Lecture 9: Quantum Money

(Charles H. Bennett was one of the pioneers of Q.C.
He was an undergrad at Brandeis in the early '60s.
He had a friend there, an undergrad called Stephen Wiesner.
By the late '60s they were grad students in physics; Wiesner @ Columbia, Bennett @ Harvard. In '69, W. went to visit B. at Harvard and told him about his cool idea for... Quantum Money (and superdense coding, and some other things...
Bear in mind: 10-15 years before inklings of quantum computing, proof of No-Cloning Thm...)

(Wiesner wrote up his ideas and submitted to the prestigious IEEE Trans. on Info. Theory. Rejected as nonsense. Supposedly resubmitted several times to various journals, always rejected. He got out of academics, I think, and the idea of q. money was only kept alive by Bennett telling people about it periodically.
Bennett went to work at IBM and was a well known physics/C.S. researcher...)

(Gilles Brassard was a French-Canadian guy who got his PhD from Cornell in 1979, studying cryptography under Hopcroft. In Oct. '79 he was swimming at a hotel beach in San Juan, P.R. A guy he'd never met swam up to him and started telling him about Wiesner's theory of quantum money.

"The most bizarre, and certainly the most magical, moment in my professional life." - Brassard.

To be fair, Brassard & Bennett were both there for the 20th F.O.C.S. conference in T.C.S. Brassard was to deliver a crypto talk, and Bennett had recognized him.

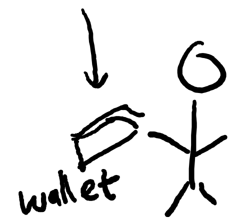
B. & B. started talking about cryptographic angles on quantum money - bear in mind, in 1979 RSA had _just_ come out; Diffie-Hellman was a few years before. In '82, they wrote a notable paper called "Quantum Crypto"; went on to be Q.C. pioneers (e.g., they were on the Teleportation paper).

And Wiesner? His paper finally published in '83 in a journal issue for CRYPTO'81 papers. He now - by choice - works as a laborer in Jerusalem.)

(So what *is* ("private key") Quantum Money?)

BANK $\xrightarrow{\text{issues}}$ "coins"/"bills"/"tokens"

ⓢ ↳ multi-qubit states



(People can carry them around, trade them, etc.)

(Even today, storing qubits is hard for fancy physics labs. So Q. Money is def. technologically infeasible now.)

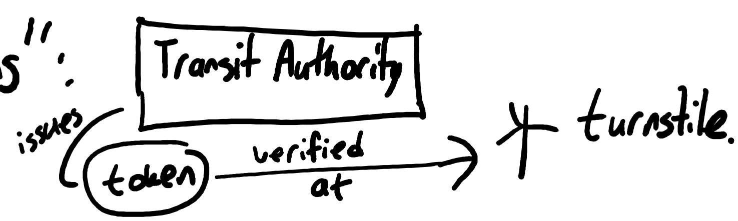
ⓢ ~~→~~ ⓢⓢ duplication ("counterfeiting") should be impossible (w.h.p.) b/c of "no cloning"

(This is the potential beauty of quantum money. Any classical info can be "copied": Even if printed in fancy ink on paper/textile/plastic.)

To test if coin ? is valid/forged, must take it to bank.

(This may seem annoying, that 3rd party, bank, must be involved to verify transaction. So you might prefer to think instead of..."

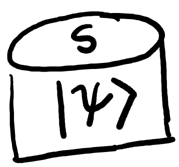
"Quantum subway tokens":



Wiesner's Scheme

- "n" is a "security parameter", e.g. $n = 256$
  (trades off security vs. efficiency)
- To create a quantum coin, Bank...
  - Picks $s \in \{0,1\}^n$ at random
    ↑ "serial number"
  - Picks $q \in \{0,1,+,-\}^n$, (2n random bits)
    e.g. $(0,+,-,1,1,\ldots,+)$

    Creates associated n-qubit state

    $$|\psi\rangle = |0\rangle \otimes |+\rangle \otimes |-\rangle \otimes |1\rangle \otimes |1\rangle \otimes \cdots \otimes |+\rangle$$
    (e.g.)
- 

  ← this is the coin/token
  ($|\psi\rangle$ in a container, with s printed on the side)

Bank maintains big list of (s,q) pairs.

OR [BBBW '82]: Bank/transit authority one time picks a secret key $K \in \{0,1\}^n$. Then $q := AES_K(s)$
↑ pseudorand. fcn.

