# Post-Quantum Proof Techniques Part 1:

# Introduction to Quantum Rewinding

Fermi Ma

(Simons & Berkeley)

Based on:

- "Quantum Proofs of Knowledge" by **Dominique Unruh** (2012)
- "Computationally Binding Quantum Commitments" by **Dominique Unruh** (2016)
- "Zero Knowledge Against Quantum Attacks" by **John Watrous** (2005)
- "Quantum Arthur Merlin Games" by **Chris Marriott** and **John Watrous** (2005)
- "Traité des substitutions et des équations algébriques" by **Camille Jordan** (1870)

# Today's Goal:

We want *classical* cryptography secure against *quantum* attacks (post-quantum cryptography)

# What this talk will cover:

# What this talk will cover:

1. Is LWE all we need for post-quantum security?

# What this talk will cover:

1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol

# What this talk will cover:

1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):

# What this talk will cover:

1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
    - Review: classical proof of knowledge

# What this talk will cover:

1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
    - Review: classical proof of knowledge
    - How to define post-quantum commitments

# What this talk will cover:

1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma

# What this talk will cover:

1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol

# What this talk will cover:

1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge

# What this talk will cover:

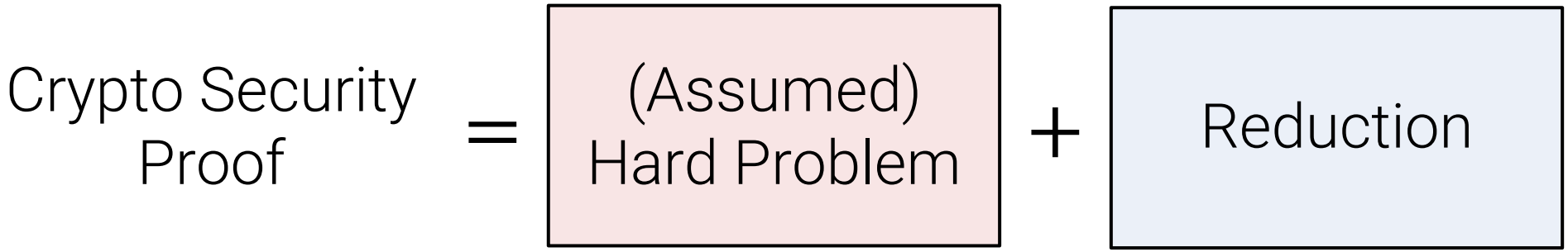
1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge
   - Watrous's ZK rewinding lemma

# What this talk will cover:

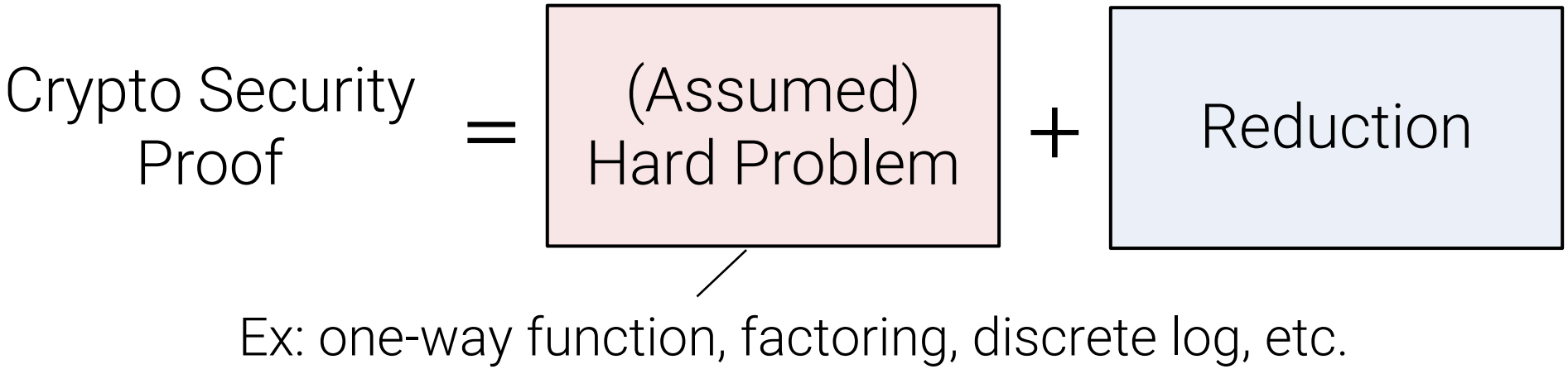
1. Is LWE all we need for post-quantum security?
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge
   - Watrous's ZK rewinding lemma

# How do cryptographers prove security?

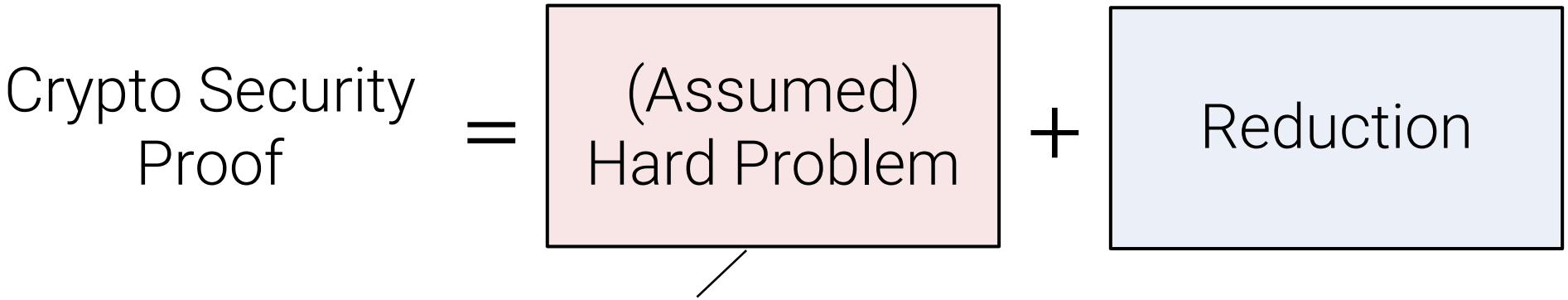
# How do cryptographers prove security?



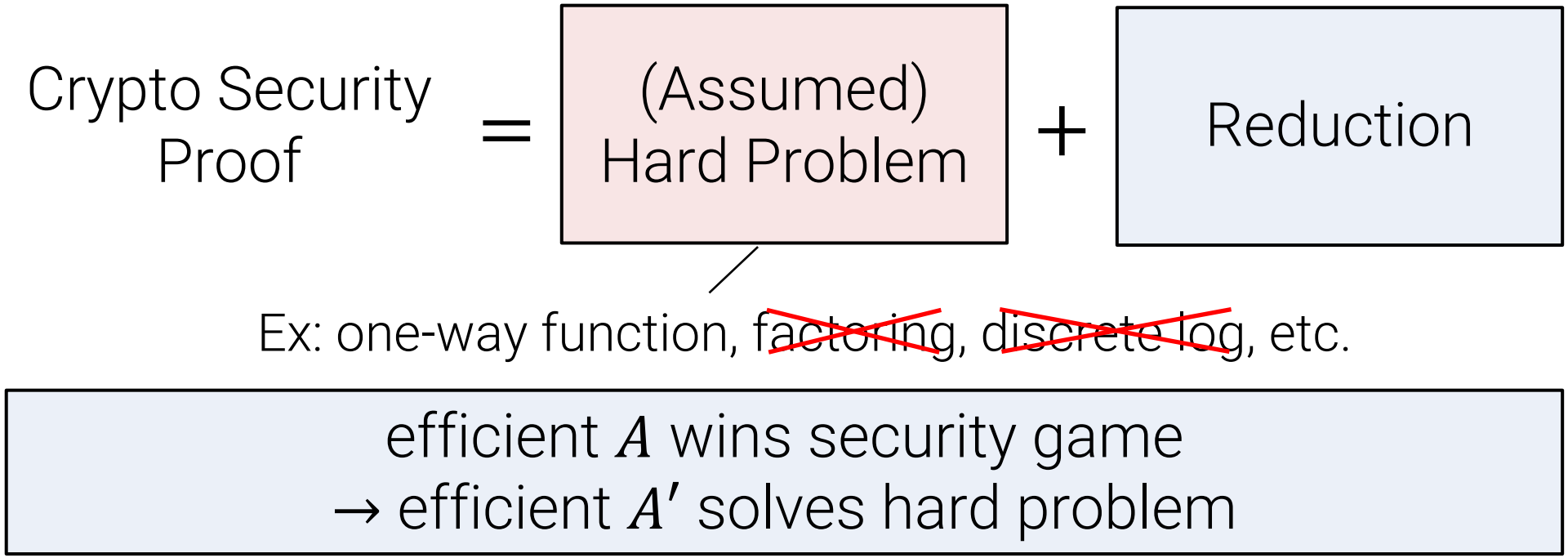
# How do cryptographers prove security?



# How do cryptographers prove security?



# How do cryptographers prove security?




**Key point:** problem must be hard for quantum computers!

# How do cryptographers prove security?

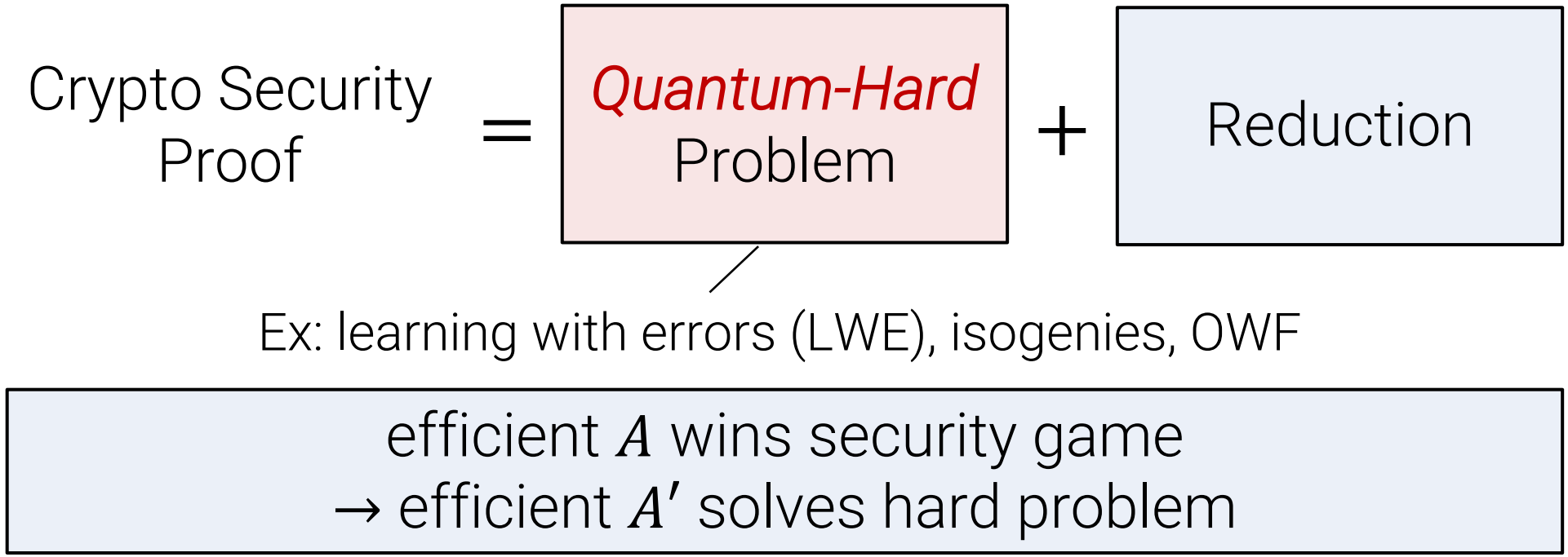
Crypto Security Proof = *Quantum-Hard* Problem + Reduction

efficient $A$ wins security game
$\rightarrow$ efficient $A'$ solves hard problem

**Key point:** problem must be hard for quantum computers!

Fortunately, we have (plausibly) quantum-hard problems.

