You can't copy your friend's answers on a quantum test!

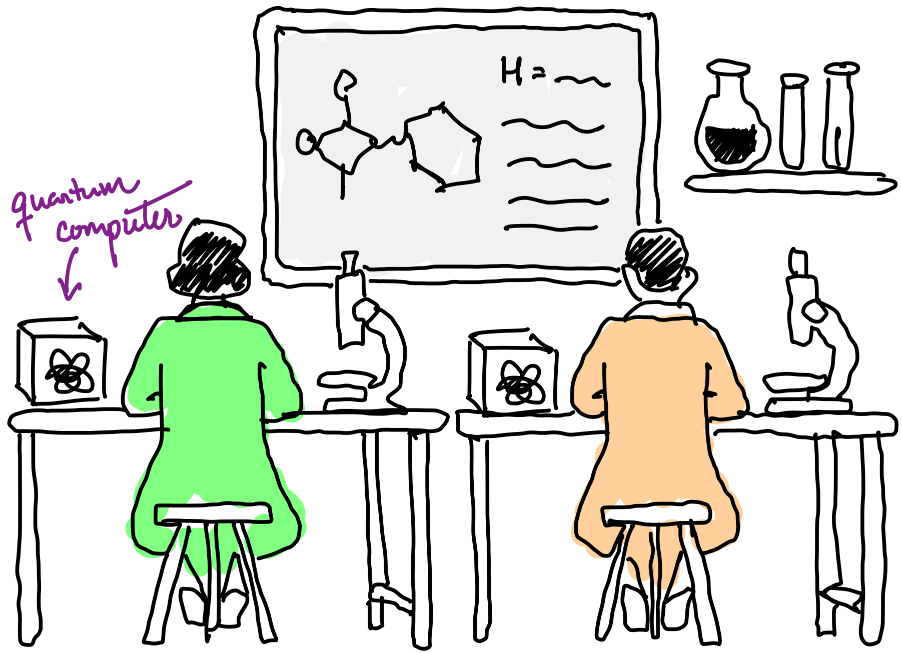
Chinmay Nirkhe

University of Washington

Based on a joint work with Vojtěch Havlíček

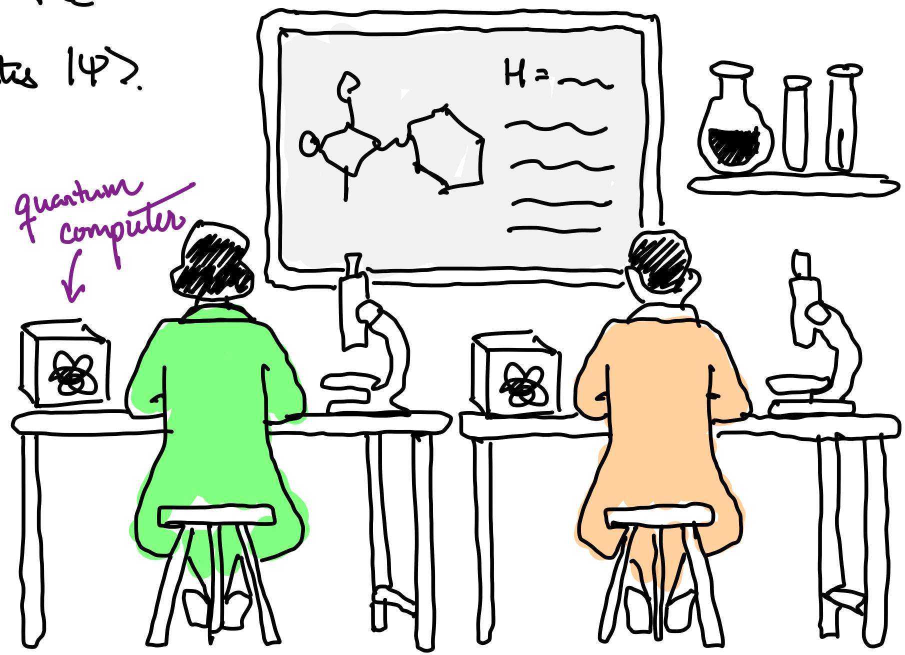
Picture an exam where the task is to create a quantum state $|\psi\rangle$ such that $|\psi\rangle$ is a groundstate of a local Hamiltonian H.

Picture an exam where the task is to create a quantum state $|\psi\rangle$ such that $|\psi\rangle$ is a groundstate of a local Hamiltonian H.



Picture an exam where the task is to create a quantum state $|\psi\rangle$ such that $|\psi\rangle$ is a groundstate of a local Hamiltonian H.

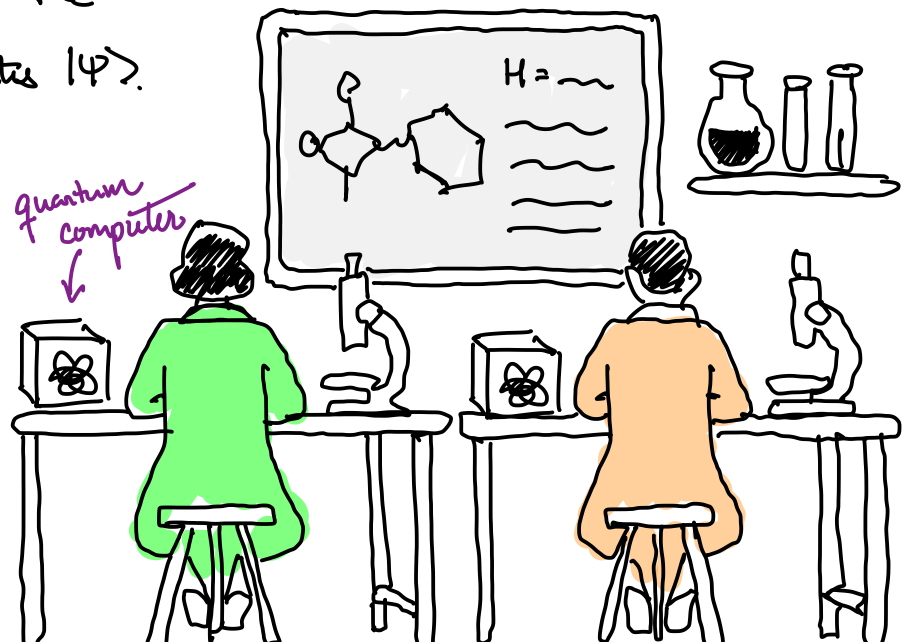
Alice knows how to solve the problem and quickly generates $|\psi\rangle$.



