From the Hardness of Detecting Superpositions to Cryptography:

Quantum Public Key Encryption and Commitments

Minki Hhan (KIAS)

QCrypt 2023

based on the joint work with Tomoyuki Morimae (Kyoto Univ.)
Takashi Yamakawa (NTT & Kyoto Univ.)

Contribution of [HMY'23]

1. New *quantum* search-to-decision reduction
   - Based on a recent work of Aaronson, Atia, Susskind
   - Simple & Interesting properties: Locality preserving, with (quantum) advice
   - Similar ideas implicitly appeared in previous works (quantum Goldreich-Levin, …)

Original motivation was from quantum gravity

Open problem in [JQSY19]

2. Applications to Quantum Cryptography
   - New public key encryption based on non-abelian group action
   - Efficient flavor conversion of quantum bit commitments
     previous: $O(\lambda^2)$-multiplicative factor [CLS01,Yan22]
     ours: $O(1)$-additive factor

Concurrent work [GJMZ23]

Contribution of [HMY'23]

1. New *quantum* search-to-decision reduction
   - Based on a recent work of Aaronson, Atia, Susskind
   - Simple & Interesting properties: Locality preserving, with (quantum) advice
   - Similar ideas implicitly appeared in previous works (quantum Goldreich-Levin, …)

Original motivation was from quantum gravity

Open problem in [JQSY19]

2. Applications to Quantum Cryptography
   - New public key encryption based on non-abelian group action
   - Efficient flavor conversion of quantum bit commitments
     previous: $O(\lambda^2)$-multiplicative factor [CLS01,Yan22]
     ours: $O(1)$-additive factor

Concurrent work [GJMZ23]

Main Toolkit Background

Susskind cared a "macroscopic" quantum state of space-time

$$\frac{|BlackHole\rangle + |NoBlackHole\rangle}{2}$$

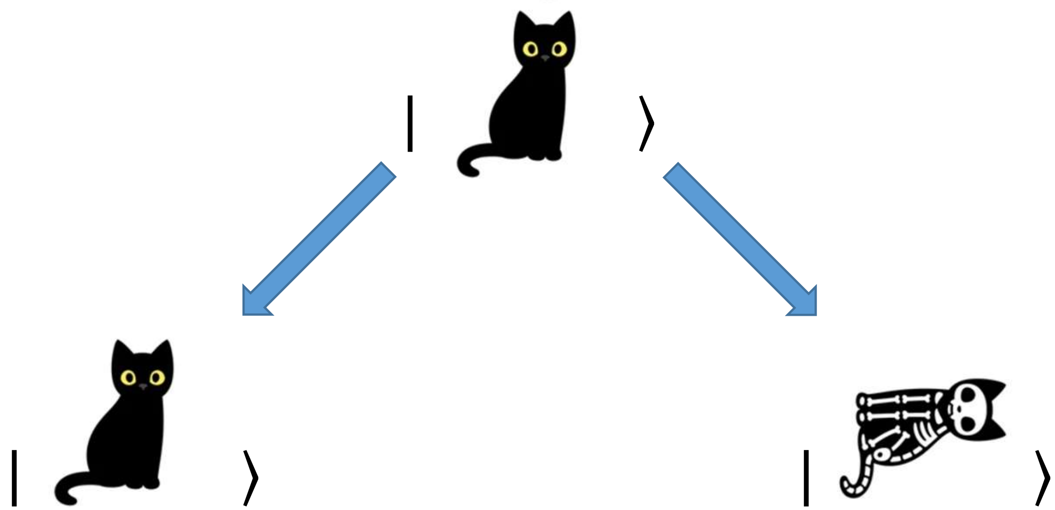
Susskind conjectured:

> Complexity(Seeing interference between $|v\rangle$ and $|w\rangle$)
> ≈ Complexity(Mapping $|v\rangle$ to $|w\rangle$ or vice versa)

… I cannot understand why

Schrödinger's cat

1. Prepare a cat in ket.
2. Measure if a single atom decaying or not. $(\frac{|decaying\rangle+|not\rangle}{\sqrt{2}})$
3. If decaying kill the cat; do nothing otherwise.