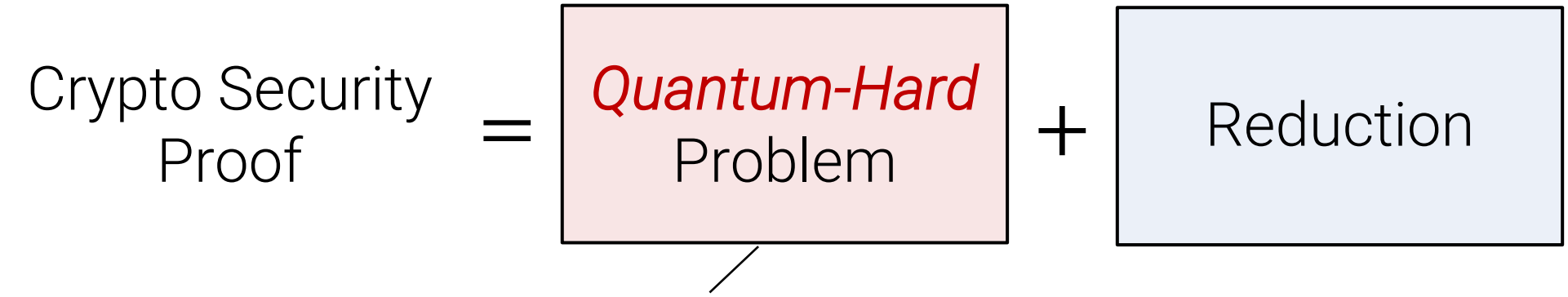
# How do cryptographers prove security?




**Key point:** problem must be hard for quantum computers!

Fortunately, we have (plausibly) quantum-hard problems.

# How do cryptographers prove security?




**Key point:** problem must be hard for quantum computers!

Fortunately, we have (plausibly) quantum-hard problems.

# Done?

**Conjecture**

classical security reduction + quantum-hard problem

→ post-quantum security?

**Conjecture**

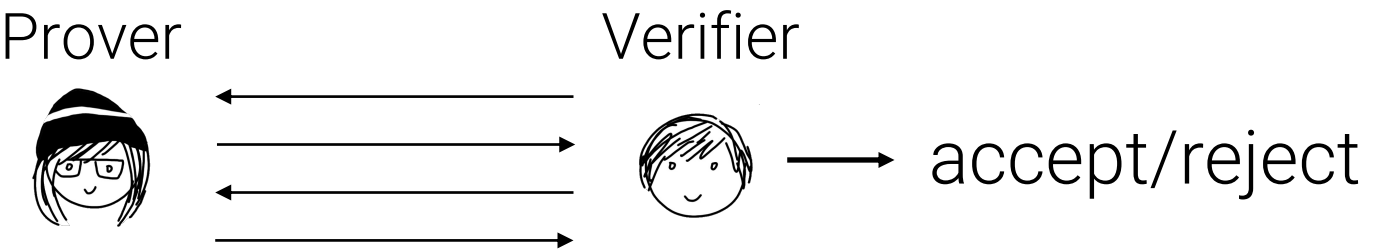
classical security reduction + quantum-hard problem
→ post-quantum security?

# No!

**Conjecture**
classical security reduction + quantum-hard problem
→ post-quantum security?

# No!

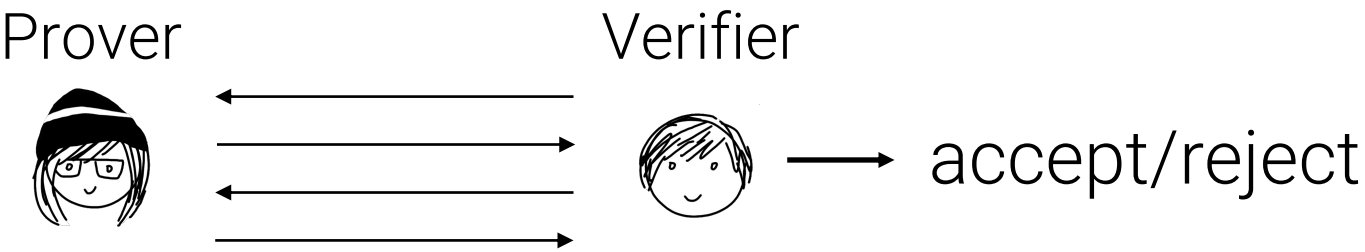
[BCMVV18] Protocol



**Conjecture**
classical security reduction + quantum-hard problem
→ post-quantum security?

# No!

[BCMVV18] Protocol

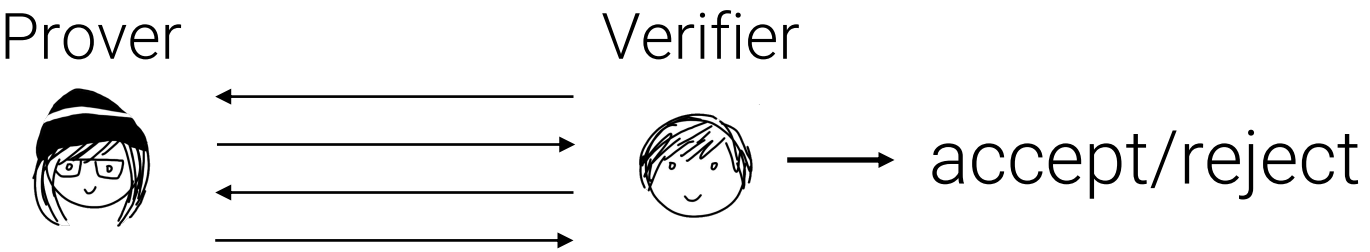



- Efficient classical P *cannot* make V accept assuming LWE

**Conjecture**
classical security reduction + quantum-hard problem
→ post-quantum security?

# No!

[BCMVV18] Protocol

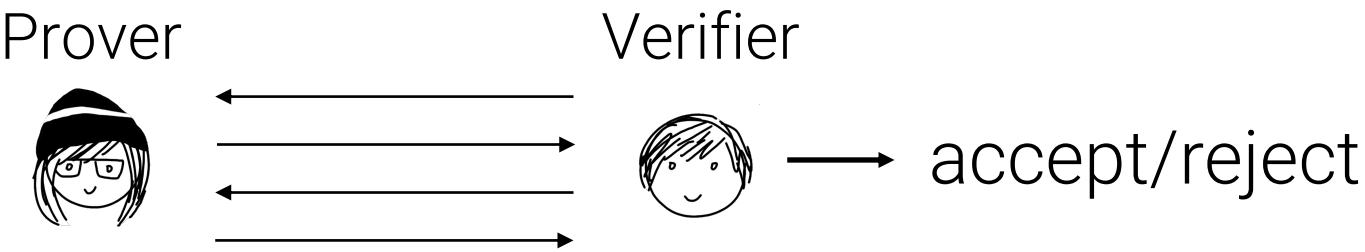



- Efficient classical P *cannot* make V accept assuming LWE
- Efficient quantum P *can* convince V to accept.

**Conjecture**
classical security reduction + quantum-hard problem
→ post-quantum security?

# No!

[BCMVV18] Protocol




- Efficient classical P *cannot* make V accept assuming LWE.
- Efficient quantum P *can* convince V to accept.

In [BCMVV18] this is presented as a proof of quantumness.

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical reduction:

efficient *classical* $A$ wins security game
→ efficient *classical* $A'$ solves hard problem

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical reduction:

efficient *classical* $A$ wins security game
→ efficient *classical* $A'$ solves hard problem

Quantum reduction:

efficient *quantum* $A$ wins security game
→ efficient *quantum* $A'$ solves hard problem

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

| | |
|---|---|
| Classical reduction: | efficient *classical* $A$ wins security game → efficient *classical* $A'$ solves hard problem |
| Quantum reduction: | efficient *quantum* $A$ wins security game → efficient *quantum* $A'$ solves hard problem |

Crucially, the classical security reduction for the [BCMVV18] protocol ***does not handle quantum attacks***.

**Takeaway**

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***

$a$

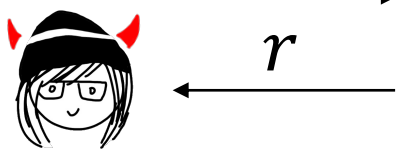
[BCMVV18] Reduction

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***



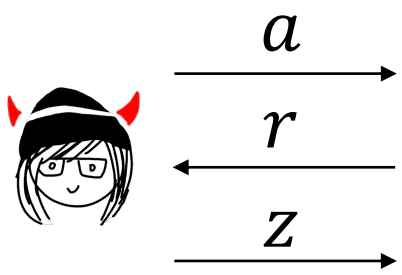

[BCMVV18] Reduction

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***



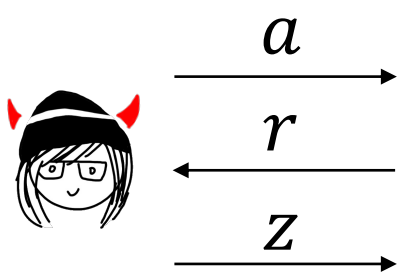

[BCMVV18] Reduction

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***




[BCMVV18] Reduction

1) Record $(a, r, z)$

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***


[BCMVV18] Reduction

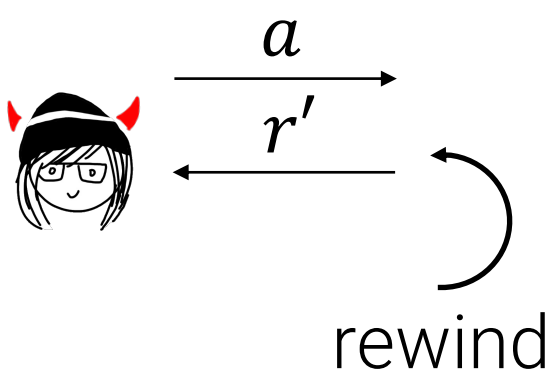
1) Record $(a, r, z)$
2) Rewind

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***




[BCMVV18] Reduction

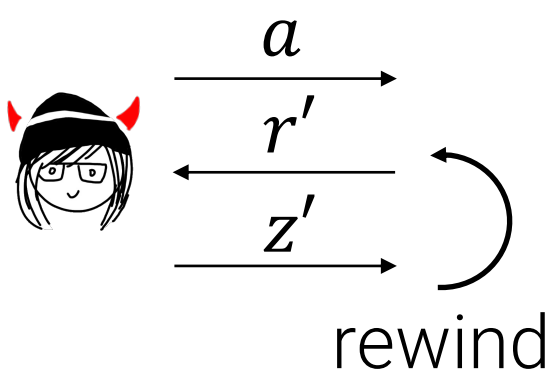
1) Record $(a, r, z)$
2) Rewind

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***




[BCMVV18] Reduction

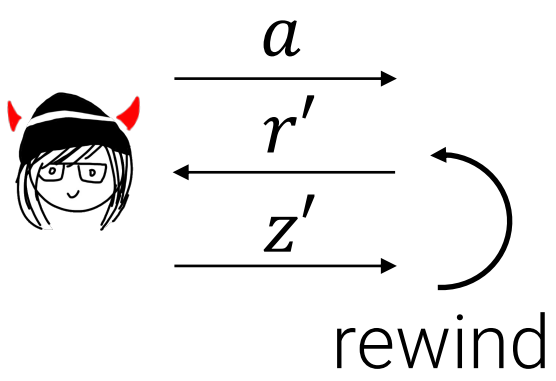
1) Record $(a, r, z)$
2) Rewind

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***




[BCMVV18] Reduction

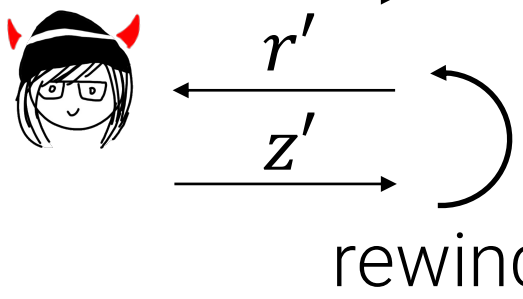
1) Record $(a, r, z)$
2) Rewind
3) Record $(a, r', z')$