Now no storage needed — especially nice for subway turnstiles.

Verification of $(|\psi\rangle, s)$

- Bank looks at serial #s, determines q.

(NB: Bank cannot just look at $|\psi\rangle$ to check against q.)

- Bank measures i^{th} qubit in appropriate basis ($\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$), checks whether outcome matches q_i
- If all n checks pass, ☺ (?)
  Bank: gives back the (post-measurement) $|\psi\rangle$
  Turnstile: eats token & lets you pass
- If ≥ 1 check fails, ☹
  Bank: calls the police?
  Turnstile: spits token back out?

[[Hmm. More on this later.]]

[[It's not totally obvious the Authority should freak out if, say, 1 out of n measurements fail. Maybe one qubit decohered in the holder's wallet...

Well, we'll discuss later. For now, assume 1 failure = police!]]

Non-counterfeitability

$$(s, |\psi\rangle) \not\rightarrow (s, |\psi\rangle),\ (s, |\psi\rangle)$$

(Want to rule out a malicious party doing this.)

(We know by "No Cloning Theorem" that doing $|\psi\rangle \mapsto |\psi\rangle \otimes |\psi\rangle$ with 100% prob, for all $|\psi\rangle$ is impossible. But we didn't rule out the ability to do this w/ prob. 90% or 10%.)

Simple attack that works w. prob. $\left(\frac{5}{8}\right)^n$.

[Like 2^{-175} if $n = 256$. "Un-physically" tiny, which is good!]

- Measure each qubit of $|\psi\rangle$ in standard basis
- Get some outcomes, e.g. $r = 01101\ldots$
- Make 2 (or more!) copies of $(s, |01101\ldots\rangle)$

Pr[both copies get you thru Turnstile] = ?

- for each i, $\frac{1}{2}$ chance q_i (← true expected state of i^{th} qubit) was in $\{0,1\}$ $\Rightarrow \Pr[r_i = q_i] = 1 \Rightarrow$ Turnstile happy w/ prob. 1
- if $q_i \in \{\pm\}$... r_i equally likely $|0\rangle$ or $|1\rangle$...
  $\Pr[\text{turnstile measures } |r_i\rangle \text{ to be } |q_i\rangle] = 1/2$
  $\Rightarrow \Pr[\text{turnstile OK with both tokens' } i^{th} \text{ qubit}] = \frac{1}{4}$.

$$\frac{1}{2}\cdot 1 + \frac{1}{2}\cdot\frac{1}{4} = 5/8$$

Non-counterfeitability – continued

Actually, a smarter attack succeeds at duplicating w/ prob. $(3/4)^n$

(still safely unphysically small)

& this proven optimal by

Molina et al.,
Pastawski et al., 2011

(You'll prove this on homework!)

Aaronson '13: extended to show same bound for trying to make k+1 coins from k, $\forall k \geq 2$.

Wiesner '83: Claimed $(3/4)^n$ bound, but totally bogus reasoning…
unquestioned for 25 years…!

(Now for some criticisms...)

Defect 1: Verification requires sending state to Bank over quantum channel.

(Or walking it over to the bank...)

Gavinsky '11: A way to verify using just classical comm. with Bank.

(eavesdroppable!)

Molina et al. version:

- You text Bank "s"
- It texts back a random "challenge string" $c \in \{0,1\}^n$.
- You measure $|\psi_i\rangle$ in std basis if $c_i = 0$, sgn basis if $c_i = 1$.

  Text results to Bank

- Bank considers the $\approx 50\%$ of $i \in [n]$ where c_i matches the basis of (its known) q_i. Declares "verified!" if all your measurements "correct" on these i's.

(Won't formally discuss security, but you should think it looks plausible.)

Downside: This ruins the coin.

(Well, 3 things. (i) Gavinsky showed this can't be helped if you want classical verif.

(ii) At least Bank can give you IOU to be cashed in later.

(iii) As we'll see, it's not great to let user hang on to post-verified coins anyway.)

Remark: This is *very* similar to Bennett & Brassard's "Quantum Key Distribution", "BB84": A way to securely transmit one-time-pads.

[Actually so feasible in practice, several companies sell the service. Will be on homework!]

Defect 2: 3rd-party (Bank) verification.