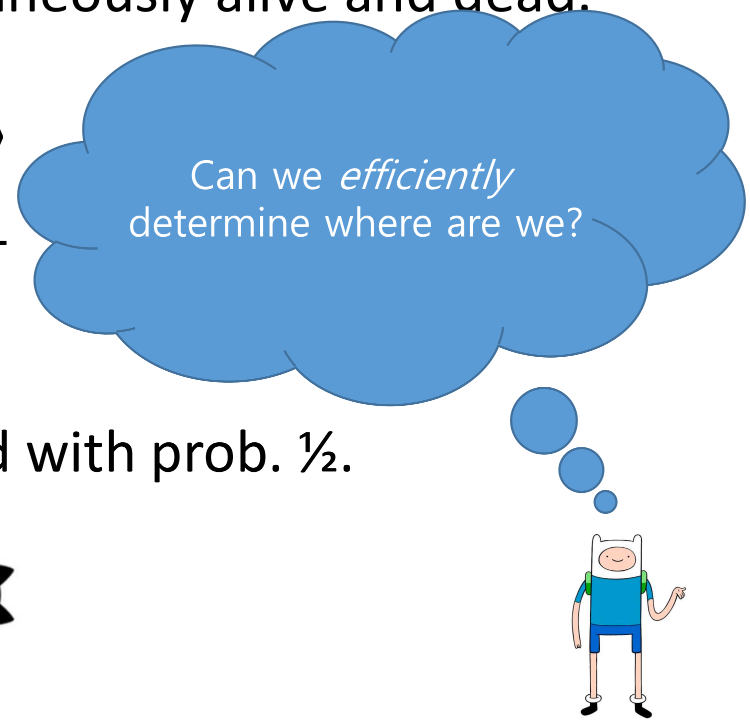
Schrödinger's cat

According to quantum physics, the cat is simultaneously alive and dead.

$|$  $\rangle + |$  $\rangle$

$\overline{}$

$\sqrt{2}$

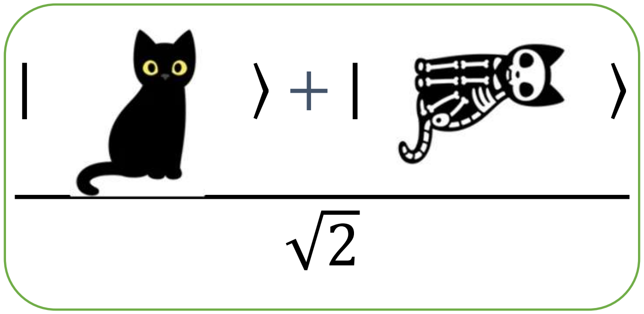


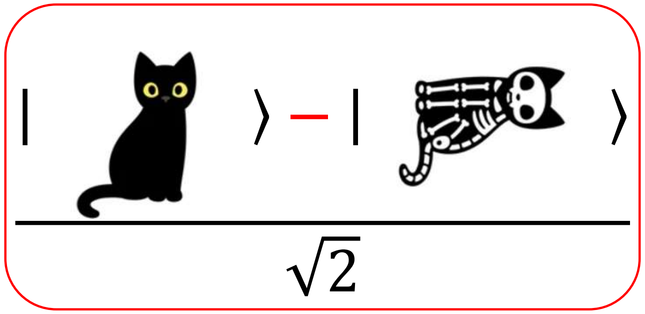
Classically, the cat lives with prob. ½ and is killed with prob. ½.

½ ×  ½ × 

Detecting interference

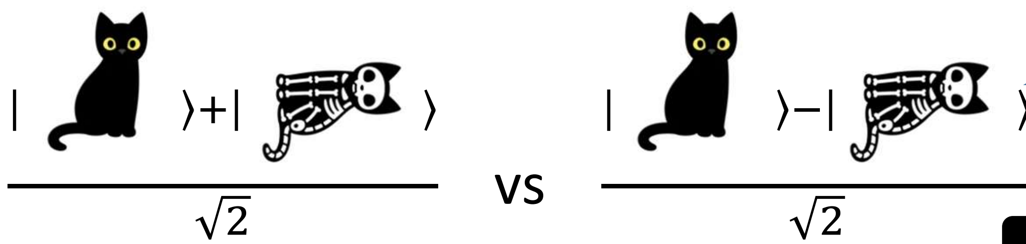
Distinguishing classical from quantum = Detecting interference (convexity)





Theorem for Schrödinger's cat

Our primary task is to distinguish the following two states.



Observing interference between |Alive⟩ and |Dead⟩

has similar circuit size

[Aaronson, Atia, Susskind’20] This task is *computationally* equivalent to the task to *swap* |  ⟩ and |  ⟩, meaning that a unitary U such that

Swapping |Alive⟩ and |Dead⟩

Detecting superposition in Schrödinger's cat is as hard as *resurrecting a dead cat* to alive (Necromancy-hard)

Formal Theorem [Aaronson, Atia, Susskind arXiv:2009.07450]

Let $|x\rangle, |y\rangle$ be two orthogonal states, $|\psi\rangle = \frac{|x\rangle+|y\rangle}{\sqrt{2}}, |\phi\rangle = \frac{|x\rangle-|y\rangle}{\sqrt{2}}$.