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***




[BCMVV18] Reduction

1) Record $(a, r, z)$
2) Rewind
3) Record $(a, r', z')$

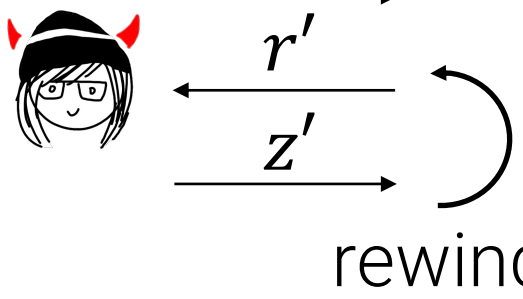
break LWE

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***




[BCMVV18] Reduction

1) Record $(a, r, z)$
2) Rewind
3) Record $(a, r', z')$

break LWE →

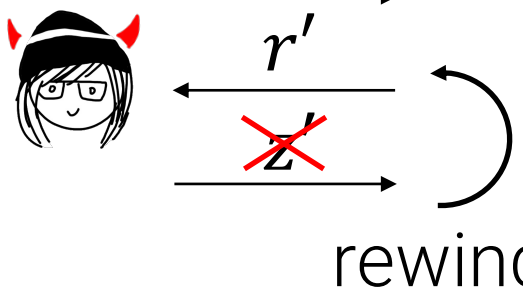
Reduction doesn't work for quantum adversaries because measuring the response can disturb the adversary's state.

## Takeaway

Quantum computers can break classically secure crypto *without* solving the underlying hard problem!

How is this possible?

Classical security of [BCMVV18] relies on ***rewinding***




[BCMVV18] Reduction

1) Record $(a, r, z)$
2) Rewind
3) ~~Record $(a, r', z')$~~

~~break LWE~~

Reduction doesn't work for quantum adversaries because measuring the response can disturb the adversary's state.

More generally, classical rewinding reductions do not capture quantum adversaries.

More generally, classical rewinding reductions do not capture quantum adversaries. But rewinding is one of the most common techniques in cryptography!

More generally, classical rewinding reductions do not capture quantum adversaries. But rewinding is one of the most common techniques in cryptography!

Is it possible that rewinding-based crypto (zero knowledge proofs, proofs of knowledge, etc.) is quantumly broken?

More generally, classical rewinding reductions do not capture quantum adversaries. But rewinding is one of the most common techniques in cryptography!

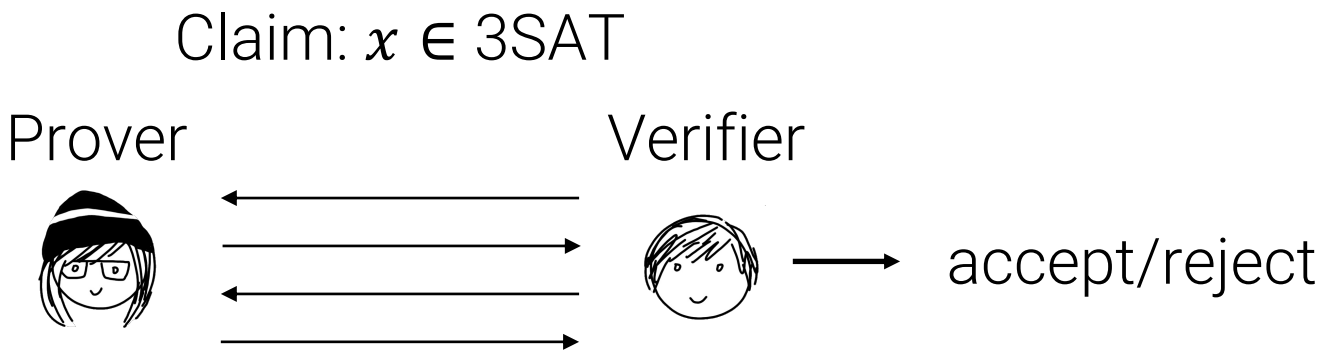
Is it possible that rewinding-based crypto (zero knowledge proofs, proofs of knowledge, etc.) is quantumly broken?

**Rest of this talk:** extend classical rewinding reductions to handle quantum attacks, i.e., “quantum rewinding”

**Rest of this talk:** extend classical rewinding reductions to handle quantum attacks, i.e., “quantum rewinding”

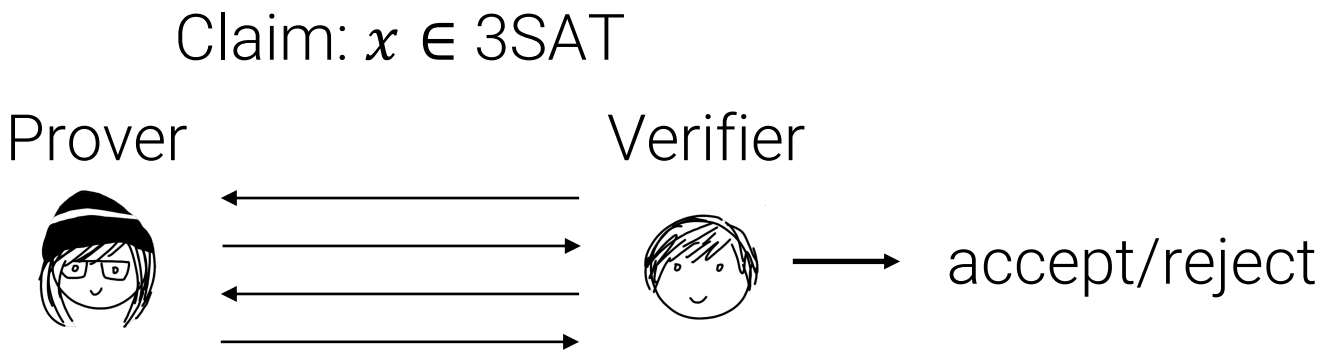
**Rest of this talk:** extend classical rewinding reductions to handle quantum attacks, i.e., "quantum rewinding"

**Focus:** interactive proof systems



**Rest of this talk:** extend classical rewinding reductions to handle quantum attacks, i.e., "quantum rewinding"

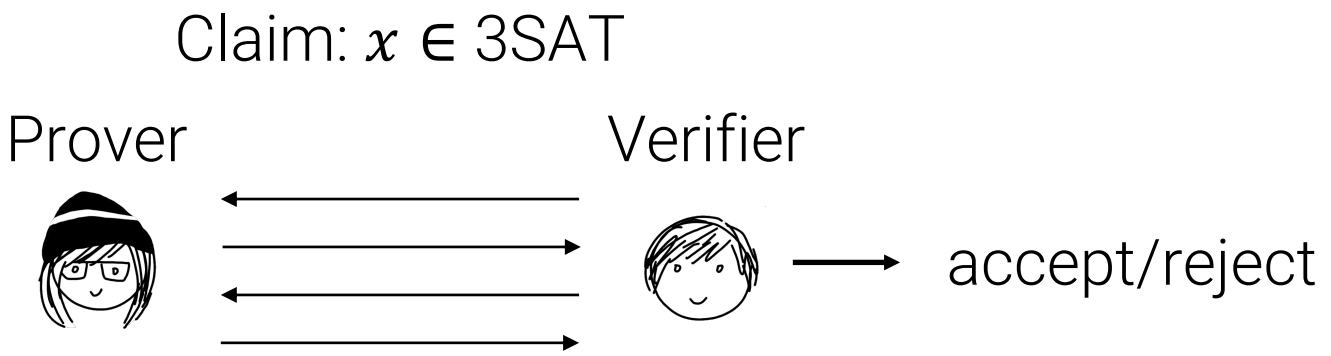
**Focus:** interactive proof systems




**Proof of Knowledge:**
If $P^*$ convinces $V$ to accept,
then $P^*$ must "know" a witness.

**Rest of this talk:** extend classical rewinding reductions to handle quantum attacks, i.e., "quantum rewinding"

**Focus:** interactive proof systems



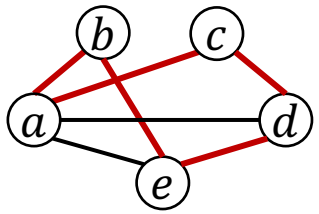

**Proof of Knowledge:**
If $P^*$ convinces $V$ to accept, then $P^*$ must "know" a witness.

**Zero Knowledge [GMR85]:**
View of malicious $V^*$ can be efficiently ***simulated*** without $P$.

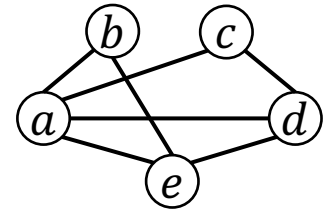
# What this talk will cover:

1. Is LWE all we need for post-quantum security? ✓
2. Review: Blum's Hamiltonicity protocol
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge
   - Watrous's ZK rewinding lemma

# Blum's Protocol for Hamiltonian Cycles

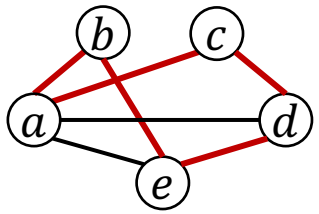
$G =$ 


Prover 

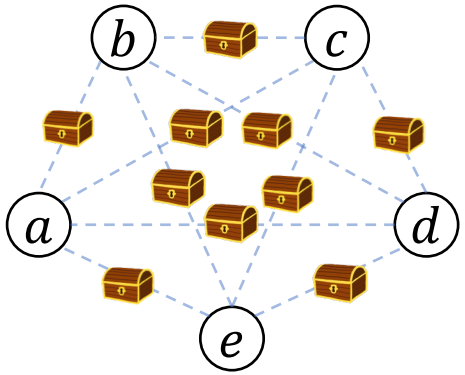
$G =$ 

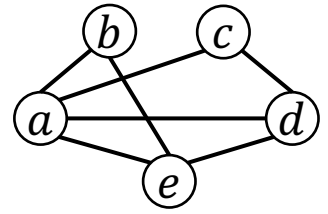

Verifier 

# Blum's Protocol for Hamiltonian Cycles

$G =$ 


Prover 



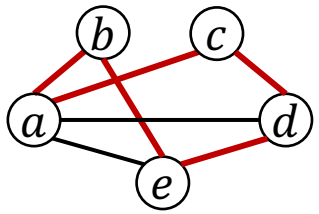

$G =$ 


Verifier 

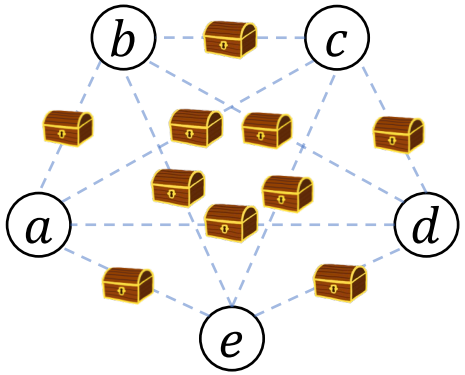
Sample $\pi \leftarrow S_V$.

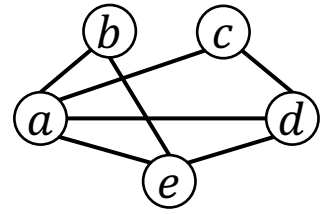
Commit to the adjacency matrix of $\pi(G)$

# Blum's Protocol for Hamiltonian Cycles

$G =$ 


Prover 




$G =$ 


Verifier 

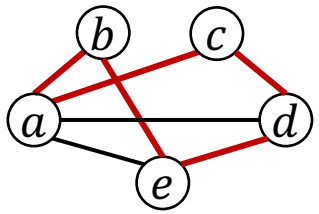
Sample $\pi \leftarrow S_V$.