Picture an exam where the task is to create a quantum state $|\psi\rangle$ such that $|\psi\rangle$ is a groundstate of a local Hamiltonian H.

Alice knows how to solve the problem and quickly generates $|\psi\rangle$.

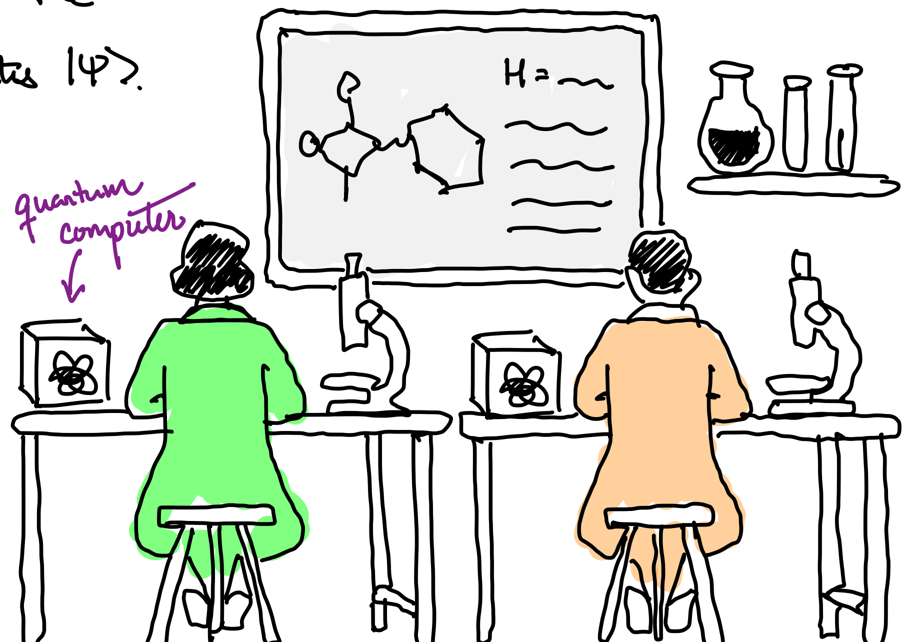
But, then she walks away and Bob tries to use the opportunity and copy $|\psi\rangle$.



Picture an exam where the task is to create a quantum state $|\psi\rangle$ such that $|\psi\rangle$ is a groundstate of a local Hamiltonian H.

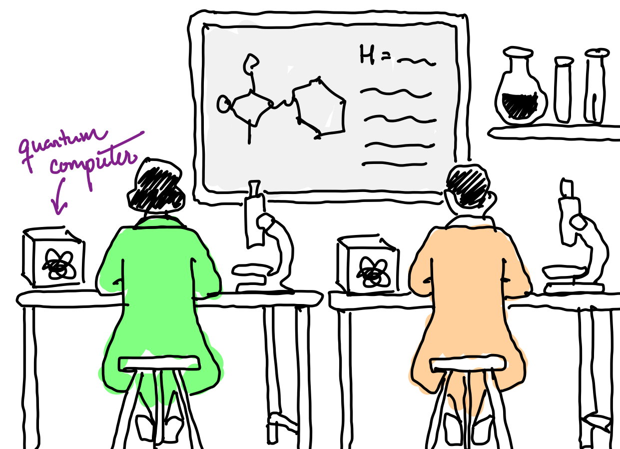
Alice knows how to solve the problem and quickly generates $|\psi\rangle$.

But, then she walks away and Bob tries to use the opportunity and copy $|\psi\rangle$.



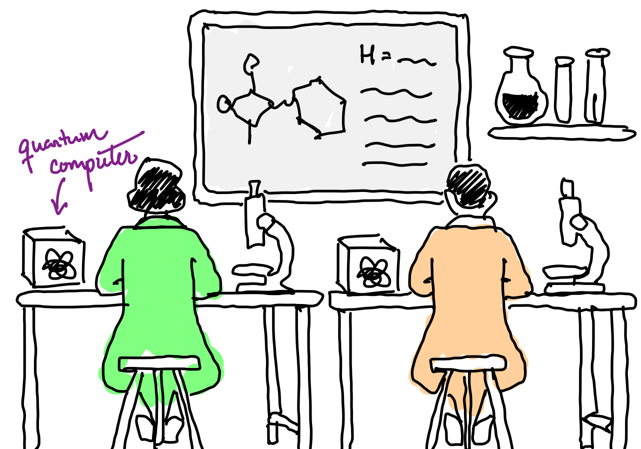
Can he?

Caveats :



Caveats:

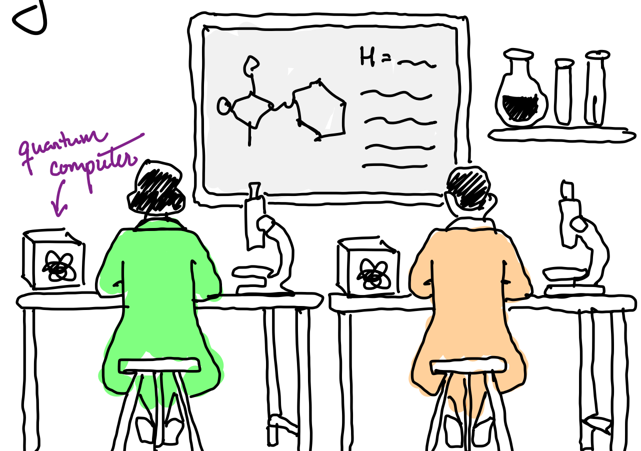
① Bob's cheating must be efficient. He can't spend too long using $|\psi\rangle_{Alice}$. He can use the q. computer.



