + in N rounds.
  We get caught with probability $p_\text{☠}\sim 1/N$.
- *How would you identify* −, 0, 1*?*
- *How many rounds for n qubits?* (hint: parallel, ans: $O(n/p_\text{☠})$)

4 A different attack: weak coupling

- In bomb-testing, we flip the secret state if the ancilla is near 1.
  Here we ensure that the state doesn't change very much in any round, coupling the ancilla and the secret state with $U_\delta=e^{-i\delta(X\otimes X)}$.

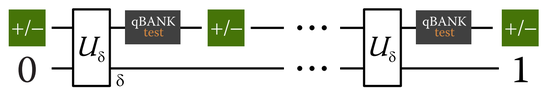
  Applied to z-basis states, U_δ is close to the identity.

  When the secret state is in the x-basis, U_δ simplifies a lot to $e^{\mp i\delta(I\otimes X)}$.

- 

  Probability to fail one test $\sim\delta^2$.

  Do N tests, reuse the ancilla; it remains 0. Total probability of failure $p_\text{☠}\sim 1/N$.

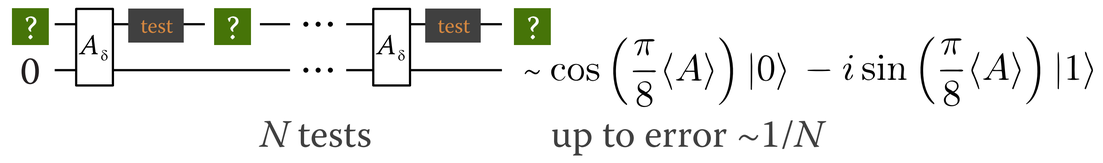
- 

  Do N rounds, reuse the ancilla; it slowly moves towards 1.
  The secret state always passes the test.

- We can safely identify whether the secret state is in the z- or x-basis.

5 Single-copy tomography from strict testing

- Let's couple the ancilla and the unknown state by $A_\delta=e^{-i\delta(A\otimes X)}$.
- We can now estimate the expectation value of the operator A in a single copy of an unknown state, if we have a strict tester for this state.



- After N rounds of testing, the ancilla has info about $\langle A\rangle$.
  During all this, we almost never fail a test, as the overall $p_\text{☠}\sim 1/N$.

Our preprint 1404.1507

Quantum money — Bennett, Brassard, Breidbart, Wiesner, Advances in Cryptology (1983)
Gavinsky, IEEE CCC (2012)
Pastawski, Yao, Jiang, Lukin, Cirac, Proceedings NAS (2012)
Aaronson, Christiano, ACM STC (2012)
Quantum Zeno effect — Elitzur, Vaidman, Foundations of Physics (1993)

Acknowledgements

We would like to thank Scott Aaronson, Dorit Aharonov, David Gosset, Guy Kindler, Carl Miller, StephenWiesner and Lev Vaidman for valuable discussions, and the Simons institute Quantum Hamiltonian Complexity program, during which a substantial part of this work was done. DN also thanks the Slovak Research and Development Agency grant APVV-0808-12 QIMABOS. OS also thanks the ARO Grant W922NF-09-1-0440 and NSF Grant CCF-0905626. DU was supported by the Estonian ICT program 2011-2015 (3.2.1201.13-0022), the European Union through the European Regional Development Fund through the sub-measure "Supporting the development of R&D of info and communication technology", by the European Social Fund's Doctoral Studies and Internationalisation Programme DoRa, and by the Estonian Centre of Excellence in Computer Science, EXCS. AB is supported by NSERC, Industry Canada and CIFAR.