For any $\Delta > 0$, the following have the same circuit complexity up to O(1)

1) A unitary U such that

$$\frac{|\langle y|U|x\rangle + \langle x|U|y\rangle|}{2} = \Delta$$

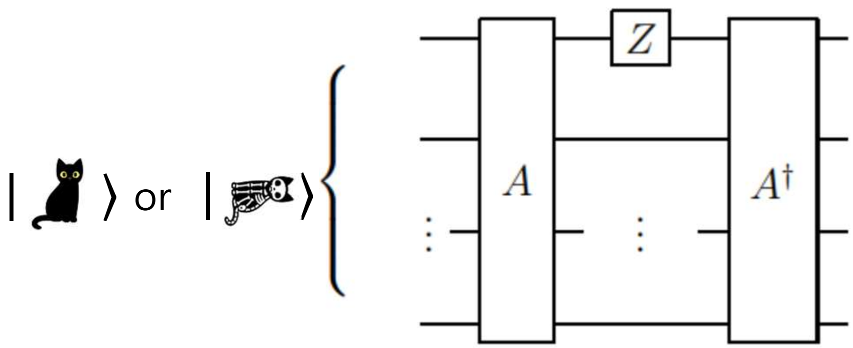
$\Delta = 1$: perfect case
this covers the
imperfect version

2) An algorithm A such that

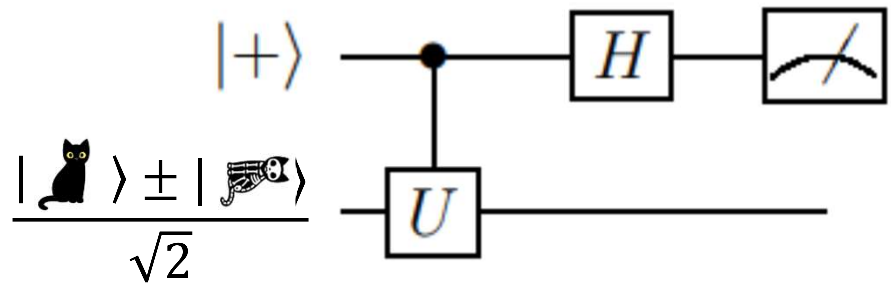
$$|\Pr[A|\psi\rangle \to 1] - \Pr[A|\phi\rangle \to 1]| = \Delta$$

[HMorimaeYamakawa]
We prove the same result with ancillary qubits, find some properties, …

Proof by circuits



swap to distinguish



distinguish to swap

CS / Cryptographic interpretation

1) (Swapping) A unitary U such that

$$\frac{|\langle y|U|x\rangle + \langle x|U|y\rangle|}{2} = \Delta$$

Search: Find x from y (or vice versa)

2) (Distinguishing) An algorithm A that distinguishes $|\psi\rangle, |\phi\rangle$ with bias Δ, that is,

$$|\Pr[A|\psi\rangle \to 1] - \Pr[A|\phi\rangle \to 1]| = \Delta$$

Decision: Determine if it is $|\psi\rangle$ or $|\phi\rangle$

"Search-to-decision reduction"

- (SAT) If we can efficiently decide if a formula has a solution, then we can find a solution of a formula.
- (Crypto) If one-way function exists, then there is a unpredictable bit.

AAS equivalence theorem shows **a new quantum search-to-decision reduction**.

AAS theorem as search-to-decision reduction

AAS theorem is **a new *quantum* search-to-decision reduction**.

This is our main message.

Similar ideas are implicitly used in literature

- Quantum Goldreich-Levin theorem
- Some technical parts of collapsing/collapse-binding literatures (pure vs mixed instead of interference)

We found new applications in **quantum cryptography**

- Quantum-ciphertext public key encryptions from non-abelian group action
- Efficient flavor conversion of quantum bit commitments

Example: Quantum Goldreich-Levin theorem

One-way permutation is $P: [N] \to [N]$ that is

- easy to compute forward ($|x, 0\rangle \to |x, P(x)\rangle$ is easy for any x)
- hard to invert ($|P(x), 0\rangle \to |P(x), x\rangle$ is hard for random x)

Question:
Can we extract "hard-to-predict" **bit** from this inversion-hard function?

[Goldreich-Levin] $r \cdot x$ is hard to compute given $(P(x), r)$.

A quantum proof by [Adcock&Cleve'02]
We can interpret it using the equivalence theorem.