Commit to the adjacency matrix of $\pi(G)$

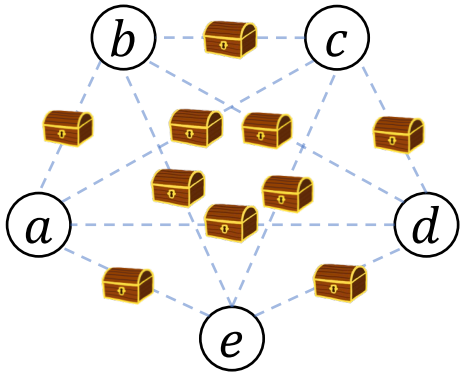
$r$

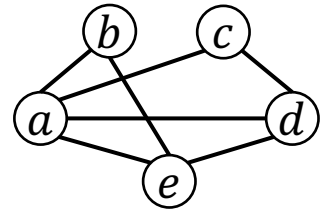
Sample random $r \leftarrow \{0,1\}$

# Blum's Protocol for Hamiltonian Cycles

$G =$ 


Prover 




$G =$ 

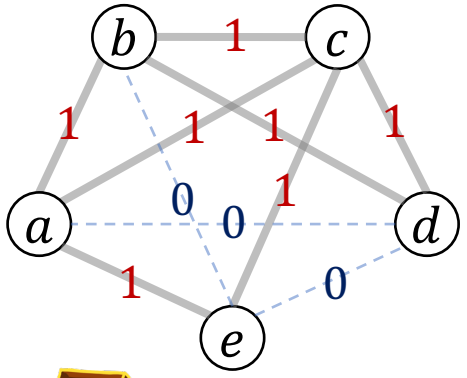

Verifier 

Sample $\pi \leftarrow S_V$.

Commit to the adjacency matrix of $\pi(G)$

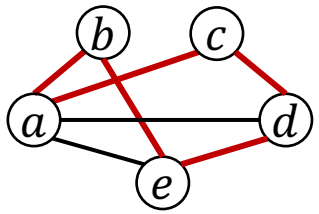
$r$

Sample random $r \leftarrow \{0,1\}$

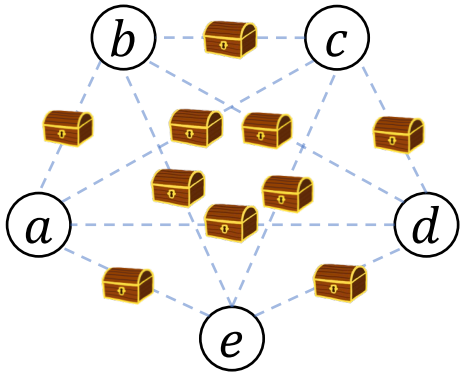
$\pi,$ 

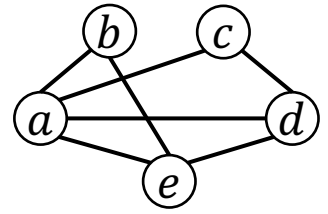

 (if $r = 0$)

# Blum's Protocol for Hamiltonian Cycles

$G =$ 


Prover 




$G =$ 

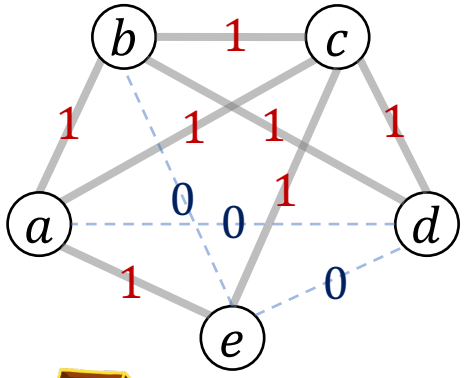

Verifier 

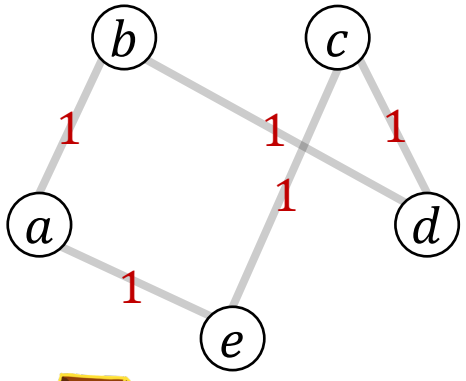
Sample $\pi \leftarrow S_V$.

Commit to the adjacency matrix of $\pi(G)$

$r$

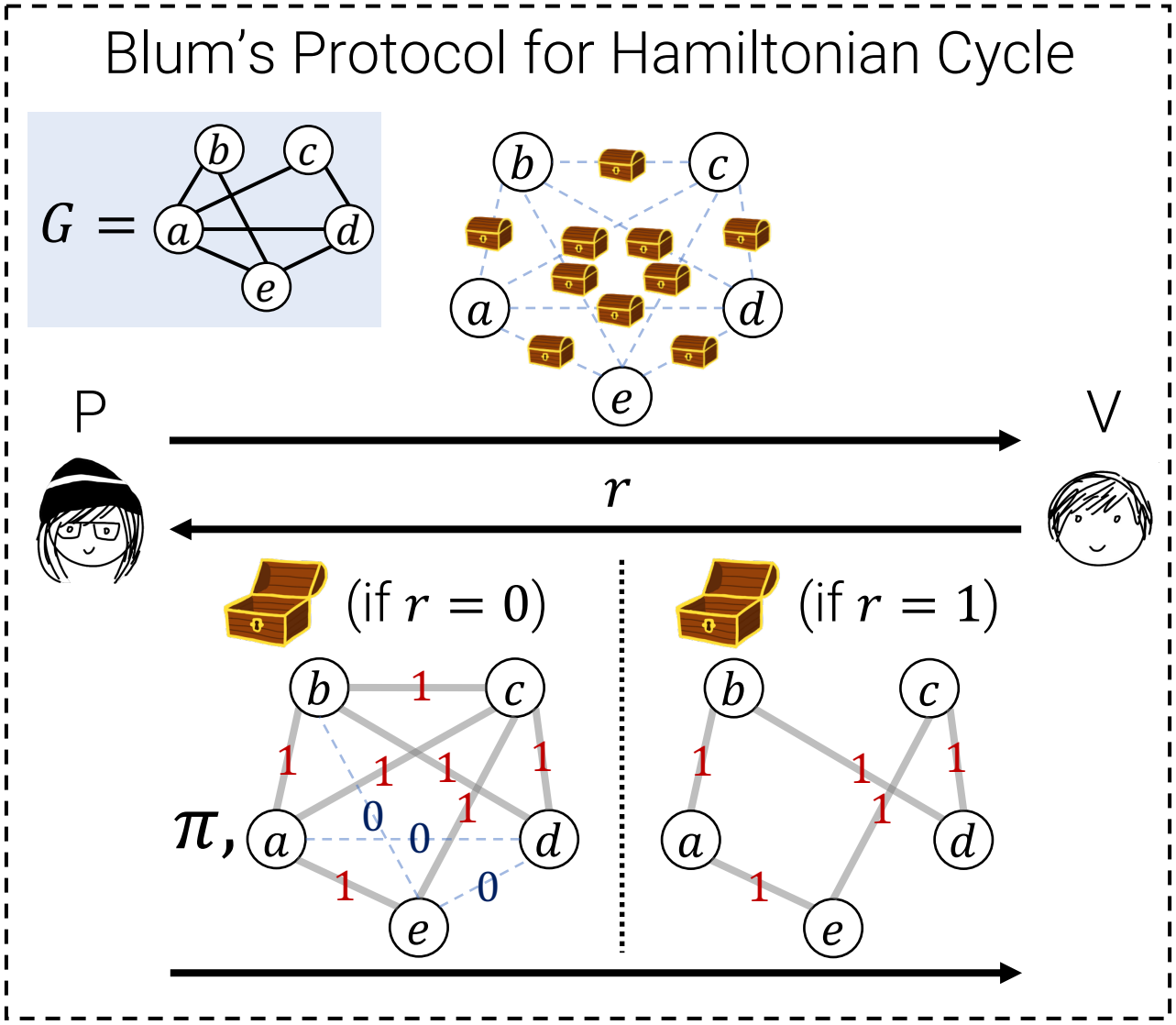
Sample random $r \leftarrow \{0,1\}$

$\pi$, 


or 


 (if $r = 0$)

 (if $r = 1$)

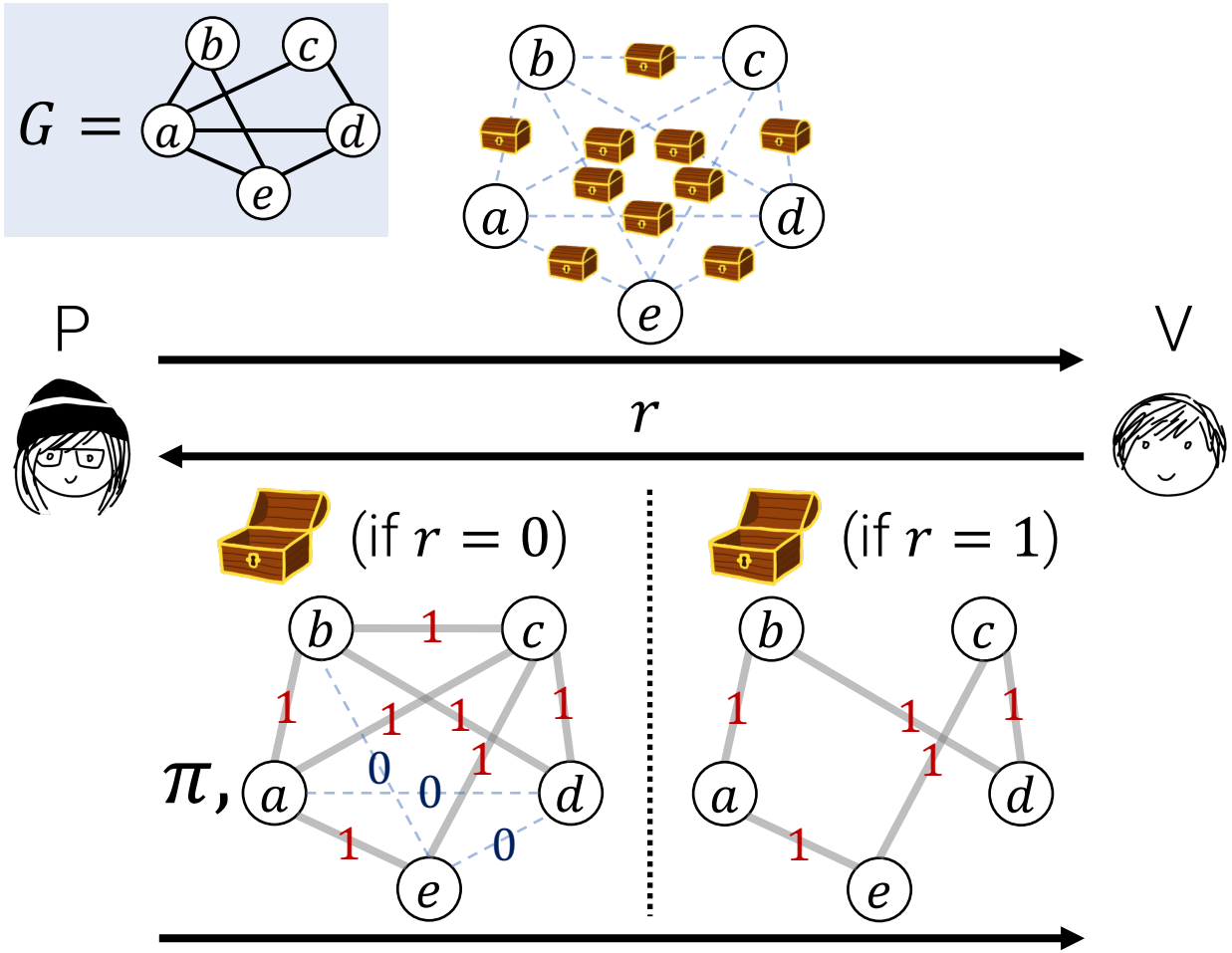



## Proof of knowledge (intuition)

By ***binding***, the first message determines a graph $H$ such that:

- $H$ is a permutation of $G$
- $H$ contains a Ham cycle

## Blum's Protocol for Hamiltonian Cycle




## Proof of knowledge (intuition)

By ***binding***, the first message determines a graph $H$ such that:

- $H$ is a permutation of $G$
- $H$ contains a Ham cycle

## Zero knowledge (intuition)

First message reveals nothing since commitments are ***hiding***.