Caveats:

1. Bob's cheating must be efficient. He can't spend too long using $|\psi\rangle_{Alice}$. He can use the q. computer.

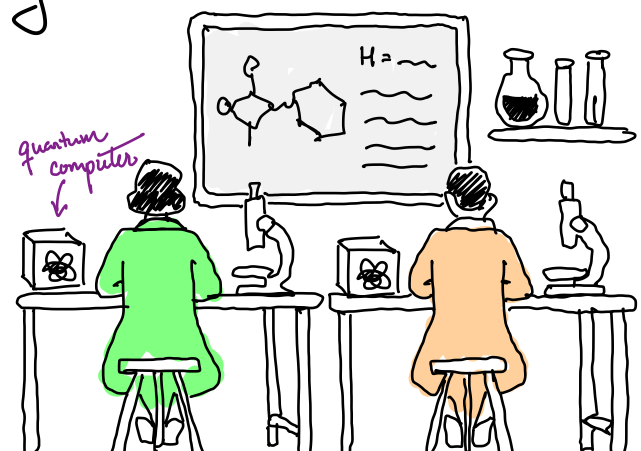
2. Alice shouldn't detect any tampering. Her state can change or become entangled with Bob's, but the reduced state of Alice must still be a groundstate of H.



Caveats:

1. Bob's cheating must be efficient. He can't spend too long using $|\psi\rangle_{Alice}$. He can use the q. computer.

2. Alice shouldn't detect any tampering. Her state can change or become entangled with Bob's, but the reduced state of Alice must still be a groundstate of H.



3. Bob's solution must also be a groundstate.

A first answer might trivially be <u>NO</u>.

A first answer might trivially be NO.

Why? The no-cloning theorem.

A first answer might trivially be NO.

Why? The no-cloning theorem.

No cloning theorem:

There is no quantum transformation mapping $|\psi\rangle|0\ldots0\rangle \mapsto |\psi\rangle|\psi\rangle$

for all $|\psi\rangle$.

A first answer might trivially be NO.

Why? The no-cloning theorem.

No cloning theorem:

There is no quantum transformation mapping $|\psi\rangle|0\ldots0\rangle \mapsto |\psi\rangle|\psi\rangle$

for all $|\psi\rangle$. Only holds when

there is uncertainty about what $|\psi\rangle$ is.

A first answer might trivially be NO.

Why? The no-cloning theorem.

No cloning theorem:

There is no quantum transformation mapping $|\psi\rangle|0\ldots0\rangle \mapsto |\psi\rangle|\psi\rangle$ for all $|\psi\rangle$. Only holds when there is uncertainty about what $|\psi\rangle$ is.

If Bob knew nothing about the exam, he wouldn't be very good at cheating.

A first answer might trivially be NO.

Why? The no-cloning theorem.

No cloning theorem:

There is no quantum transformation mapping $|\psi\rangle|0\ldots0\rangle \mapsto |\psi\rangle|\psi\rangle$

for all $|\psi\rangle$. Only holds when there is uncertainty about what $|\psi\rangle$ is.

If Bob knew nothing about the exam, he wouldn't be very good at cheating.

Either Alice or the Examiner will detect the malfiesance.

But Bob has more information. In particular, he knows the exam question H.

But Bob has more information. In particular, he knows the exam question H.

This rules out information-theoretic arguments of impossibility such as the no-cloning theorem.

But Bob has more information. In particular, he knows the exam question H.

This rules out information-theoretic arguments of impossibility such as the no-cloning theorem.

Why? If H was an "easy" question, Bob could solve $|\psi\rangle$ from H without having to cheat off of Alice. In particular, he can always calculate $|\psi\rangle$ given H with enough time by "guessing and checking".

A notion of efficient copying

A notion of efficient copying

The Hamiltonian $H = \sum h_i$ consists of terms acting on k out of n qubits. (Think $k = 2$ or 3).

A notion of efficient copying

(time invariant)

The Hamiltonian $H = \sum h_i$ consists of terms acting on k out of n qubits. (Think $k = 2$ or 3).

A notion of efficient copying

(time invariant)

The Hamiltonian $H = \sum h_i$ consists of terms acting on k out of n qubits. (Think $k = 2$ or 3).

Each h_i is a $2^k \times 2^k$ Hermitian matrix.

A notion of efficient copying

(time invariant)

The Hamiltonian $H = \sum h_i$ consists of terms acting on k out of n qubits. (Think $k=2$ or 3).

Each h_i is a $2^k \times 2^k$ Hermitian matrix.

$|\psi\rangle$ is a groundstate if $\langle\psi|H|\psi\rangle = \lambda_{min}(H)$.

A notion of efficient copying

(time invariant)

The Hamiltonian $H = \sum h_i$ consists of terms acting on k out of n qubits. (Think $k = 2$ or 3).

Each h_i is a $2^k \times 2^k$ Hermitian matrix.

as a $2^n \times 2^n$ matrix.

$|\psi\rangle$ is a groundstate if $\langle \psi | H | \psi \rangle = \lambda_{min}(H)$.

A notion of efficient copying

(time invariant)

The Hamiltonian $H = \sum h_i$ consists of terms acting on k out of n qubits. (Think $k = 2$ or 3).

Each h_i is a $2^k \times 2^k$ Hermitian matrix.

as a $2^n \times 2^n$ matrix.

$|\psi\rangle$ is a groundstate if $\langle\psi|H|\psi\rangle = \lambda_{min}(H)$.

A copying algorithm is efficient if it takes n^c (polynomial time) on a quantum computer.

The Computational No-Cloning Conjecture

There is no general efficient algorithm mapping

$$(H, |\psi\rangle, |0\ldots0\rangle) \mapsto (H, |\psi\rangle, |\psi\rangle)$$

where H is a classical input, $|\psi\rangle$ a groundstate to H.