Example: Quantum Goldreich-Levin theorem

One-way permutation is $P: [N] \to [N]$ that is

- easy to compute forward ($|x, 0\rangle \to |x, P(x)\rangle$ is easy for any x)
- hard to invert ($|P(x), 0\rangle \to |P(x), x\rangle$ is hard for random x)

Equivalently, it is hard to swap $|P(x), 0,0\rangle$ and $|P(x), 1, x\rangle$

By AAS equivalence, it is hard to distinguish

$$|P(x)\rangle \otimes \frac{|0,0\rangle \pm |1, x\rangle}{\sqrt{2}}$$

Example: Quantum Goldreich-Levin theorem

It is hard to distinguish

$$|P(x)\rangle \otimes \frac{|0,0\rangle \pm |1,x\rangle}{\sqrt{2}}$$

Measure the second parts on a Hadamard basis.

- $|P(x)\rangle \otimes \sum_r |r \cdot x, r\rangle$ if the sign is +
- $|P(x)\rangle \otimes \sum_r |r \cdot x \oplus 1, r\rangle$ if the sign is -

Two states are hard to distinguish,

i.e., computing $r \cdot x$ from $(P(x), r)$ is hard!

Applications

Swapping $|x\rangle$ and $|y\rangle$ is equivalent to distinguishing

$$|x\rangle \pm |y\rangle$$

- Quantum-ciphertext PKE from non-abelian group action

  Previously, only minicrypt constructions are known
- Efficient flavor conversion of quantum bit commitment

  Two definitions of commitments are essentially the same

Cryptographic (non-abelian) group action

Group G and set S, group action $G \times S \to S$ denoted by $(g, s) \mapsto g \cdot s$:

$$e \cdot s = s, \qquad g \cdot (h \cdot s) = (gh) \cdot s$$

(One-way)	Hard to find g from $(s, g \cdot s)$	$(s, g \cdot s) \mapsto g$ is hard
(Pseudorandom)	$(s, g \cdot s)$ looks like random (s, t)	$(s, g \cdot s) \approx (s, t)$

PKE from *non-abelian* group action is an open problem posed in [JQSY19]

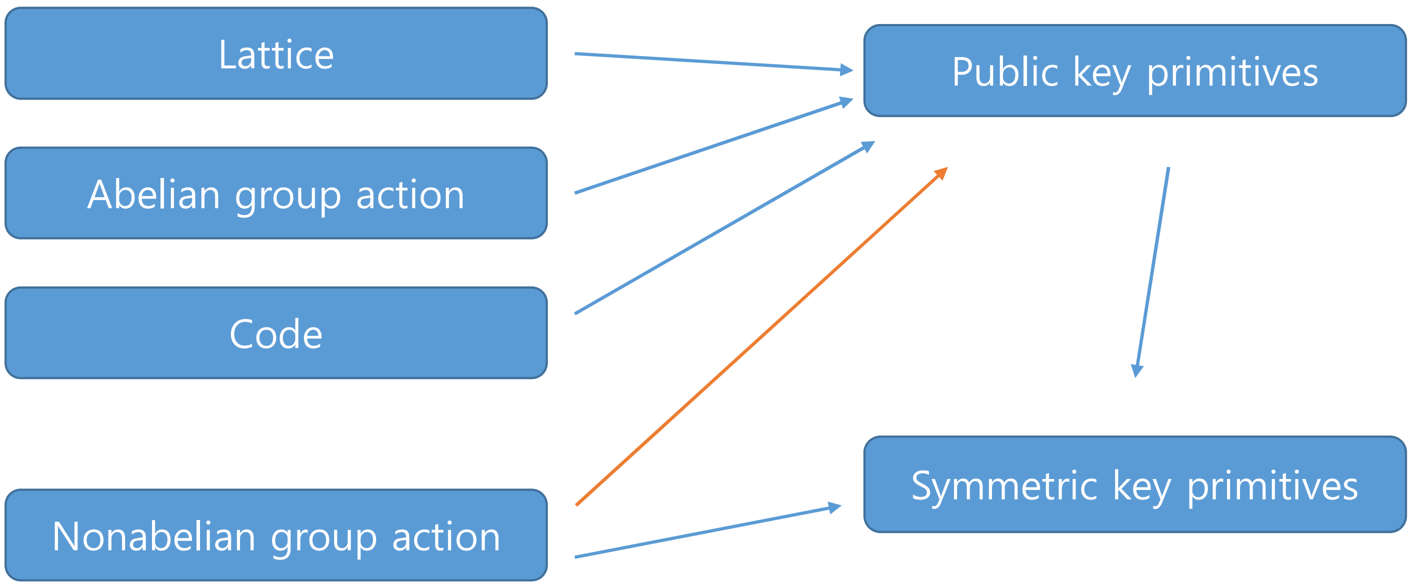
Abelian group actions naturally allow Diffie-Hellman style key exchange
Alice: $(g, g \cdot s)$ Bob: $(h, h \cdot s)$, share $(g \cdot s, h \cdot s)$ then each can compute

$$(gh) \cdot s = g \cdot (h \cdot s) = h \cdot (g \cdot s) = (hg) \cdot s$$

[HMorimaeYamakawa] Quantum PKE from non-abelian group action

Classical construction (possibility)
Quantum construction (Our)

