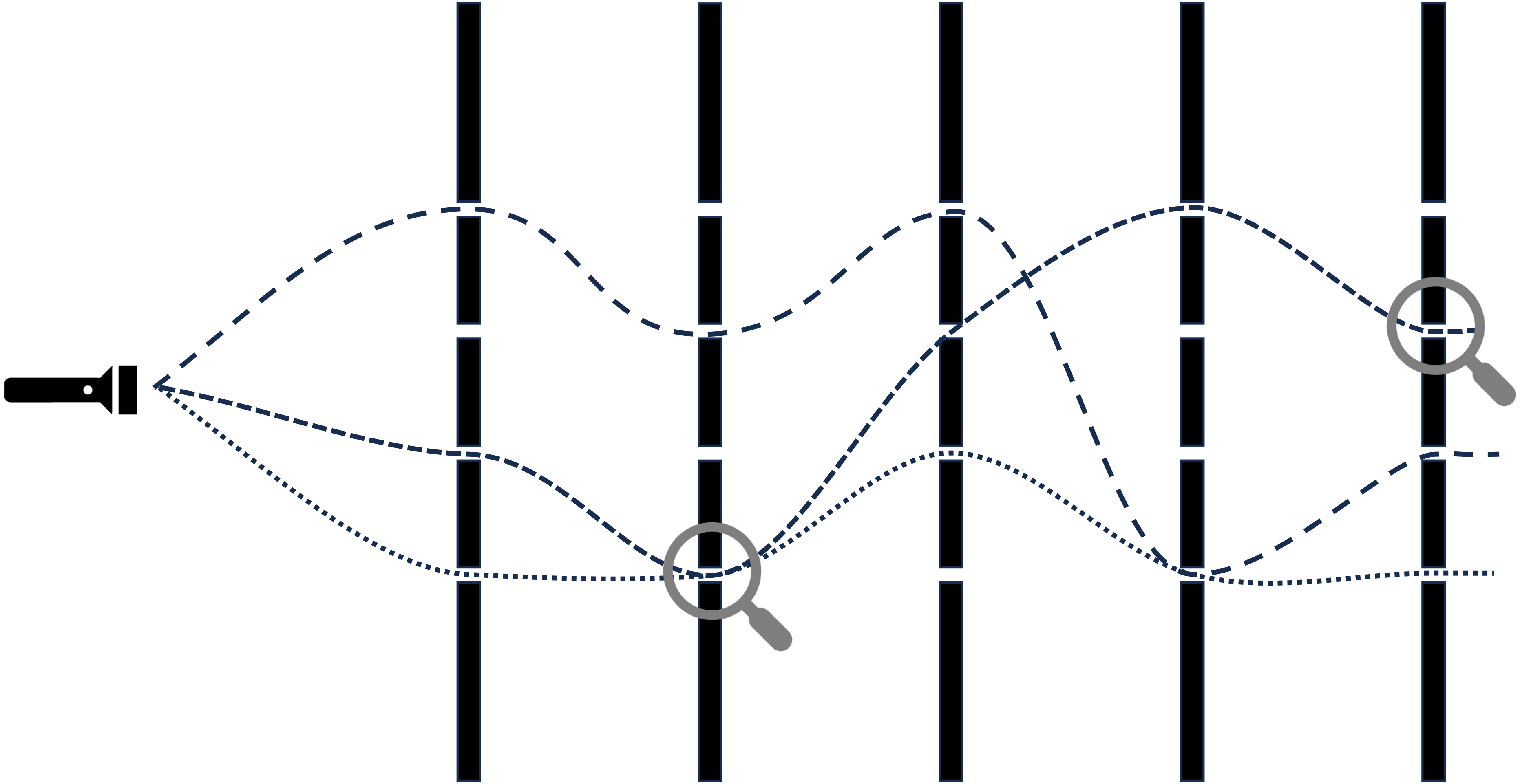
CS 258: Quantum Cryptography

Mark Zhandry

Previously…



What happens if we look at the particle in two places?