The Computational No-Cloning Conjecture

There is no general efficient algorithm mapping

$$(H, |\psi\rangle, |0\ldots0\rangle) \mapsto (H, |\psi\rangle, |\psi\rangle)$$

where H is a classical input, $|\psi\rangle$ a groundstate to H.

- efficient means runtime of n^c (polynomial time).

The Computational No-Cloning Conjecture

There is no general efficient algorithm mapping

$$(H, |\psi\rangle, |0\ldots0\rangle) \mapsto (H, |\psi\rangle, |\psi\rangle)$$

where H is a classical input, $|\psi\rangle$ a groundstate to H.

- efficient means runtime of n^c (polynomial time).
- there is also a formulation when H has a degenerate groundspace.

The Computational No-Cloning Conjecture

There is no general efficient algorithm mapping

$$(H, |\psi\rangle, |0\ldots0\rangle) \mapsto (H, |\psi\rangle, |\psi\rangle)$$

where H is a classical input, $|\psi\rangle$ a groundstate to H.

The Computational No-Cloning Conjecture

There is no general efficient algorithm mapping

$$(H, |\psi\rangle, |0\ldots0\rangle) \mapsto (H, |\psi\rangle, |\psi\rangle)$$

where H is a classical input, $|\psi\rangle$ a groundstate to H.

Why groundstates of Hamiltonians?

The Computational No-Cloning Conjecture

There is no general efficient algorithm mapping

$$(H, |\psi\rangle, |0\ldots0\rangle) \mapsto (H, |\psi\rangle, |\psi\rangle)$$

where H is a classical input, $|\psi\rangle$ a groundstate to H.

Why groundstates of Hamiltonians?

Because [Kitaev '99] proved that calculating groundenergy is complete for all efficiently verifiable q. computations (QMA).

Let's try to imagine a world where computational cloning is always easy.

Let's try to imagine a world where computational cloning is always easy.

- solutions to q. problems can easily be publically disseminated

Let's try to imagine a world where computational cloning is always easy.

- solutions to q. problems can easily be publically disseminated
- quantum copy-protection schemes can be broken

Let's try to imagine a world where computational cloning is always easy.

- solutions to q. problems can easily be publically disseminated
- quantum copy-protection schemes can be broken
- quantum money can easily be counterfeited.

Let's try to imagine a world where computational cloning is always easy.

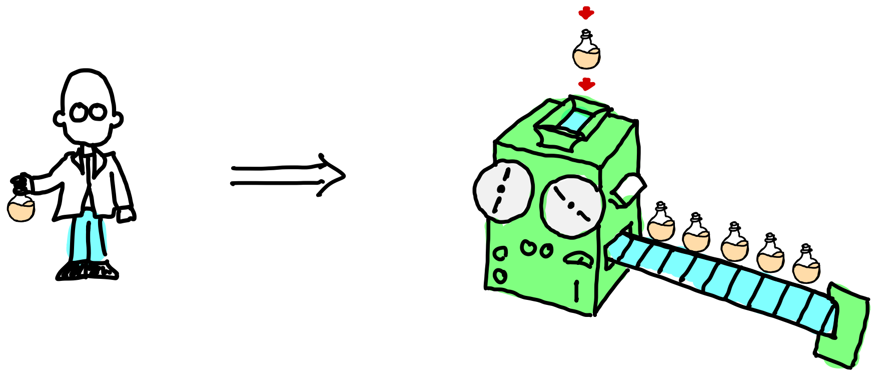
- solutions to q. problems can easily be publically disseminated
- quantum copy-protection schemes can be broken
- quantum money can easily be counterfeited.

let's take a deeper look at this.

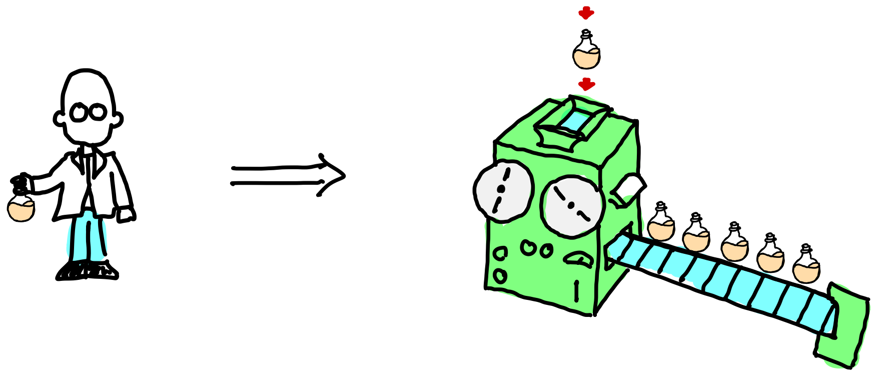
Almost all the complexity in creating multiple copies of the groundstate is captured in the first copy

Almost all the complexity in creating multiple copies of the groundstate is captured in the first copy

Almost all the complexity in creating multiple copies of the groundstate is captured in the first copy

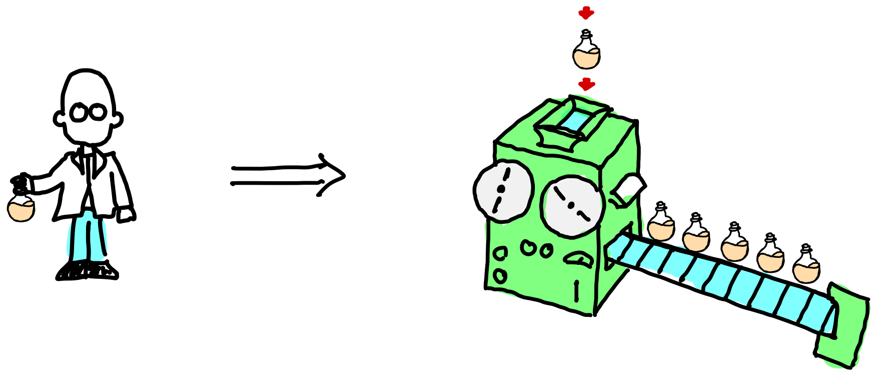


Almost all the complexity in creating multiple copies of the groundstate is captured in the first copy



Replication of quantum solutions is easy.