Contributions in diagram (+ more)



[HMorimaeYamakawa] Quantum PKE from non-abelian group action

PKE from non-abelian group action, idea

Possible via AAS equivalence theorem albeit with quantum ciphertexts

Encode bit in *phase*

For group action $G \times S \to S$, if a ciphertext of b is of the form

$$|\phi^b\rangle = \frac{|0\rangle|s\rangle + (-1)^b|1\rangle|g \cdot s\rangle}{\sqrt{2}}$$

for random $s \in S, g \in G$.

How to construct?

AAS theorem: Distinguishing $|\phi^0\rangle$ from $|\phi^1\rangle$ is at least as hard as finding a map from $|s\rangle$ to $|g \cdot s\rangle$; it probably know g, breaking one-wayness

PKE from non-abelian group action

For a public key $(s_0 = s, s_1 = g \cdot s)$, a ciphertext of b is of the form

$$|\phi^b\rangle \propto |0\rangle \sum_{h:h\cdot s_0=y} |h\rangle + (-1)^b|1\rangle \sum_{h:h\cdot s_1=y} |h\rangle$$

for random $y \in S$.

- easily constructible

1. Prepare $\sum_{h\in G}|0\rangle|h\rangle + (-1)^b|1\rangle|h\rangle$
2. Append new register and compute $\sum_{h\in G}|0\rangle|h\rangle|h \cdot s_0\rangle + (-1)^b|1\rangle|h\rangle|h \cdot s_1\rangle$
3. Measure the last register to obtain y, which collapses to the ciphertext.

- if underlying action is pseudorandom then it is IND-CPA secure
- if underlying action is one-way, then it is IND-CPA secure … or we can construct a one-shot signature

Cf) Inspired by the "win-win" result of [Zha19]

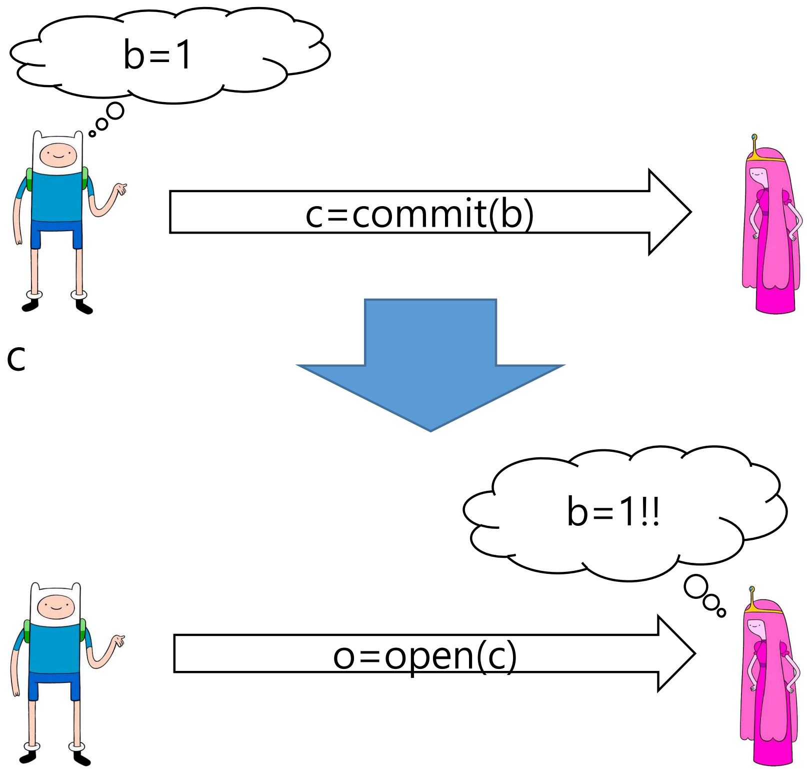
(Non-interactive) Bit commitment

Sender A vs Receiver B

Sender commit a bit b,
and later can reveal “it’s the commitment of b.”

[Committing] A commits bit b (say =1) with
“the commitment” c

[Opening] A reveals “the opening” o and
B convinces what was b (=1)



Security of Bit commitment

Sender A vs Receiver B

Sender commit a bit b,
and later can reveal "it's the commitment of b."