The observer effect

Looking at photon inherently changes its final state

Choose random $b, c \leftarrow \{0, 1\}$

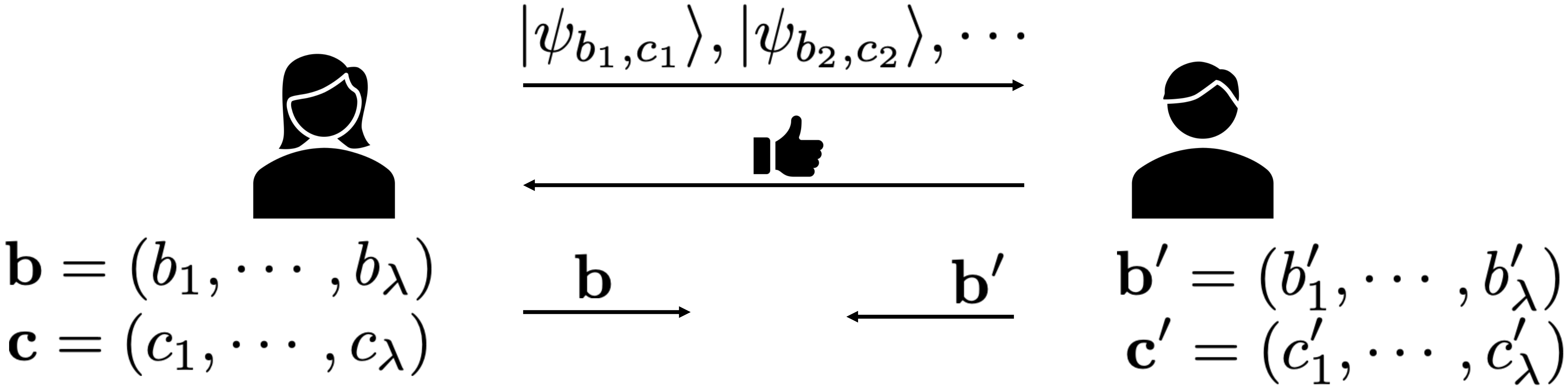
$$|\psi_{b,c}\rangle = \mathbf{H}^b|c\rangle = \begin{cases} |0\rangle & \text{if } b = c = 0 \\ |1\rangle & \text{if } b = 0, c = 1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if } b = 1, c = 0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if } b = c = 1 \end{cases}$$

$$|+\rangle$$

$$|-\rangle$$

Recall:

$$\mathbf{H} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$



$$|\psi_{b_1,c_1}\rangle, |\psi_{b_2,c_2}\rangle, \cdots$$

👍

$$\mathbf{b} = (b_1, \cdots, b_\lambda)$$

$$\mathbf{c} = (c_1, \cdots, c_\lambda)$$

$$\mathbf{b}$$

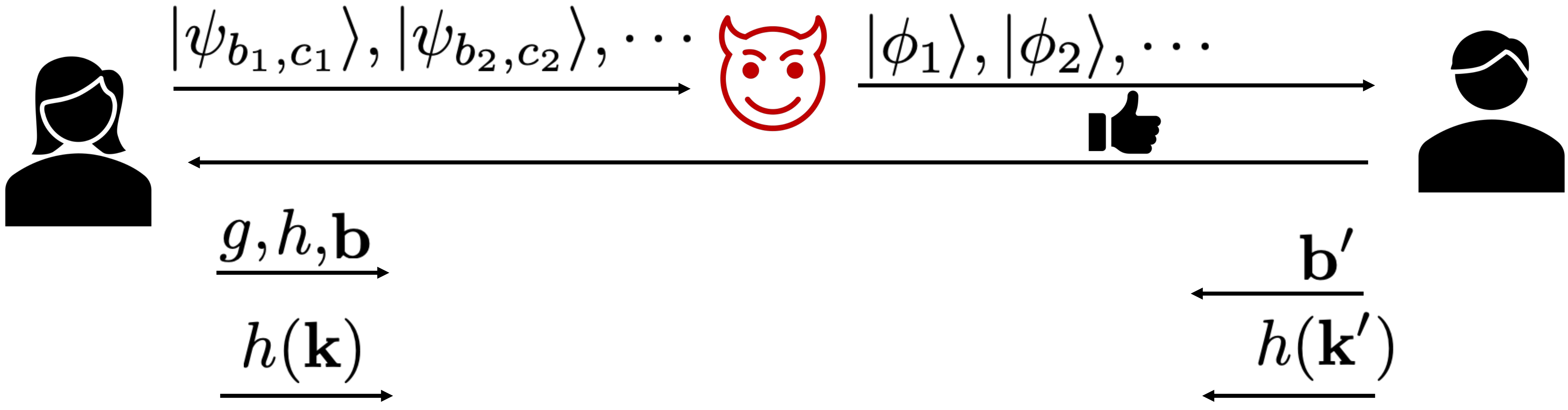
$$\mathbf{b}'$$

$$\mathbf{b}' = (b'_1, \cdots, b'_\lambda)$$

$$\mathbf{c}' = (c'_1, \cdots, c'_\lambda)$$

$$\mathbf{k} = (c_i)_{i:b_i=b'_i} = (c'_i)_{i:b_i=b'_i}$$

Expected key length = $\lambda/2$



$|\psi_{b_1,c_1}\rangle, |\psi_{b_2,c_2}\rangle, \cdots$

$|\phi_1\rangle, |\phi_2\rangle, \cdots$

👍

$g, h, \mathbf{b}$

$h(\mathbf{k})$

$\mathbf{b}'$

$h(\mathbf{k}')$

Check if $h(\mathbf{k}) = h(\mathbf{k}')$

Check if $h(\mathbf{k}) = h(\mathbf{k}')$

Actual shared key is $g(\mathbf{k}) = g(\mathbf{k}')$

QKD’s main promise is security against computationally unbounded attackers and without computational assumptions. However, it is unclear whether it will be “worth it”.

Today: Composite systems, No-cloning and Quantum Money

Composite systems

Suppose we had two states

$$|\psi\rangle = \sum_i \alpha_i |i\rangle \qquad\qquad |\phi\rangle = \sum_j \beta_j |j\rangle$$

The two together also form a quantum state on a larger system

$$|\psi\rangle \otimes |\phi\rangle = \sum_{i,j} \alpha_i \beta_j |i, j\rangle$$

Also write as $|\psi\rangle|\phi\rangle$

$\{|i, j\rangle\}_{i,j}$ is computational basis for composite system

$$\begin{tikzcd}
|\psi\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \end{pmatrix} \arrow[dr] & & |\phi\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \end{pmatrix} \arrow[dl] \\
& |\psi\rangle|\phi\rangle = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \vdots \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \\ \vdots \end{pmatrix} &
\end{tikzcd}$$

Composite systems

Often convenient to name systems

$|\psi\rangle_{\mathcal{A}}$ $|\phi\rangle_{\mathcal{B}}$

System $\mathcal{A}$ is in state $|\psi\rangle$ System $\mathcal{B}$ is in state $|\phi\rangle$

$|\zeta\rangle_{\mathcal{AB}}$

Joint system $\mathcal{AB}$ is in state $|\zeta\rangle$

Entanglement

$$|\zeta\rangle_{\mathcal{AB}} = \sum_{i,j} \gamma_{i,j} |i\rangle_{\mathcal{A}} |j\rangle_{\mathcal{B}}$$

Separable states: $|\zeta\rangle_{\mathcal{AB}} = |\psi\rangle_{\mathcal{A}} |\phi\rangle_{\mathcal{B}}$

Most states are **not** separable. In such case, we say $\mathcal{A}, \mathcal{B}$ are **entangled**

Entanglement

Example: EPR pairs

$$|\mathsf{EPR}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Operating on Composite Systems

Suppose we have two unitary operations

$$U_{\mathcal{A}} \qquad\qquad V_{\mathcal{B}}$$

This gives a new unitary on system $\mathcal{AB}$

$$(U \otimes V)_{\mathcal{AB}}$$

$$(U \otimes V)_{(i,j),(i',j')} = U_{i,i'} V_{j,j'}$$

Operating on Composite Systems

$$(U \otimes V)(|\psi\rangle \otimes |\phi\rangle) = (U|\psi\rangle) \otimes (V|\phi\rangle)$$

Partial Measurements

$$|\zeta\rangle_{\mathcal{AB}} = \sum_{i,j} \gamma_{i,j} |i\rangle_{\mathcal{A}} |j\rangle_{\mathcal{B}}$$

Can measure subsystem $\mathcal{A}$ ➡ Obtain i with probability $\displaystyle\sum_j |\gamma_{i,j}|^2$

State collapses to

$$|i\rangle_{\mathcal{A}} \sum_j \frac{\gamma_{i,j}}{\sqrt{\sum_{j'} |\gamma_{i,j'}|^2}} |j\rangle_{\mathcal{B}}$$