Almost all the complexity in creating multiple copies of the groundstate is captured in the first copy

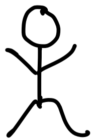


Replication of quantum solutions is easy.

With enough copies, we can calculate properties of the groundstate once we have the first copy.

(Public-key) quantum money

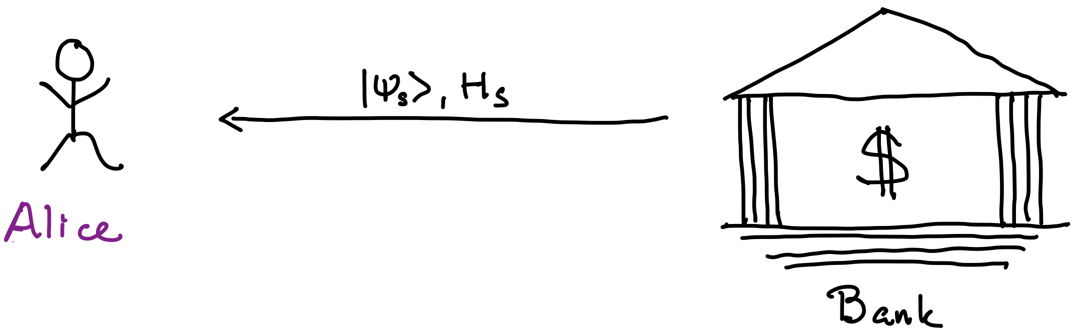
(Public-key) quantum money



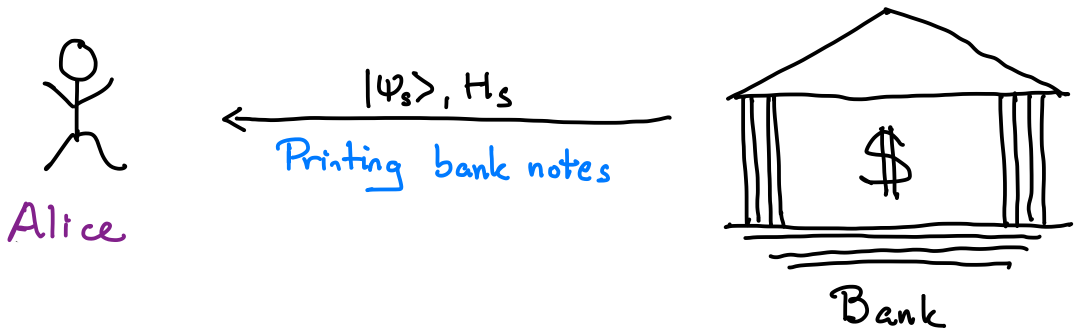
Alice

Bank

(Public-key) quantum money

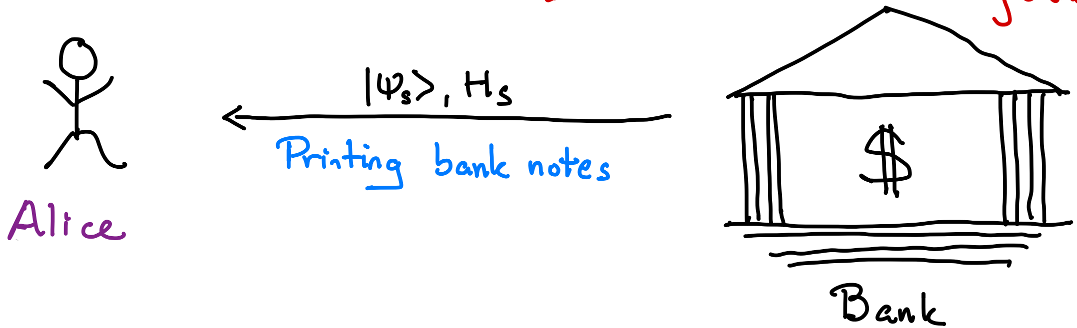


(Public-key) quantum money



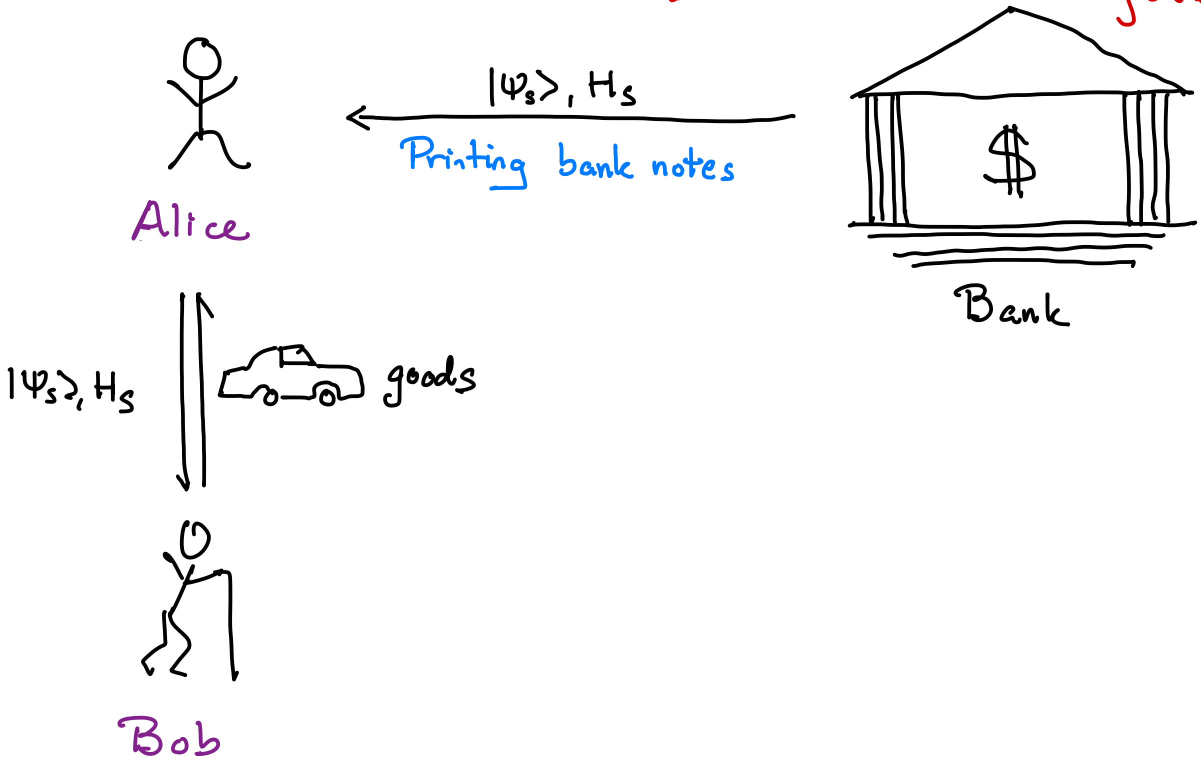
(Public-key) quantum money

Bank produces a note $|\psi_s\rangle$ and a Hamiltonian H_s s.t. $|\psi_s\rangle$ is a groundstate of H_s.



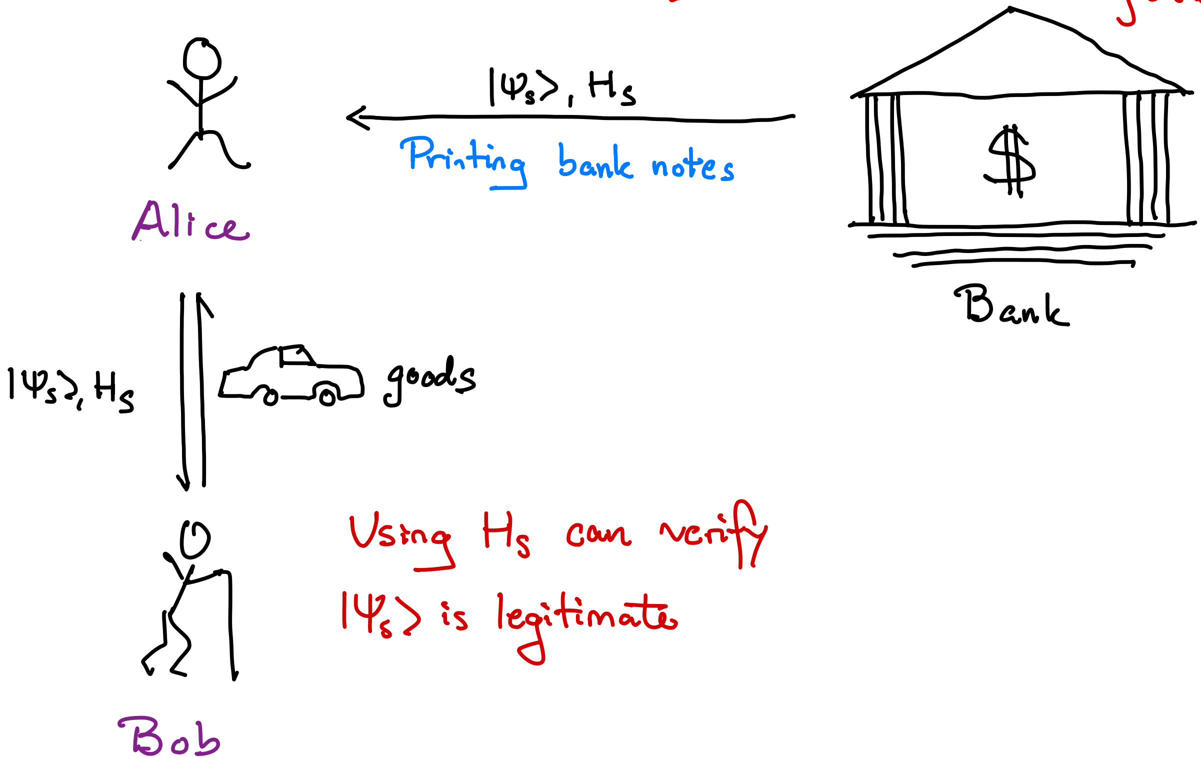
(Public-key) quantum money

Bank produces a note $|\psi_s\rangle$ and a Hamiltonian H_s s.t. $|\psi_s\rangle$ is a groundstate of H_s.



(Public-key) quantum money

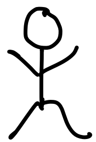