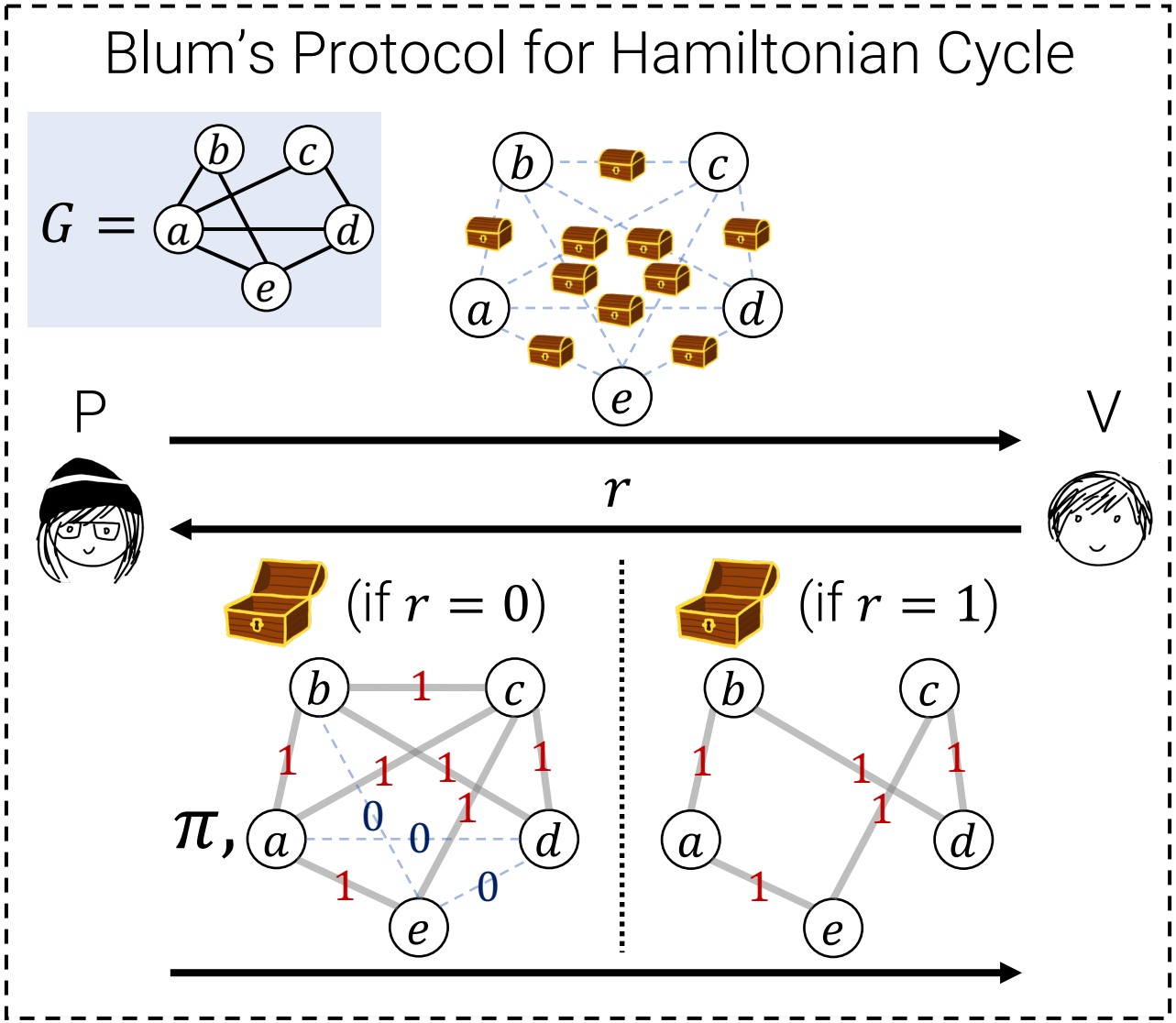
Last message also reveals nothing:

- $(r = 0)$ random permutation of $G$
- $(r = 1)$ random cycle

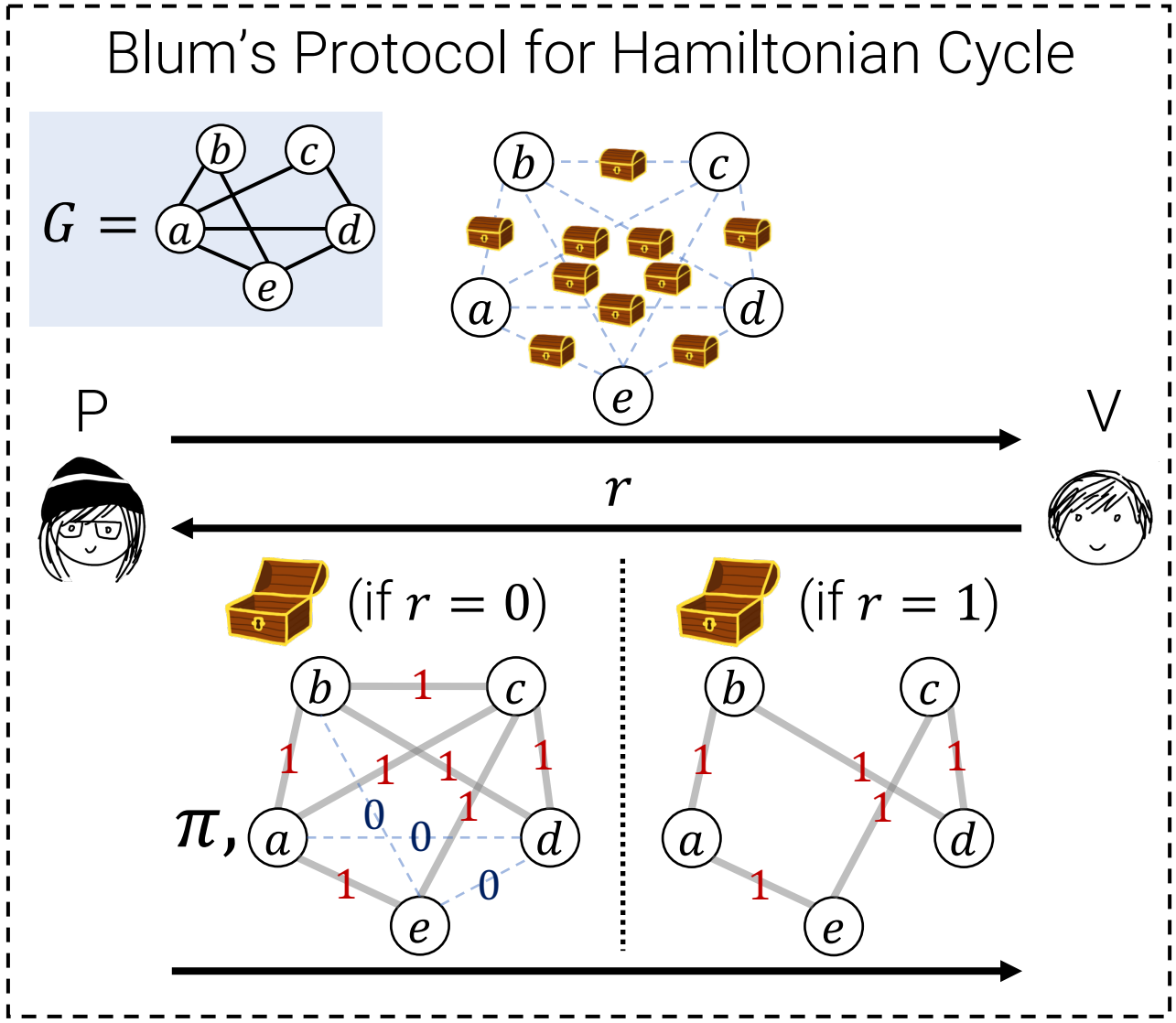
# What this talk will cover:

1. Is LWE all we need for post-quantum security? ✓
2. Review: Blum's Hamiltonicity protocol ✓
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge
   - Watrous's ZK rewinding lemma

# Classical Proof of Knowledge



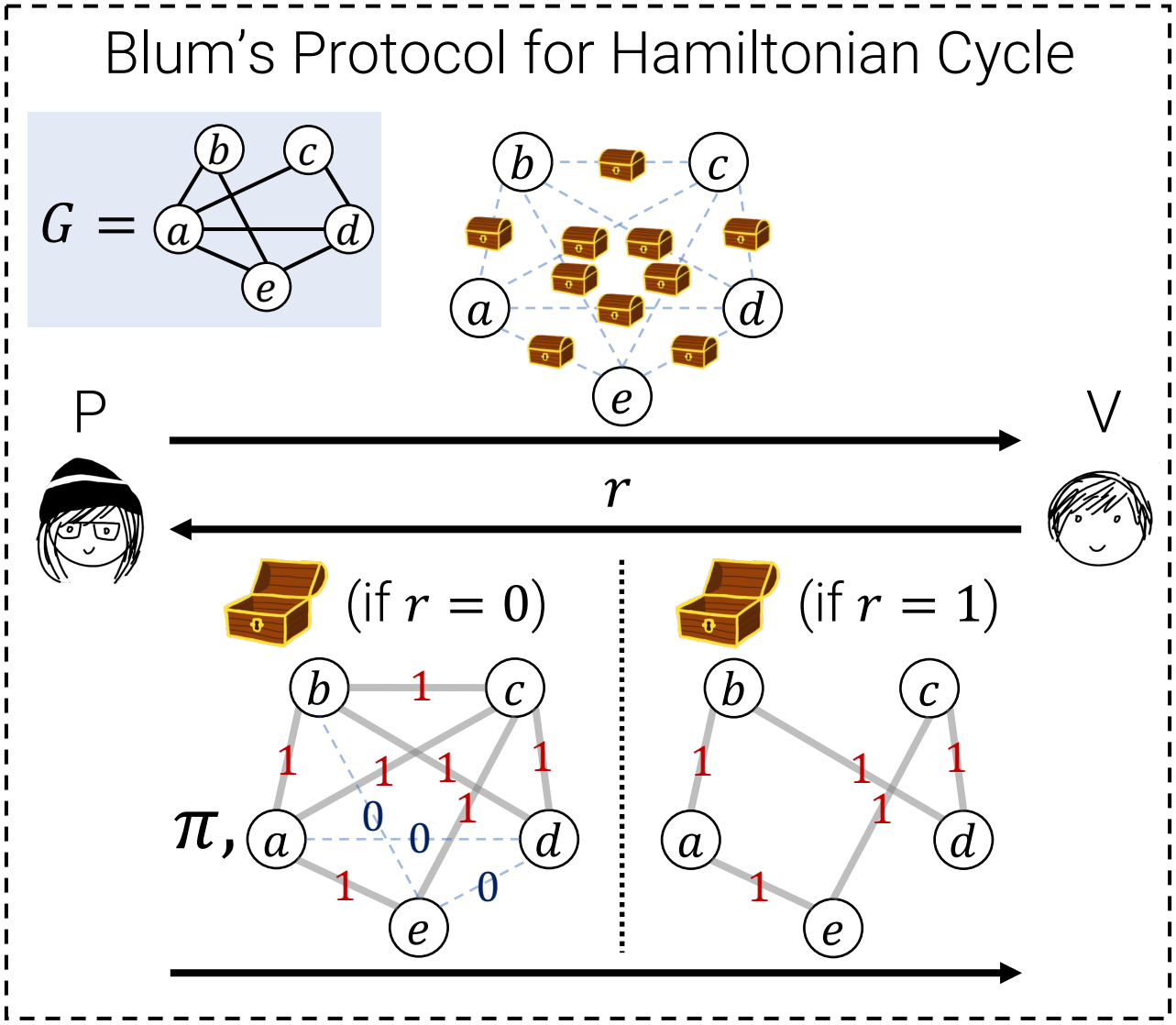

**PoK:** If efficient classical $P^*$ convinces $V$ with prob $\frac{1}{2} + \varepsilon$, then we can extract a witness from $P^*$.