Receiver cannot know b until reveal. **Hiding**

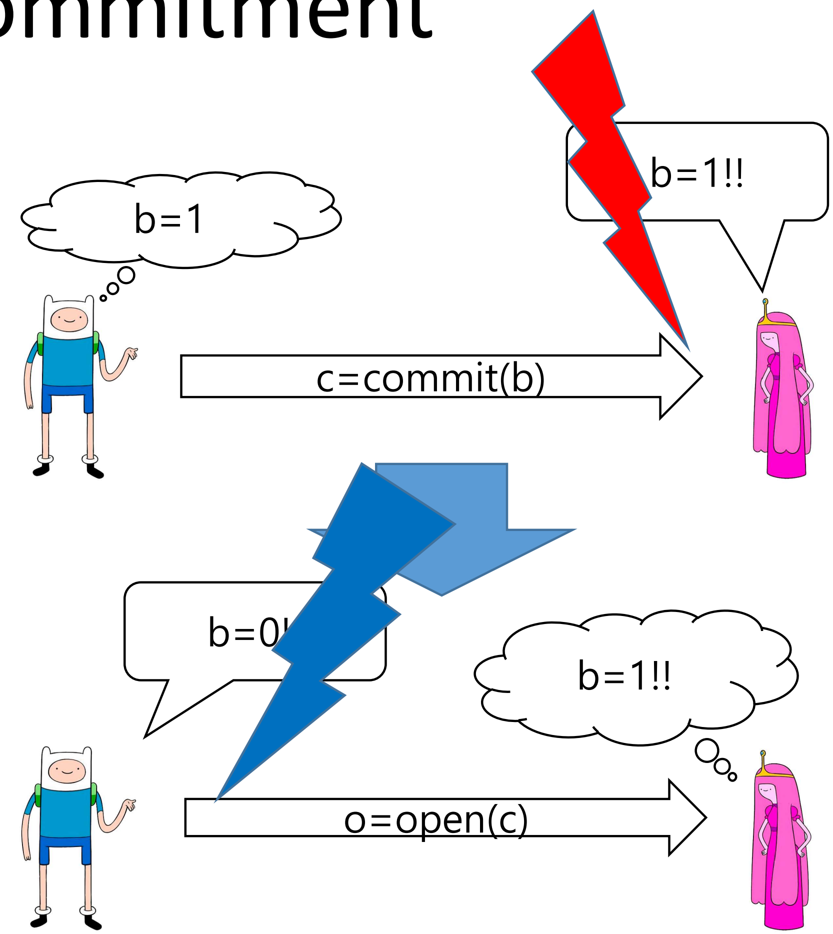
Sender can't change b after commit. **Binding**

We want the binding/hiding statistically hold,

which is impossible (even for quantum)

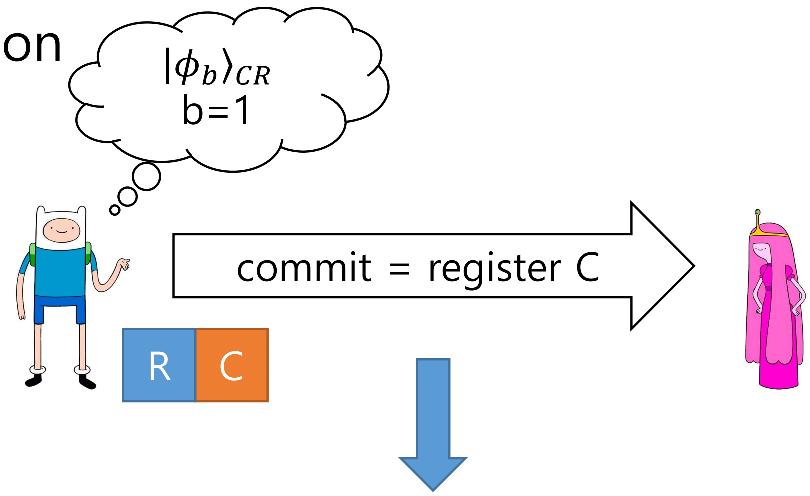
Relax one of them by secure against
(non-uniform) polynomial time algorithms.

1. **(Statistically) Hiding** commitment
2. **(Statistically) Binding** commitment



(Canonical) Quantum bit commitment

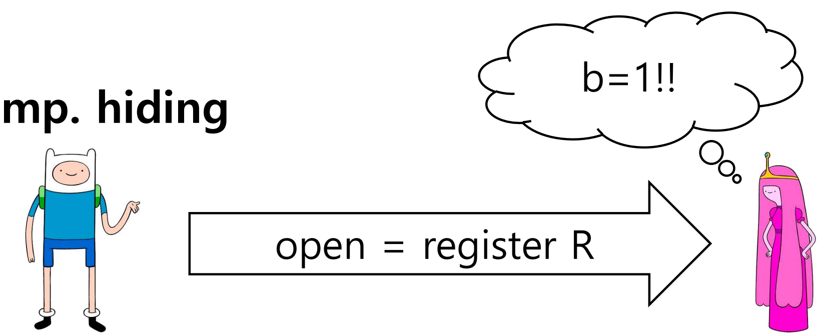
Using quantum channels for communication