Bank produces a note $|\psi_s\rangle$ and a Hamiltonian H_s s.t. $|\psi_s\rangle$ is a groundstate of H_s.



Using H_s can verify $|\psi_s\rangle$ is legitimate

(Public-key) quantum money

Bank produces a note $|\psi_s\rangle$ and a Hamiltonian H_s s.t. $|\psi_s\rangle$ is a groundstate of H_s.



Alice

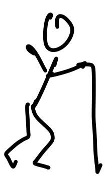
$|\psi_s\rangle, H_s$

Printing bank notes

Bank

$|\psi_s\rangle, H_s$

goods



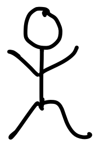
Bob

Using H_s can verify $|\psi_s\rangle$ is legitimate

Verifying bank notes

(Public-key) quantum money

Bank produces a note $|\psi_s\rangle$ and a Hamiltonian H_s s.t. $|\psi_s\rangle$ is a groundstate of H_s.



Alice

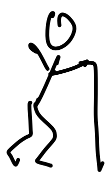
$|\psi_s\rangle, H_s$

Printing bank notes

Bank

$|\psi_s\rangle, H_s$

goods



Bob

Using H_s can verify $|\psi_s\rangle$ is legitimate

Verifying bank notes

Bob can verify the note without talking to the bank.