# Classical Proof of Knowledge

**PoK:** If efficient classical $P^*$ convinces $V$ with prob $\frac{1}{2} + \varepsilon$, then we can extract a witness from $P^*$.

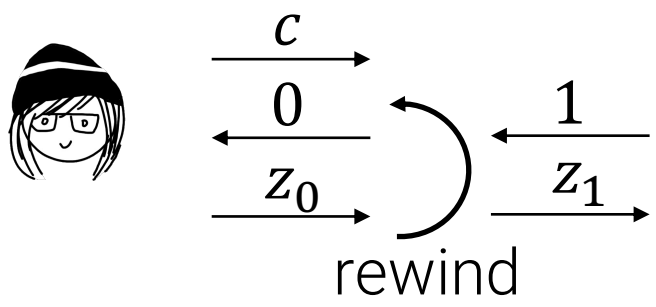
**Rewinding:** query $P^*$ repeatedly (on random $r$) until it answers successfully on $r = 0$ and $1$.

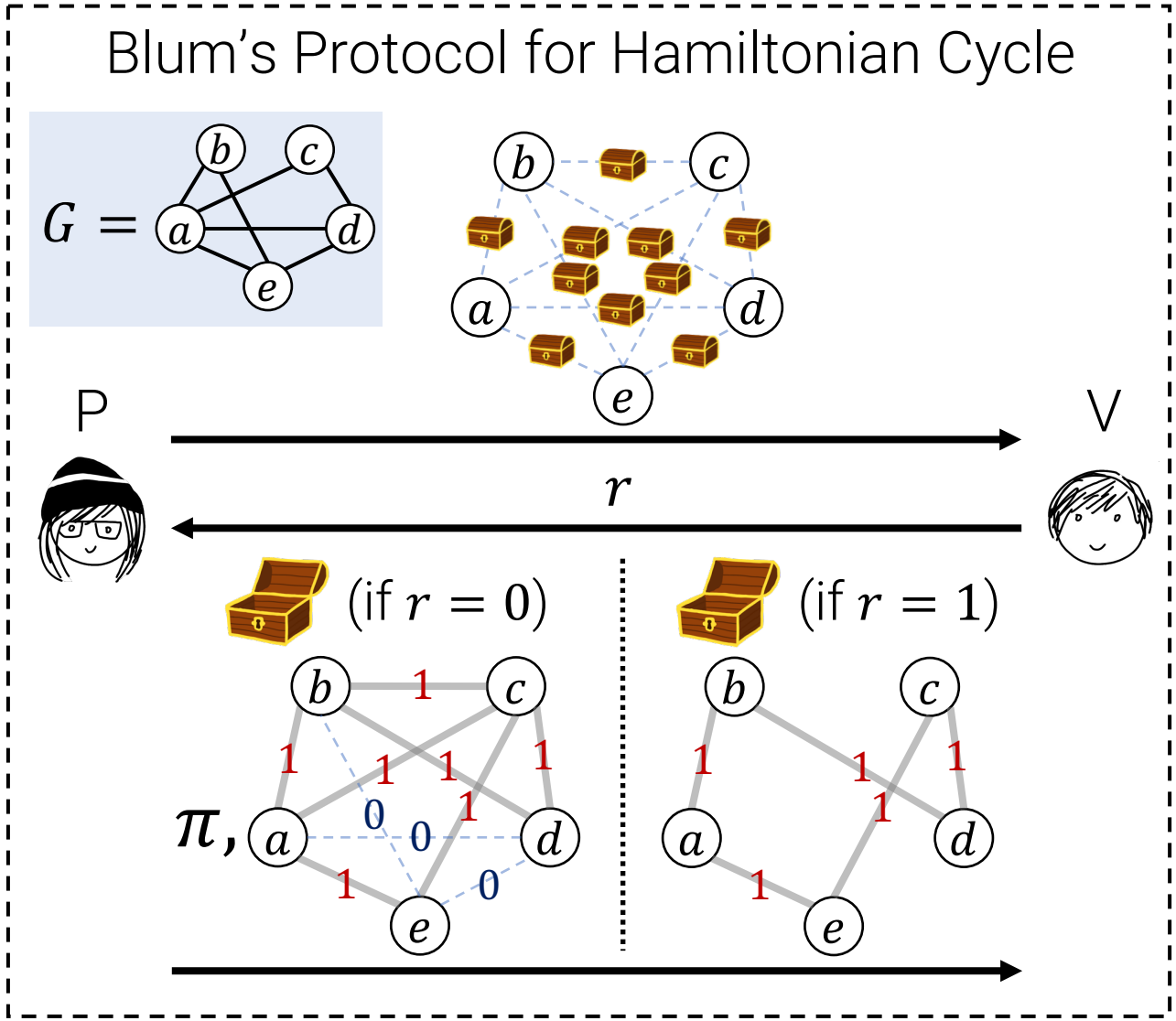



# Classical Proof of Knowledge

**PoK:** If efficient classical $P^*$ convinces $V$ with prob $\frac{1}{2} + \varepsilon$, then we can extract a witness from $P^*$.

**Rewinding:** query $P^*$ repeatedly (on random $r$) until it answers successfully on $r = 0$ and $1$.

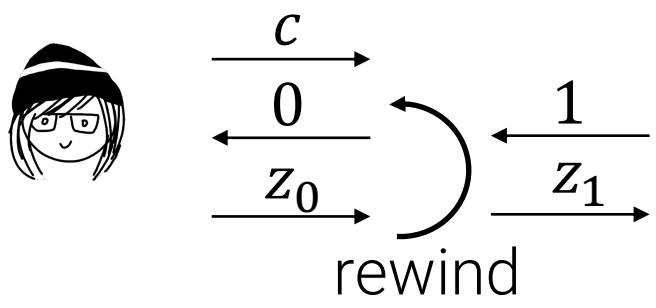




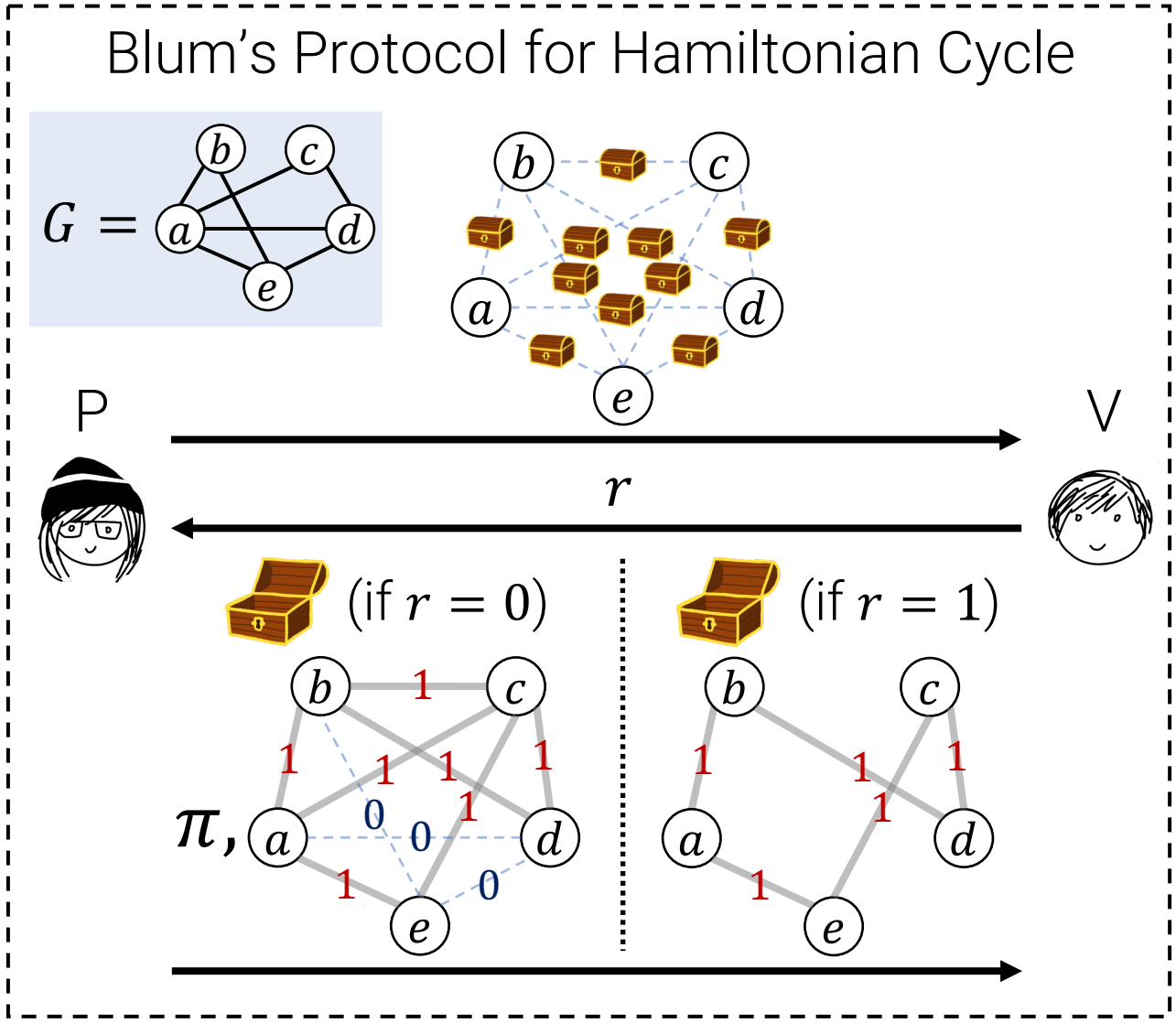

# Classical Proof of Knowledge

**PoK:** If efficient classical $P^*$ convinces $V$ with prob $\frac{1}{2} + \varepsilon$, then we can extract a witness from $P^*$.