- Simpler constructions
- Inherently non-interactive [Yan22]

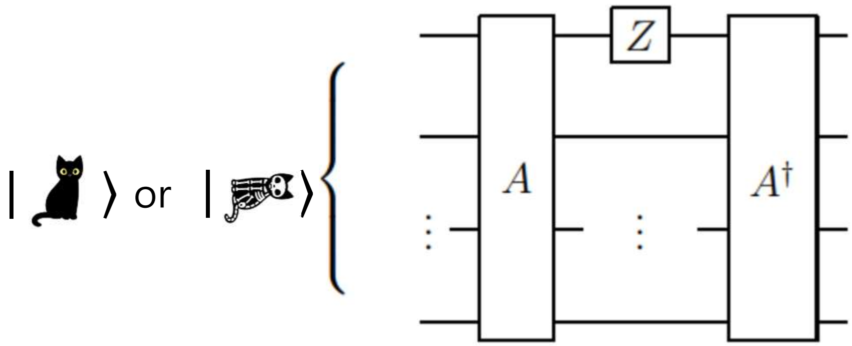
A prepares $|\phi_b\rangle_{CR}$ and sends C as a commitment,
sends R as an opening.

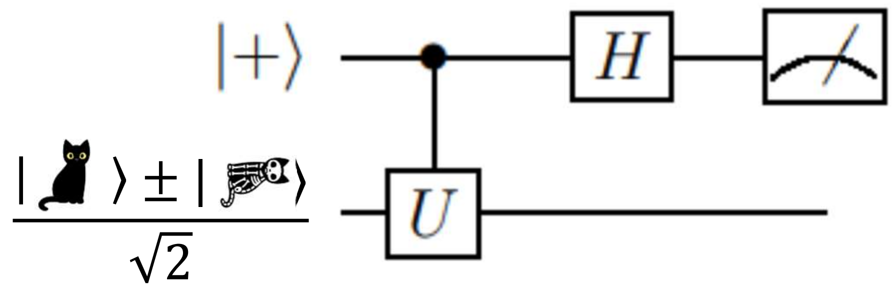
- Efficient **conversion of flavors** [Yan22]
  stat. hiding comp. binding ↔ stat. binding comp. hiding



[HMorimaeYamakawa] Better conversion
Two notions are essentially equivalent

More on AAS equivalence





Locality-preserving:

If A (or U) does not act on some qubits, then U (or A) does not act on those qubits either.

Advice version:

The theorem holds even if there is ancillary qubits (with a worse bound)

Efficient conversion (hiding ⇔ binding), idea

$U_0|0\rangle = |\phi_0\rangle_C$ and $U_1|0\rangle = |\phi_1\rangle_{CR}$ be the commitment states;
Sender holds the reveal register **R**
and sends the commitment register **C**.

Hiding/Biding have the following locality features.

(Hiding) $|\phi_0\rangle_{CR}$ and $|\phi_1\rangle_{CR}$ are hard to distinguish by unitary over **C**

(Binding) $|\phi_0\rangle_{CR}$ and $|\phi_1\rangle_{CR}$ are hard to swap by unitary over **R**

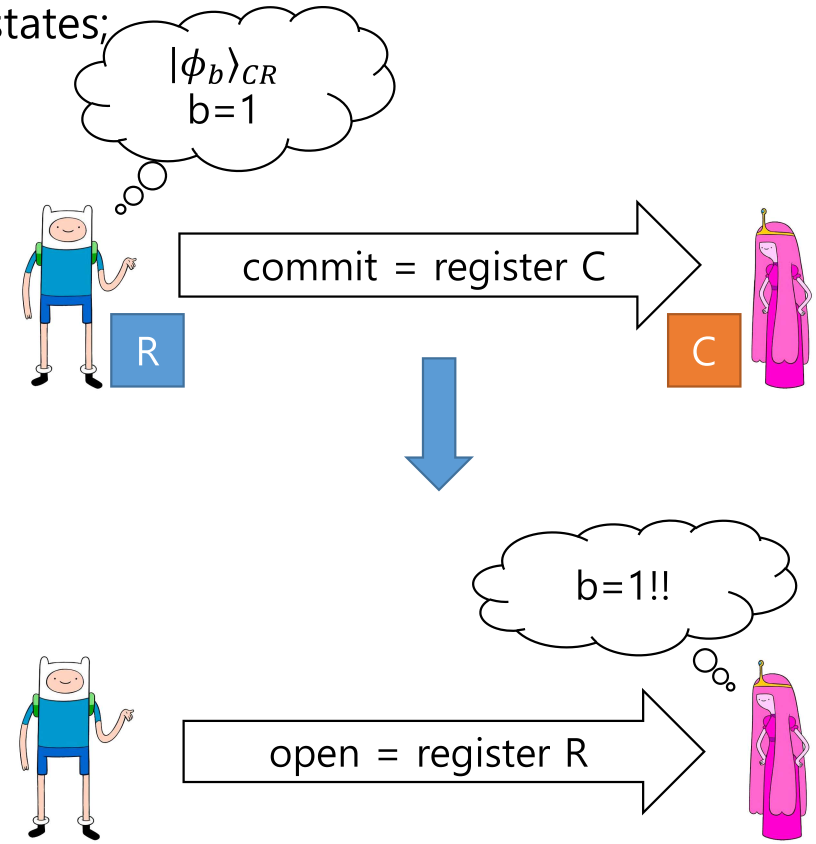
Let $|\psi_b\rangle = \frac{|\phi_0\rangle+(-1)^b|\phi_1\rangle}{\sqrt{2}}$, then AAS theorem says that