(Privacy)

(Public-key) quantum money

Security of the quantum money scheme.

(Public-key) quantum money

Security of the quantum money scheme.

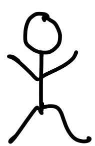
What is stopping Alice from copying the input $|\psi_s\rangle$, keeping one copy and paying Bob with the other?

(Public-key) quantum money

Security of the quantum money scheme.

What is stopping Alice from copying the input $|\psi_s\rangle$, keeping one copy and paying Bob with the other?

The Hardness of Cloning!



Alice

$$|\psi_s\rangle, H_s \longmapsto |\psi_s\rangle \otimes |\psi_s\rangle, H_s$$

must be hard for security.

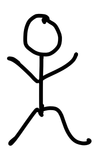
(Public-key) quantum money

Security of the quantum money scheme.

What is stopping Alice from copying the input $|\psi_s\rangle$, keeping one copy and paying Bob with the other?

The Hardness of Cloning!

Technically, need a notion of average-case hardness



Alice

$$|\psi_s\rangle, H_s \longmapsto |\psi_s\rangle \otimes |\psi_s\rangle, H_s$$

must be hard for security.

Our goal is to prove that no efficient algorithm exists for cloning groundstates.

Our goal is to prove that no efficient algorithm exists for cloning groundstates.

(resolve a major open question in q. information)

From a vague goal to an achievable mathematical theorem

From a vague goal to an achievable mathematical theorem

Proving outright a statement like "____ transformation takes exponential time" is super challenging. Akin to proving $P \neq NP$ in difficulty.

From a vague goal to an achievable mathematical theorem

Proving outright a statement like "___ transformation takes exponential time" is super challenging. Akin to proving $P \neq NP$ in difficulty.

Instead, we hope to prove something like if "cloning groundstates is efficient", then something mathematically unexpected must be true.

From a vague goal to an achievable mathematical theorem

Proving outright a statement like "___ transformation takes exponential time" is superchallenging. Akin to proving $P \neq NP$ in difficulty.

Instead, we hope to prove something like if "cloning groundstates is efficient", then something mathematically unexpected must be true.

In this case, the unexpected statement will be: $BQP \supseteq NP$.

From a vague goal to an achievable mathematical theorem

Proving outright a statement like "___ transformation takes exponential time" is super challenging. Akin to proving $P \neq NP$ in difficulty.

Instead, we hope to prove something like if "cloning groundstates is efficient", then something mathematically unexpected must be true.

In this case, the unexpected statement will be: $BQP \supseteq NP$.

i.e. quantum computers can efficiently solve NP problems.

From a vague goal to an achievable mathematical theorem

Proving outright a statement like "___ transformation takes exponential time" is super challenging. Akin to proving $P \neq NP$ in difficulty.

Instead, we hope to prove something like if "cloning groundstates is efficient", then something mathematically unexpected must be true.

In this case, the unexpected statement will be: $BQP \supseteq NP$.
i.e. quantum computers can efficiently solve NP problems.

Not expected to be true.

From a vague goal to an achievable mathematical theorem

From a vague goal to an achievable mathematical theorem

Goal: there is no algorithm for cloning groundstates unless BQP $\supseteq$ NP.

i.e. quantum computers can efficiently solve NP problems.

From a vague goal to an achievable mathematical theorem

Goal: there is no algorithm for cloning groundstates unless $BQP \supseteq NP$.

i.e. quantum computers can efficiently solve NP problems.

- a complexity-theoretic argument for the hardness of cloning

From a vague goal to an achievable mathematical theorem

Goal: there is no algorithm for cloning groundstates unless BQP ⊇ NP.

i.e. quantum computers can efficiently solve NP problems.

- a complexity-theoretic argument for the hardness of cloning

- some (non-state of the art) cryptographic arguments exist

From a vague goal to an achievable mathematical theorem

Goal: there is no algorithm for cloning groundstates unless BQP ⊇ NP.

i.e. quantum computers can efficiently solve NP problems.

- a complexity-theoretic argument for the hardness of cloning

- some (non-state of the art) cryptographic arguments exist
  - even prove average-case hardness

From a vague goal to an achievable mathematical theorem

Goal: there is no algorithm for cloning groundstates unless $BQP \supseteq NP$.

i.e. quantum computers can efficiently solve NP problems.

- a complexity-theoretic argument for the hardness of cloning

- some (non-state of the art) cryptographic arguments exist
  - even prove average-case hardness

complexity arguments $\gg$ cryptography arguments

What are the hardest states to clone?

What are the hardest states to clone?

Intuitively, identifying the hardest to clone states will make it easier to prove our desired statement.

What are the hardest states to clone?

Intuitively, identifying the hardest to clone states will make it easier to prove our desired statement.

> The maximally entangled state for a subspace.

What are the hardest states to clone?

Intuitively, identifying the hardest to clone states will make it easier to prove our desired statement.

The maximally entangled state for a subspace.

Let $\Pi \subseteq \mathbb{C}^{d_2}$ be a subspace defined by basis $|b_1\rangle, \dots, |b_{d_1}\rangle$.

The Π-maximally entangled state $\in \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ is the state

$$|\Phi_\Pi\rangle := \frac{1}{\sqrt{d_1}} \sum_{i=1}^{d_1} |b_i\rangle \otimes |b_i^*\rangle.$$

What are the hardest states to clone?

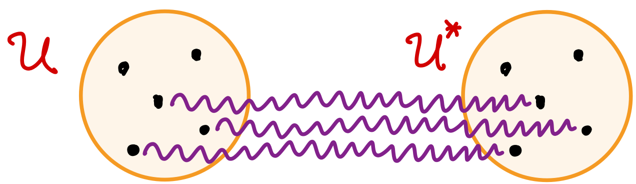
The Π-maximally entangled state $\in \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ is the state

$$|\Phi_\Pi\rangle := \frac{1}{\sqrt{d_1}} \sum_{i=1}^{d_1} |b_i\rangle \otimes |b_i^*\rangle .$$

What are the hardest states to clone?