**Rewinding:** query $P^*$ repeatedly (on random $r$) until it answers successfully on $r = 0$ and $1$.



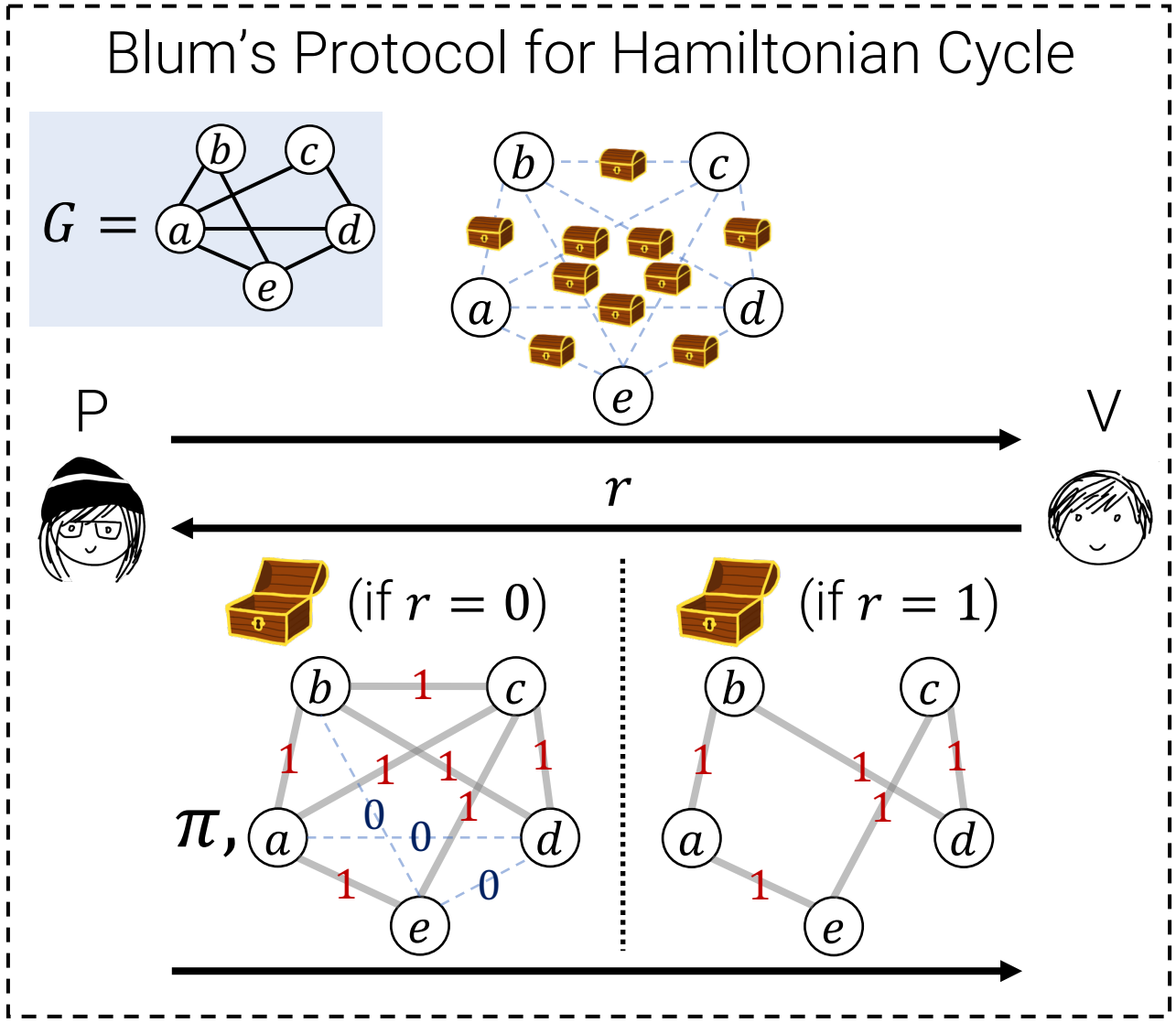

Get two accepting transcripts after $O\left(\frac{1}{\varepsilon}\right)$ rewinds.




# Classical Proof of Knowledge

**PoK:** If efficient classical $P^*$ convinces $V$ with prob $\frac{1}{2} + \varepsilon$, then we can extract a witness from $P^*$.

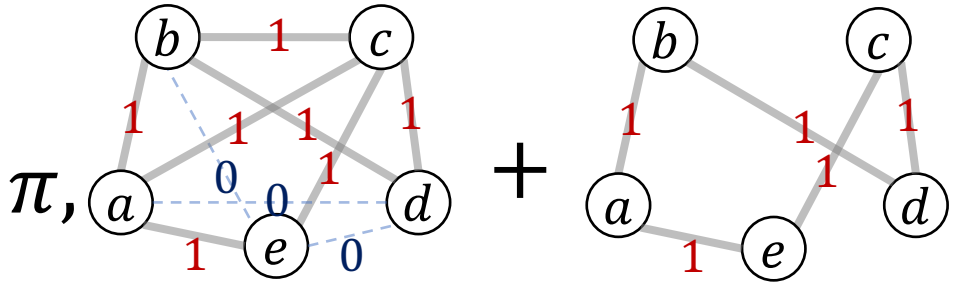
**Observation:** two accepting transcripts → Ham cycle (unless $P^*$ breaks binding)

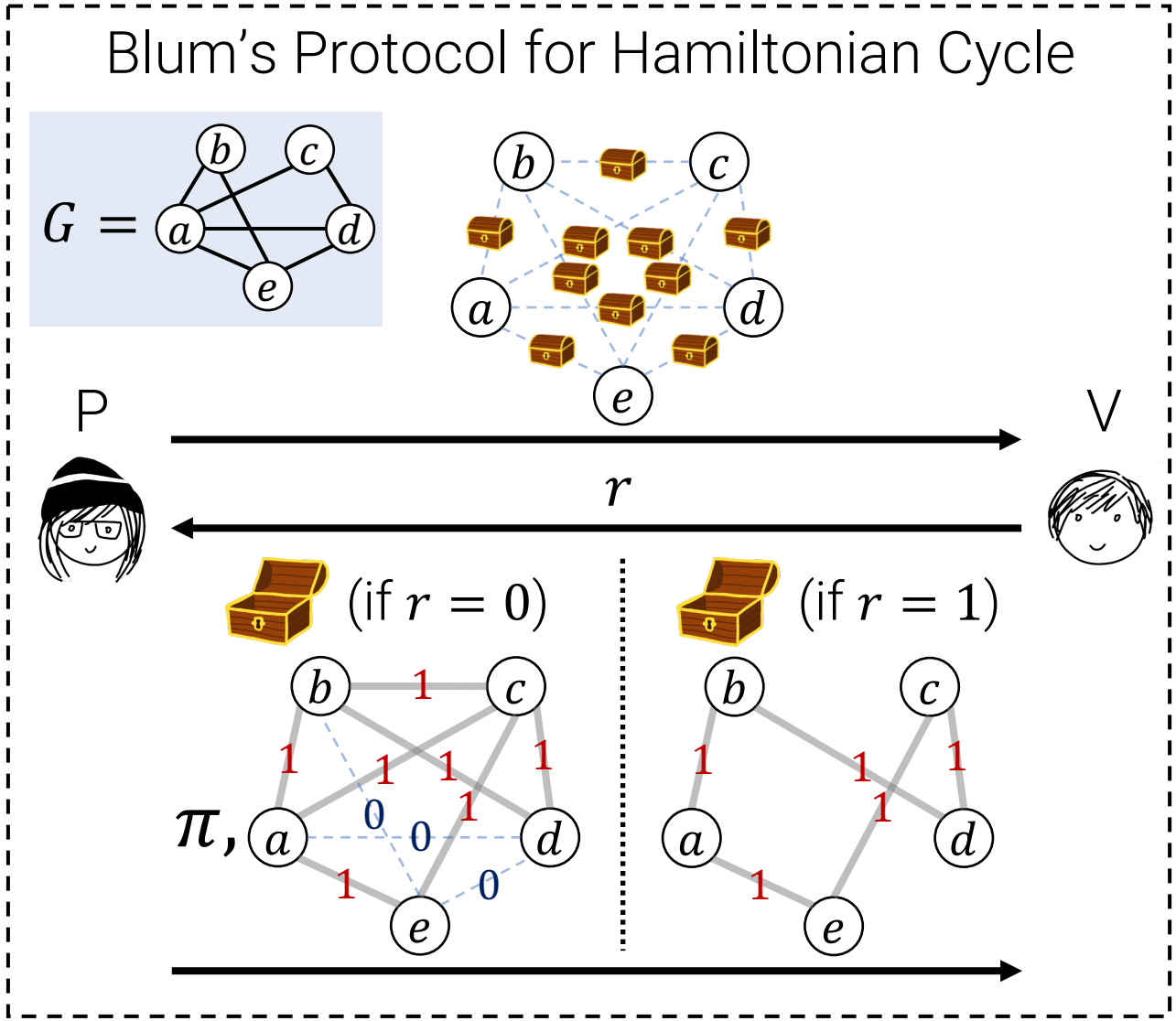



# Classical Proof of Knowledge

**PoK**: If efficient classical $P^*$ convinces $V$ with prob $\frac{1}{2} + \varepsilon$, then we can extract a witness from $P^*$.

**Observation**: two accepting transcripts → Ham cycle (unless $P^*$ breaks binding)

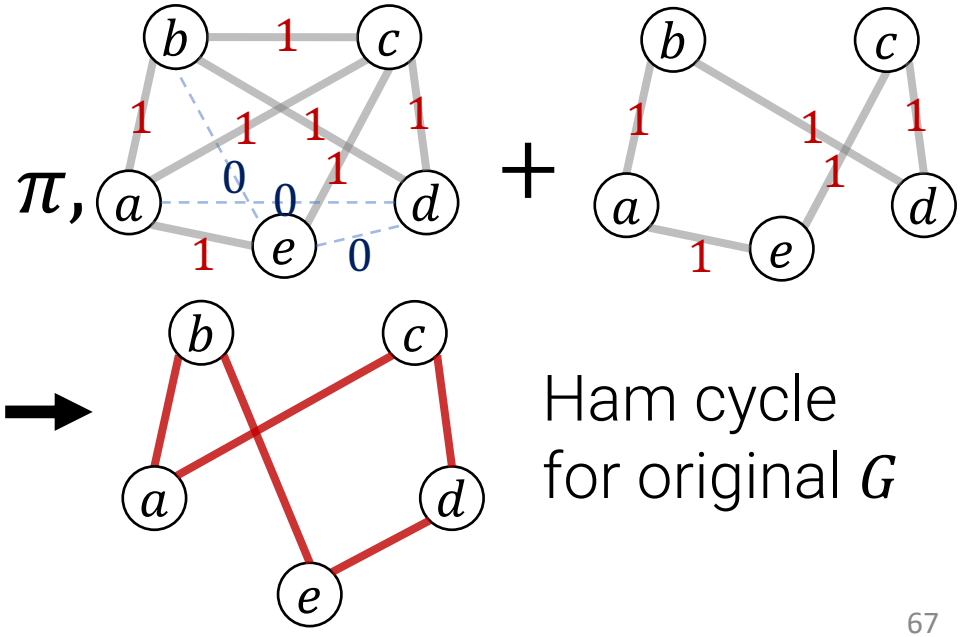





# Classical Proof of Knowledge

**PoK**: If efficient classical $P^*$ convinces $V$ with prob $\frac{1}{2} + \varepsilon$, then we can extract a witness from $P^*$.

**Observation**: two accepting transcripts → Ham cycle (unless $P^*$ breaks binding)



# What this talk will cover:

1. Is LWE all we need for post-quantum security? ✓
2. Review: Blum's Hamiltonicity protocol ✓
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge ✓
   - How to define post-quantum commitments
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge
   - Watrous's ZK rewinding lemma

# Binding Against Quantum Attack

Classical PoK for Blum relies on the binding property of the commitments.

# Binding Against Quantum Attack

Classical PoK for Blum relies on the binding property of the commitments.
But for quantum attackers, we'll need to revisit the ***definition*** of binding.

# Binding Against Quantum Attack

Classical PoK for Blum relies on the binding property of the commitments.
But for quantum attackers, we'll need to revisit the ***definition*** of binding.

Commitment Syntax

sender

$ck$ ←

receiver

$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$ →

$m, d$ →

Accept if
$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$.

# Binding Against Quantum Attack

Classical PoK for Blum relies on the binding property of the commitments.
But for quantum attackers, we'll need to revisit the ***definition*** of binding.

Commitment Syntax


sender

$ck$ ←

receiver


$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$ →

$m, d$ →

Accept if
$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$.

**Classical definition:**
PPT adversary can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

# Binding Against Quantum Attack

Classical PoK for Blum relies on the binding property of the commitments.
But for quantum attackers, we'll need to revisit the ***definition*** of binding.

Commitment Syntax


sender

$ck$ ←

receiver


$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$ →

$m, d$ →

Accept if
$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$.

**Classical definition:**
PPT adversary can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

Can we just replace PPT with QPT?