(Binding) swapping $|\phi_0\rangle_{CR}$ and $|\phi_1\rangle_{CR}$
by unitary over **R**

| |

(Hiding') distinguishing $|\psi_0\rangle_{CR}$ and $|\psi_1\rangle_{CR}$
by unitary over **R**

Not orthogonal



Our compiler

$U_0|0\rangle = |\phi_0\rangle_{CR}$ and $U_1|0\rangle = |\phi_1\rangle_{CR}$ be the commitment states

The new commitment scheme commits b by

$$\frac{|0\rangle|\phi_0\rangle + (-1)^b|1\rangle|\phi_1\rangle}{\sqrt{2}}$$

1) If original scheme is X-hiding then new scheme is X-binding
2) If original scheme if Y-binding then new scheme is Y-hiding

X,Y=perfect, statistical, computational

Concurrent work by Gunn,Ju,Ma,Zhandry

Conclusion

1. New quantum search-to-decision reduction based on the equivalence theorem [AAS20] of detecting interference and swapping two states, with some generalizations.

2. Showing the power of new reduction by applications
   - New quantum-ciphertext PKE from non-abelian group action
   - Efficient quantum commitment flavor conversion

Thanks!

Any question?

Annoying definition of “swapping”

Swapping advantage is highly non-standard.

Orthogonality/specific target are annoying.

$$\frac{|\langle y|U|x\rangle + \langle x|U|y\rangle|}{2} = \Delta$$

We may need to do a large amount of extra works for obtaining a bound on the usual definition something like:

$$\frac{|\langle y|U|x\rangle|^2 + |\langle x|U|y\rangle|^2}{2}$$

Alternative version from [GJMZ23]

Hermitian $W = \Pi_{+1} - \Pi_{-1}$ where $\Pi_{\pm 1}$ are the ± 1 eigenspaces of W

A quantum state $|\psi\rangle$ is **chosen by adversary**.

Let $|\psi_{\pm}\rangle = \Pi_{\pm 1}|\psi\rangle$, the following two advantages are similar:

1) Distinguishing $\Pi_b|\psi\rangle$ for unknown $b \in \{\pm 1\}$.

2) Mapping $\Pi_{\pm 1}|\psi\rangle$ into **any** state in $\Pi_{\mp 1}$, or

$$||\Pi_{-1} U \Pi_{+1}|\psi\rangle||^2$$

If we simply write $\Pi_b = |b\rangle\langle b| \otimes I$ and $|\psi\rangle = |0, x\rangle + |1, y\rangle$, it says TFAE:

1) Distinguishing $|0, x\rangle \pm |1, y\rangle$
2) Mapping $|0, x\rangle$ to $|1, \star\rangle$

Collapsing version from [Zha22]

Recall that distinguishing $|x\rangle \pm |y\rangle$ is equivalent to the distinguishing

$|x\rangle + |y\rangle$ and (1/2,x),(1/2,y)

which is equivalent to distinguishing $|x\rangle + |y\rangle$ from *its measurement result!*

In general, we can extend it for one direction: let x_j be orthogonal and let **q: poly**

$$|\psi\rangle = \sum_{0 \le j < q} |x_j, y_j\rangle$$

we can show that distinguishing $|\psi\rangle$ from its measurement result using a binary measurement P is hard if the following holds:

1. Measure $|\psi\rangle$ with $\{|x_j\rangle\langle x_j| \otimes I\}$ and obtain j with $|x_j, y_j\rangle$ with prob $\left\| |y_j\rangle \right\|^2$
2. Apply P to the result
3. Measure it again with $\{|x_j\rangle\langle x_j| \otimes I\}$, then whp the result is j again.