Intuition: pick out all terms consistent with measurement, re-normalize

Partial Measurements

$$|\mathsf{EPR}\rangle_{\mathcal{AB}} = \frac{1}{\sqrt{2}}|0,0\rangle_{\mathcal{AB}} + \frac{1}{\sqrt{2}}|1,1\rangle_{\mathcal{AB}}$$

⬇ measure $\mathcal{A}$

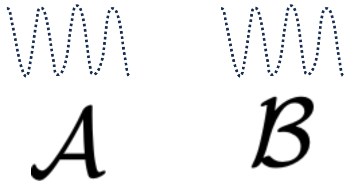
Measurement outcome b

State collapses to $|b,b\rangle$

⬇ measure $\mathcal{B}$

Measurement outcome b

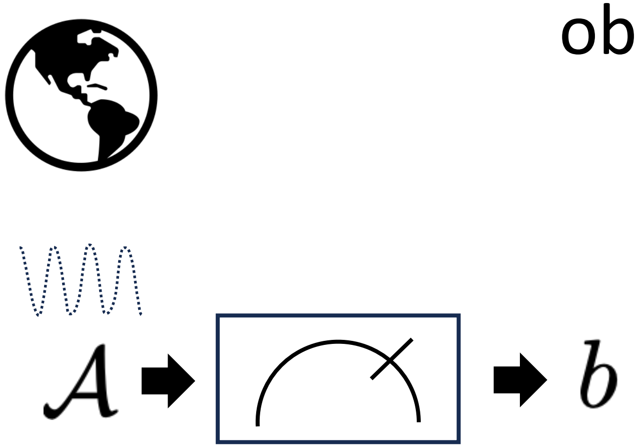
Non-locality of quantum mechanics

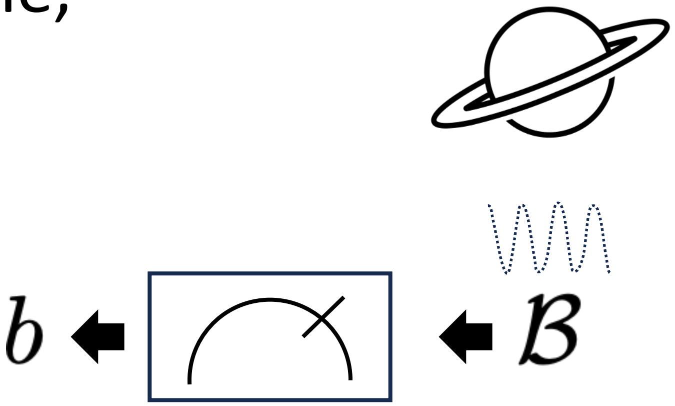


Joint state $|\mathsf{EPR}\rangle_{\mathcal{AB}} = \frac{1}{\sqrt{2}}|0,0\rangle_{\mathcal{AB}} + \frac{1}{\sqrt{2}}|1,1\rangle_{\mathcal{AB}}$

Non-locality of quantum mechanics

Somehow both systems simultaneously obtained same measurement outcome, despite being arbitrarily far apart





$$|\mathsf{EPR}\rangle_{\mathcal{AB}} = \frac{1}{\sqrt{2}}|0,0\rangle_{\mathcal{AB}} + \frac{1}{\sqrt{2}}|1,1\rangle_{\mathcal{AB}}$$

Notes

Non-locality may seem to violate speed cosmic speed limit

- Actually, despite simultaneously agreeing on measurement outcome, can’t actually be used to send info

Non-locality was rejected by some (including, famously, Einstein), and lead to the search for “local hidden variable theories” to explain quantum mechanics without non-locality

- Such theories can explain EPR paradox, but
- Such theories cannot explain other setups (Bell tests) which have been confirmed experimentally

Quantum No-Cloning

Cloner: unitary U such that

$$U|\psi\rangle = |\psi\rangle|\psi\rangle \text{ for any } |\psi\rangle$$

Technically not possible since unitaries have same input/output space

Cloner: unitary U such that

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \text{ for any } |\psi\rangle$$

Actually, we are also ok if cloner produces side-information

Cloner: unitary U such that

$$U|\psi\rangle|0\rangle|0\rangle = |\psi\rangle|\psi\rangle|\tau_\psi\rangle \quad \text{for any} \quad |\psi\rangle$$