The Π-maximally entangled state $\in \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ is the state

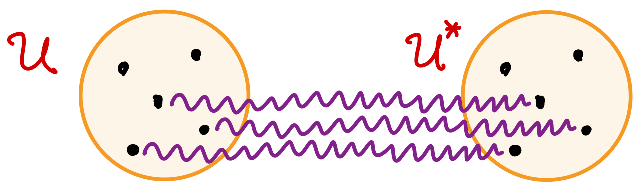
$$|\Phi_\Pi\rangle := \frac{1}{\sqrt{d_1}} \sum_{i=1}^{d_1} |b_i\rangle \otimes |b_i^*\rangle .$$



What are the hardest states to clone?

The Π-maximally entangled state $\in \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ is the state

$$|\Phi_\Pi\rangle := \frac{1}{\sqrt{d_1}} \sum_{i=1}^{d_1} |b_i\rangle \otimes |b_i^*\rangle.$$

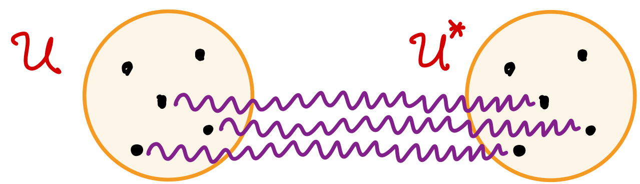


- generalizes EPR states to states over hidden subspaces.

What are the hardest states to clone?

The Π-maximally entangled state $\in \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ is the state

$$|\Phi_\Pi\rangle := \frac{1}{\sqrt{d_1}} \sum_{i=1}^{d_1} |b_i\rangle \otimes |b_i^*\rangle.$$

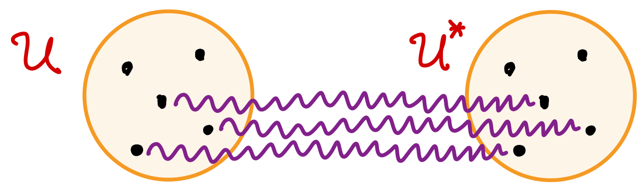


- generalizes EPR states to states over hidden subspaces.
- cloning such a state requires first unentangling the two systems which requires knowing how to map $\mathcal{U}: \mathbb{C}^{d_1} \hookrightarrow \Pi$.

What are the hardest states to clone?

The Π-maximally entangled state $\in \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_2}$ is the state

$$|\Phi_\Pi\rangle := \frac{1}{\sqrt{d_1}} \sum_{i=1}^{d_1} |b_i\rangle \otimes |b_i^*\rangle .$$



- generalizes EPR states to states over hidden subspaces.
- cloning such a state requires <u>first</u> unentangling the two systems which requires knowing how to map $\mathcal{U} : \mathbb{C}^{d_1} \hookrightarrow \Pi$.

↑ intuition only!

Making intuitions formal

Conjecture:

Making intuitions formal

Conjecture:

① Let V be an efficient quantum algorithm that accepts states in Π.

Making intuitions formal

Conjecture:

① Let V be an efficient quantum algorithm that accepts states in Π.

② If $\exists$ an algorithm W

$$|\langle V\rangle\rangle|\Phi_\pi\rangle|0\rangle \mapsto |\langle V\rangle\rangle|\Phi_\pi\rangle|\Phi_\pi\rangle$$

hen there exists another algorithm W' capable of generating states in Π.

Making intuitions formal

Conjecture:

1. Let $\mathcal{V}$ be an efficient quantum algorithm that accepts states in Π.
2. If $\exists$ an algorithm $\mathcal{W}$

$$|\langle \mathcal{V}\rangle\rangle|\Phi_\pi\rangle|0\rangle \mapsto |\langle \mathcal{V}\rangle\rangle|\Phi_\pi\rangle|\Phi_\pi\rangle$$

hen there exists another algorithm $\mathcal{W}'$ capable of generating states in Π.

Captures the intuition from the previous slide.

But this chain of thinking ignores something crucial

But this chain of thinking ignores something crucial

Are states like $|\Phi_{\pi}\rangle$ even groundstates of Hamiltonians?

But this chain of thinking ignores something crucial

Are states like $|\Phi_\pi\rangle$ even groundstates of Hamiltonians?

recall we wanted to consider physically relevant states.

But this chain of thinking ignores something crucial

Are states like $|\Phi_\Pi\rangle$ even groundstates of Hamiltonians?

recall we wanted to consider physically relevant states.

Main contribution [Havlíček - Nirkhe '24]:

A construction of NP-hard subspaces Π such that

$\exists$ a Hamiltonian H with groundstate $|\Phi_\Pi\rangle$.

The technical details

The technical details

Constructing H relies on a powerful tool in q. algorithms and complexity theory:

non-abelian quantum fourier transform

The technical details

Constructing H relies on a powerful tool in q. algorithms and complexity theory:

non-abelian quantum Fourier transform

Specifically, there is a NP-hard problem about representation of the symmetric group S_n and the multiplicity of its irreducible representations

which can be encoded in Π, H.

What's next?

What's next?

- Elephant in the room: prove the conjecture previously stated

What's next?

- Elephant in the room: prove the conjecture previously stated
- Discover other states which are hard to clone and find corresponding Hamiltonians

What's next?

- Elephant in the room: prove the conjecture previously stated
- Discover other states which are hard to clone and find corresponding Hamiltonians
- Prove hardness of cloning from state of the art assumptions like the learning with errors problem

What's next?

- Elephant in the room: prove the conjecture previously stated
- Discover other states which are hard to clone and find corresponding Hamiltonians
- Prove hardness of cloning from state of the art assumptions like the learning with errors problem

This work is definitively unfinished, but that's what makes it so tantalizing and exciting!