Hypothetical "public-key Q. money": [Aaronson '09, Lutomirski et al. '10]

- Bank one time generates random...

  secret key & public key

  K_{sec} K_{pub}

  for $q = AES_{K_{sec}}(s)$

- Users can verify $(s, |\psi\rangle)$ via some

  $Verif(s, |\psi\rangle, K_{pub})$

(Several schemes suggested over the years, but almost all soon broken

One scheme by Farhi ... Shor ... et al., based on computational intractability of some quantum knot problem, still unbroken, but complicated & no great reason to believe it secure, So... it's a great open prob. to get secure-seeming public-key quantum money!)

Issue: What to do when...

	gets Bad coin	gets Good coin
Turnstile	Spit it out, don't let you pass?	Let you thru, eat the token.
Bank	Call the cops? (Perhaps too dramatic if wallets create noise. Maybe return coin if only a few qubits "wrong"?)	Say "OK" and give back the coin? Paranoia version: eat the coin, reissue a fresh one.

[Seems like a waste of resources? Actually, we'll see the Bank <u>must</u> do this!]

(Let's see why the Authority *must* do this, under the assumption that on *Bad* coins, they naively return the post-measurement bad coin... as a Turnstile might....)

If Bank hands rejected coin-states back to user..

You're a baddie, with $(s, |\psi\rangle)$.

How you can learn $|\psi_1\rangle$ (and $|\psi_2\rangle, \ldots, |\psi_{256}\rangle$):

(and hence know how to duplicate $|\psi\rangle$ limitlessly...)

- Trash first qubit of $|\psi\rangle$, replace it with $|0\rangle$ or $|1\rangle$ or $|+\rangle$ or $|-\rangle$
- Take to Bank, ask "Is this good?"
- Repeat 20...50 ($O(\log n)$) times

When you guessed right, Bank okays it.

" " " wrong, Bank rejects it with prob. $\geq \frac{1}{2}$.

(That's it. You learn $|\psi_1\rangle$ except with prob. $\ll \frac{1}{n}$ after $O(\log n)$ trials. Repeat for all n qubits in your coin!)

(Note: your trials always have just 1 bad qubit. "Wallet noise!" you could claim.)

Say Bank less naive: calls cops on Bad coin, gives back coin when verified as good.

Attack by Nagaj, Sattath, Brodutch, Unruh, ~3 years ago:

Given 1 legit coin, does $\approx n^2$ verifs, high prob. of no cops, & learns $|\psi\rangle$!

For each $i \in [n]$, has scheme doing C checks, prob. $\approx 1/C$ of cops being called, o/w, learns $|\psi_i\rangle$.

So set $C \gg n$, and repeat $\forall i \in [n]$.

1 qubit attack: unknown $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$

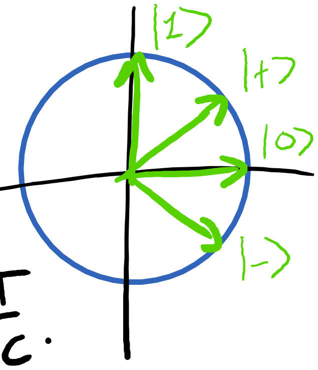
Want to slowly "learn" it, while evading an explosion of legal trouble.

Very similar situation to...

Elitzur-Vaidman Bomb!

Call unknown qubit $|u\rangle$.

(One of these 4:)



Let C be big int, let $\varepsilon = \frac{90°}{C} = \frac{\pi}{2C}$.

"Attach" a "control" qubit in state $|0\rangle$, so now $|0\rangle \otimes |u\rangle$.

Repeat C times:

- Rotate control qubit by ε (with 1-qubit unitary gate)
- CNOT (control onto target $|u\rangle$)
- Put 2nd qubit into coin, ask Bank to verify it. Get back post-measurement state.

(So control qubit is sneakily entangled with coin state)

(Analysis of 1st iteration of loop...)

Case 1: $|u\rangle = |+\rangle$. Bank will be measuring in sign-basis

$$|\varepsilon\nearrow\rangle \otimes |+\rangle = \underbrace{(\sim\sim\sim)\otimes\underbrace{\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)}_{\text{unchanged by NOT}}}_{\therefore \text{ unchanged by CNOT}}$$

$\to$ Bank gets 2nd qubit, measures in $|\pm\rangle$, gets $|+\rangle$ w. prob. 1, returns $|+\rangle$.