$|\tau_\psi\rangle$ is arbitrary state

No-cloning Thm: For dimension >1, there is no cloner

Proof:

$$\begin{aligned}\langle\phi|\psi\rangle &= \langle\phi|\psi\rangle\langle 0|0\rangle\langle 0|0\rangle\\ &= (\langle\phi|\langle 0|\langle 0|)(|\psi\rangle|0\rangle|0\rangle)\\ &= (\langle\phi|\langle 0|\langle 0|)U^\dagger U(|\psi\rangle|0\rangle|0\rangle)\\ &= (\langle\phi|\langle\phi|\langle\tau_\phi|)(|\psi\rangle|\psi\rangle|\tau_\psi\rangle)\\ &= (\langle\phi|\psi\rangle)^2\langle\tau_\phi|\tau_\psi\rangle\end{aligned}$$

➡ $|\langle\phi|\psi\rangle| = |\langle\phi|\psi\rangle|^2|\langle\tau_\phi|\tau_\psi\rangle| \leq |\langle\phi|\psi\rangle|^2$

➡ $|\langle\phi|\psi\rangle| \in \{0,1\}$, false in general, e.g. $\langle +|0\rangle = \dfrac{1}{\sqrt{2}}$

The no-cloning theorem as described only talks about **perfect** cloning, but possible to extend to **imperfect** cloning as well

No-cloning Thm for Statistical Mechanics: There is no process which takes one sample from an arbitrary distribution, and produces two iid samples from the same distribution

Key difference is that distributions in statistical mechanics is just modeling uncertainty, while states in quantum mechanics are actually physical

More to the point: you can test for a given state, while its impossible to test if a sample was generated from a given distribution

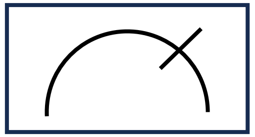
Testing for a quantum state

Let $|\psi\rangle$ be some quantum state

Let $U_\psi = \begin{pmatrix} \langle\psi| \\ \langle\phi_1| \\ \langle\phi_2| \\ \vdots \end{pmatrix}$ for orthogonal states $|\phi_i\rangle$ that are orthogonal to $|\psi\rangle$

Then U is unitary

Testing for a quantum state

$U_\psi|\phi\rangle$ ➡  ➡ 0 with probability $|\langle\phi|\psi\rangle|^2$

Always outputs 0 on $|\psi\rangle$

For “most” other states, will rarely output 0

Applying no-cloning to money

Classical “money”

Physical money

Can in principle copy with enough effort

Security derives from copying being presumably not cost-effective

Digital money

Trivial to “copy” 0’s and 1’s. Instead, security derives from verification against ledger of past transactions/balances

Promise of Quantum Money

Money made of quantum states that cannot be copied by the no-cloning theorem

Can be made “digital”, while also not needing any transaction ledger

For simplicity, let's assume just a single banknote in existence. These are called mini-schemes

Def: A quantum money mini-scheme is a pair $(\mathsf{Gen}, \mathsf{Ver})$ of quantum polynomial time* procedures such that:

- $\mathsf{Gen}(1^\lambda)$samples a classical "serial number" σ and money state $|\$\rangle$
- $\mathsf{Ver}(\sigma, |\$\rangle)$ outputs 1 (for accept) or zero (for reject)
- **Correctness:** for all λ,

$$\Pr[\mathsf{Ver}(\mathsf{Gen}(1^\lambda)) = 1] = 1$$

* We haven't actually defined quantum polynomial time yet, but it's not important for us yet

Defining Security

$\mathsf{Ver}^2(\sigma, |\$\$\rangle_{\mathcal{AB}})$: apply $\mathsf{Ver}(\sigma, \cdot)$ separately to both $\mathcal{A}$ and $\mathcal{B}$, accept if and only if both runs accept

Def: A quantum money mini-scheme $(\mathsf{Gen}, \mathsf{Ver})$ is *secret key secure* if, for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$\Pr[\mathsf{Ver}^2(\sigma,\ \mathcal{A}(|\$\rangle)\ ) = 1 : (\sigma, |\$\rangle) \leftarrow \mathsf{Gen}(1^\lambda)] \leq \epsilon(\lambda)$$

Notes:

The two money states produced by the adversary may be entangled

We allow the copied states to be potentially different from the initial state. The only important thing is that they pass verification

Wiesner's Quantum Money

$\mathsf{Gen}(1^\lambda)$:

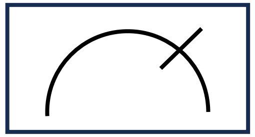
$$\left.\begin{array}{l}\mathbf{b} = (b_1, \cdots, b_\lambda) \\ \mathbf{c} = (c_1, \cdots, c_\lambda)\end{array}\right\} \sigma$$

$$|\$\rangle = \; |\psi_{b_1,c_1}\rangle, |\psi_{b_2,c_2}\rangle, \cdots$$

where $|\psi_{b,c}\rangle = \mathbf{H}^b|c\rangle$

Wiesner's Quantum Money

$\mathsf{Ver}(\sigma,\ |\phi_1\rangle|\phi_2\rangle\cdots) :$

$\mathbf{H}^{b_i}|\phi_i\rangle$ ➡  ➡ c_i'

Check that $c_i' = c_i$ for all i

Basically how Bob catches eavesdroppers in BB84

Thm: Wiesner’s quantum money mini-scheme is secret key secure

Intuition: if insecure, then can break BB84 QKD: adversary copies Alice’s state, and sends it to Bob without detection. Then when Alice reveals $\mathbf{b}$, adversary can measure her clones to learn $\mathbf{c}$, all without detection

A more careful analysis shows that best attack succeeds with probability $\left(\frac{3}{4}\right)^{\lambda}$

Some major limitations of Wiesner’s money scheme:

Storing quantum states for long periods of time is hard. Quantum states like to interact with their environment, which irreversibly alters them. This is bad for a money system!

The only way to verify a money state is to talk to the mint

The limitation of secret key quantum money

Verification requires serial number

But adversary can’t know serial number

Def: A quantum money mini-scheme $(\mathsf{Gen}, \mathsf{Ver})$ is *secret key secure* if, for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$\Pr[\mathsf{Ver}^2(\sigma,\ \mathcal{A}(|\$\rangle))\ ) = 1 : (\sigma, |\$\rangle) \leftarrow \mathsf{Gen}(1^\lambda)] \leq \epsilon(\lambda)$$

This means serial number must be kept secret, meaning the general public can’t verify. The only way to verify is to send to the mint

Public key quantum money

Def: A quantum money mini-scheme $(\mathsf{Gen}, \mathsf{Ver})$ is ***public*** *key secure* if, for all quantum polynomial-time adversaries $\mathcal{A}$, there exists a negligible function ϵ such that

$$\Pr[\mathsf{Ver}^2(\sigma,\ \mathcal{A}(\sigma, |\$\rangle)\ ) = 1 : (\sigma, |\$\rangle) \leftarrow \mathsf{Gen}(1^\lambda)] \leq \epsilon(\lambda)$$

Now that the adversary can see the serial number, it can be made public, meaning anyone can verify

It turns out that public key quantum money also can resolve the issue of preserving money states. By continuously running the verifier, it is possible to “correct” any alterations that happen to the state as it interacts with the environment.

Unfortunately, Wiesner’s quantum money scheme is not public key secure

The challenge with public key quantum money

It turns out that public key quantum money can be brute forced:

Repeat the following until success:

- Run $(\sigma', |\$'\rangle) \leftarrow \mathsf{Gen}(1^\lambda)$
- If $\sigma = \sigma'$, output $|\$'\rangle$

Note: For sk quantum money, no way to tell if your serial number is same as mint’s without destroying money state

The challenge with public key quantum money

Consequence: for public key quantum money, the no-cloning theorem actually doesn’t apply – states are information-theoretically clonable

No-cloning Thm: For dimension >1, there is no cloner

Proof: $\langle\phi|\psi\rangle$

Requires two possible non-orthogonal states. However, in public key quantum money, conditioned on seeing the serial number, there may only be one possible state. If there is only one possible state, no-cloning theorem doesn't apply

➡ $|\langle\phi|\psi\rangle| = |\langle\phi \quad |\langle\tau_\phi|\tau_\psi\rangle| \leq |\langle\phi|\psi\rangle|^2$

➡ $|\langle\phi|\psi\rangle| \in \{0,1\}$, false in general, e.g. $\langle+|0\rangle = \frac{1}{\sqrt{2}}$

The challenge with public key quantum money

As a result, we need security against bounded adversaries, and therefore also computational assumptions

But in addition, it is unclear a priori if we should even expect public key quantum money to be possible at all. We will revisit this question later in the course once we’ve developed more tools. There is currently no fully satisfying answer to this question, but there has been some good progress.

Next time: quantum computing!