$\therefore$ after $C = \frac{90°}{\varepsilon}$ repetitions, state becomes $|1\rangle\otimes|+\rangle$

Case 2: $|u\rangle = |0\rangle$. Bank measuring in std. basis.

$$|0\rangle\otimes|u\rangle \longmapsto (\cos\varepsilon|0\rangle + \sin\varepsilon|1\rangle)\otimes|0\rangle$$

$$\xmapsto{\text{CNOT}} \cos\varepsilon\,|00\rangle + \sin\varepsilon\,|11\rangle$$

Bank measures $\to \begin{cases} |00\rangle \text{ w.p. } (\cos\varepsilon)^2 \\ |11\rangle\text{, cops called w.p. } (\sin\varepsilon)^2 \le \varepsilon^2. \end{cases}$ ☺

After $C = \frac{\pi}{2\varepsilon}$ reps: $\Pr[\text{cops}] \le \frac{\pi}{2}\varepsilon$,

& otherwise state ends up $|00\rangle$.

Case 3: $|u\rangle = |1\rangle$, Bank measures in std. basis

(Essentially same as $|u\rangle = |0\rangle$ case.)

$\xmapsto{\text{CNOT}} \cos\varepsilon|01\rangle + \sin\varepsilon|10\rangle$

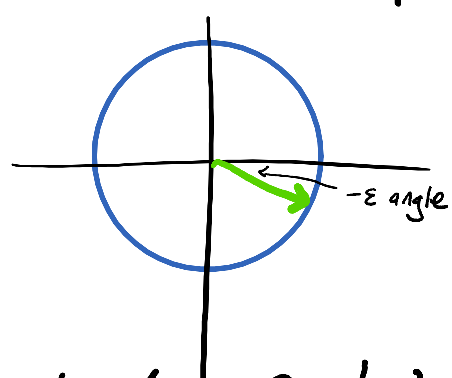
$\mapsto \Pr[\text{cops}] = (\sin\varepsilon)^2$, else collapses back to $|01\rangle$

Case 4: $|u\rangle = |-\rangle$, Bank measuring in sign basis.

$\xmapsto{\text{Rot}_\varepsilon} (\cos\varepsilon|0\rangle + \sin\varepsilon|1\rangle) \otimes |-\rangle$

$\xmapsto{\text{CNOT}} \cos\varepsilon|0,-\rangle - \sin\varepsilon|1,-\rangle$ (because $\text{NOT}|-\rangle = -|-\rangle$)

$= \underbrace{(\cos\varepsilon|0\rangle - \sin\varepsilon|1\rangle)}\otimes|-\rangle$



So Bank gets $|-\rangle$ and passes it back with prob. 1. Control qubit moves to angle $-\varepsilon$.

On next rep., control qubit rotated to angle 0. $\to |0\rangle\otimes|-\rangle$. CNOT does nothing. Bank OK's $|-\rangle$.

$\therefore$ reps cycle control qubit back & forth, angle $0, -\varepsilon$

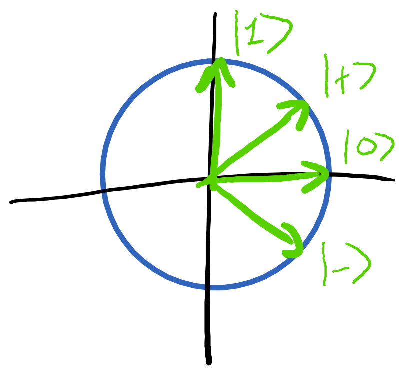
$\Pr[\text{no cops}] = 1$, final state $|0\rangle\otimes|-\rangle$ assuming C even.

Summary: • $\Pr[\text{cops}] \le \frac{\pi}{2}\varepsilon$ always.

• If $|u\rangle = |+\rangle$, control qubit ends at $|1\rangle$

• If $|u\rangle \ne |+\rangle$, ~ ~ ~ $|0\rangle$.

$\therefore$ at end, measuring in std. basis reveals "yes/no: is $|u\rangle = |+\rangle$?"



By appropriate rotations of scheme, can answer "yes/no: is $|u\rangle = |p\rangle$" for $p \in \{0,1,-\}$.

$\Pr[\text{cops}] \le 4 \cdot \frac{\pi}{2}\varepsilon = 2\pi\varepsilon$.

Repeat for all n qubits in $|\psi\rangle \rightarrow$ learn $|\psi\rangle$ (and can now counterfeit).

$$\Pr[\text{cops}] \le n \cdot 2\pi\varepsilon = \frac{\pi^2 n}{C} \le \frac{10n}{C},$$

$4Cn$ total verifs. Can take, say $C = 1000n$.
($n = 256 \Rightarrow$ invest 1 million trial verifs for 99% chance of being able to make free money!)

Conclusion: Bank should reissue coin, even on successful verification!