# Binding Against Quantum Attack

Classical PoK for Blum relies on the binding property of the commitments.
But for quantum attackers, we'll need to revisit the ***definition*** of binding.

Commitment Syntax


sender

$ck$ ←

receiver


$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$ →

$m, d$ →

Accept if
$\mathrm{com} = \mathrm{Com}_{ck}(m; d)$.

**Classical definition:**
PPT adversary can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

Can we just replace PPT with QPT?

[ARU14]: No!

# What's wrong with this definition?

Naïve post-quantum binding def:

QPT attacker can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

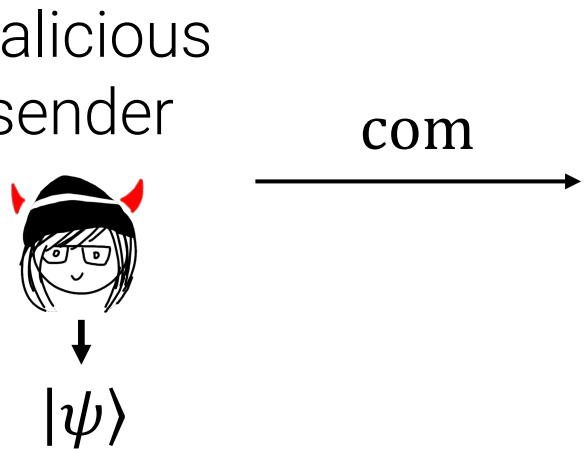
# What's wrong with this definition?

**Naïve post-quantum binding def:**

QPT attacker can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

[ARU14]: Quantum attacker* might produce $\mathbf{com}, |\psi\rangle$ such that:

- Can use $|\psi\rangle$ to open $\mathbf{com}$ to any $m$



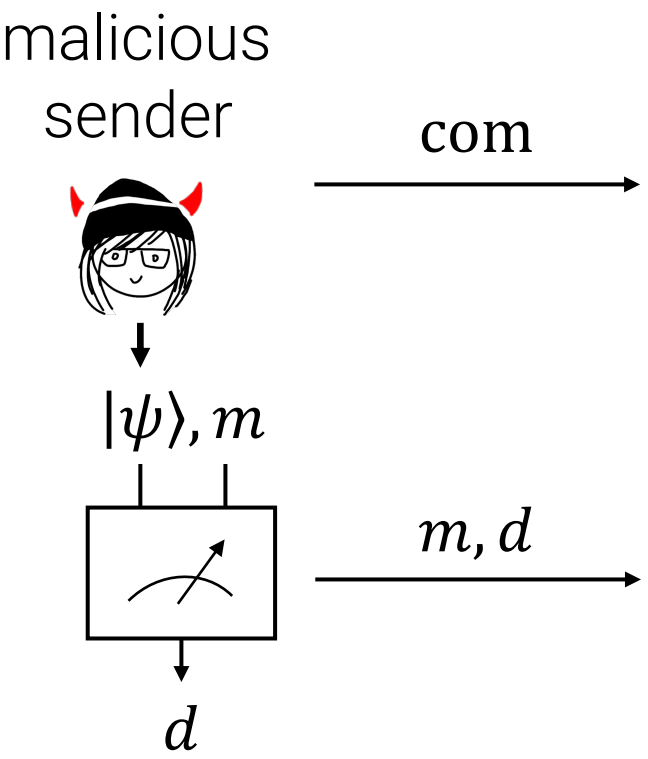
# What's wrong with this definition?

**Naïve post-quantum binding def:**

QPT attacker can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

[ARU14]: Quantum attacker* might produce $\mathbf{com}, |\psi\rangle$ such that:

- Can use $|\psi\rangle$ to open $\mathbf{com}$ to any $m$



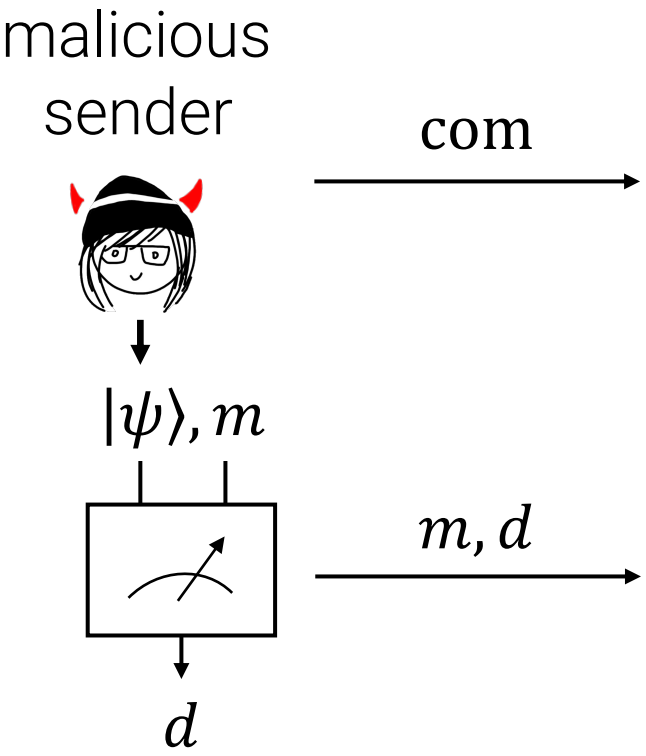
# What's wrong with this definition?

**Naïve post-quantum binding def:**

QPT attacker can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

[ARU14]: Quantum attacker* might produce $\mathbf{com}, |\psi\rangle$ such that:

- Can use $|\psi\rangle$ to open $\mathbf{com}$ to any $m$
- But can only do this once!



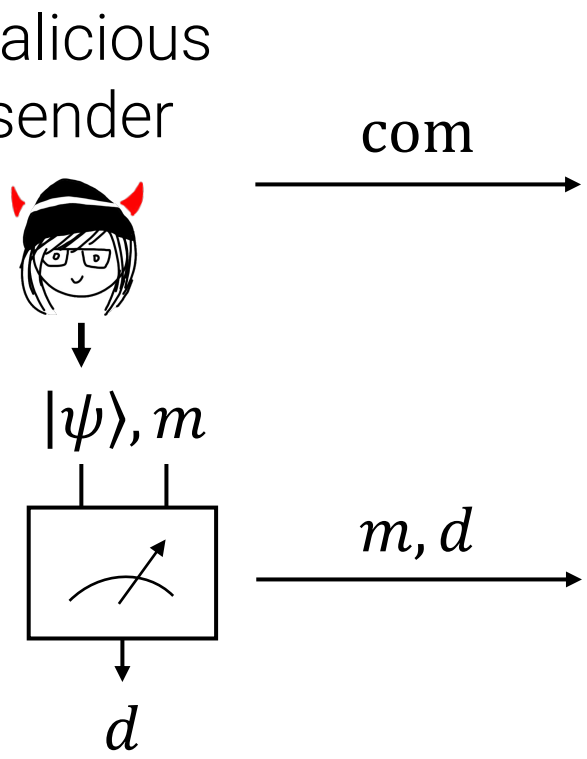
# What's wrong with this definition?

**Naïve post-quantum binding def:**

QPT attacker can't output $\mathbf{com}$ and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

[ARU14]: Quantum attacker* might produce $\mathbf{com}, |\psi\rangle$ such that:

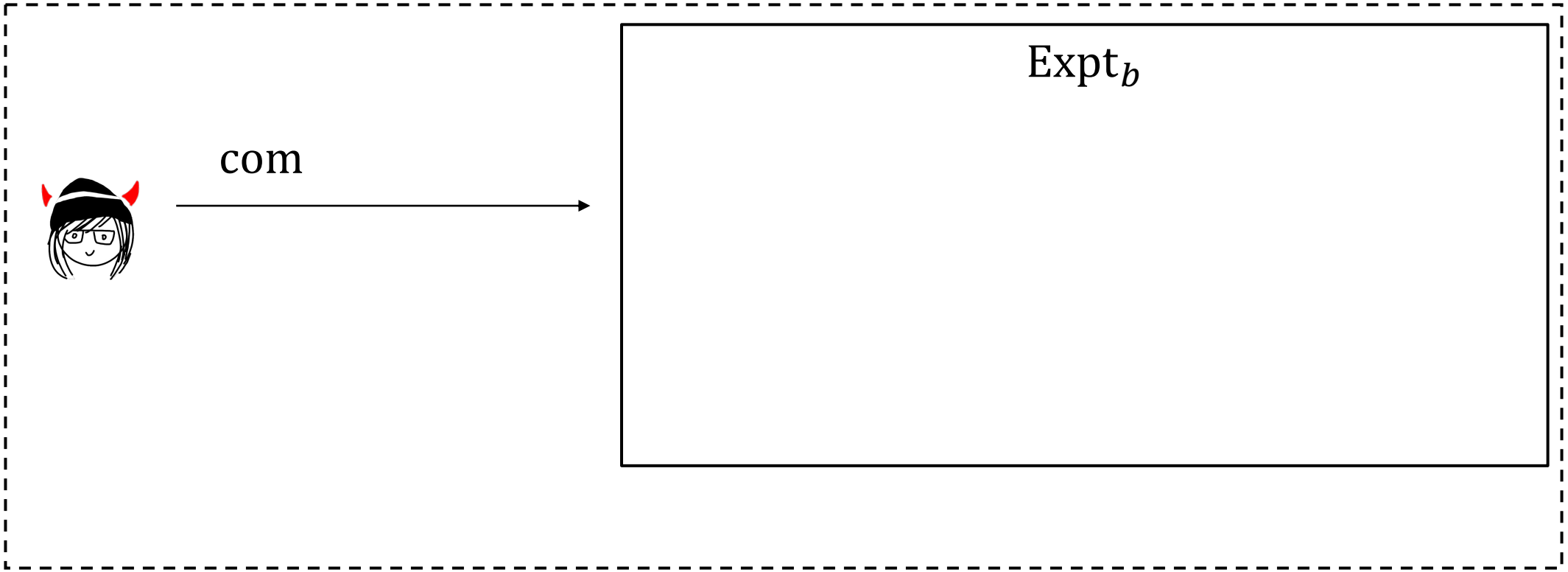
- Can use $|\psi\rangle$ to open $\mathbf{com}$ to any $m$
- But can only do this once!




*Caveat: assuming a quantum oracle

**Open: construct example without oracles

# A Better Definition: Collapse-Binding [Unruh16]



# A Better Definition: Collapse-Binding [Unruh16]

$\text{com}, \sum |m\rangle_M |d\rangle_D$

$\text{Expt}_b$

# A Better Definition: Collapse-Binding [Unruh16]

$\text{com}, \sum |m\rangle_M |d\rangle_D$

$\text{Expt}_b$

Run verifier in superposition on $M, D$ and measure its output (accept or reject); abort if reject.

# A Better Definition: Collapse-Binding [Unruh16]

$\text{com}, \sum |m\rangle_M |d\rangle_D$

$\text{Expt}_b$

Run verifier in superposition on $M, D$ and measure its output (accept or reject); abort if reject. On accept, state looks like $\sum_{\text{Com}(m,d)=\text{com}} |m\rangle_M |d\rangle_D$.

# A Better Definition: Collapse-Binding [Unruh16]

$\mathrm{com}, \sum |m\rangle_M |d\rangle_D$

**$\mathrm{Expt}_b$**

Run verifier in superposition on $M, D$ and measure its output (accept or reject); abort if reject. On accept, state looks like $\sum_{\mathrm{Com}(m,d)=\mathrm{com}} |m\rangle_M |d\rangle_D$.

- If $b = 0$: return $M, D$.
- If $b = 1$: measure $M$ and return $M, D$.

# A Better Definition: Collapse-Binding [Unruh16]

$\mathrm{com}, \sum |m\rangle_M |d\rangle_D$ →

← $M, D$

**$\mathrm{Expt}_b$**

Run verifier in superposition on $M, D$ and measure its output (accept or reject); abort if reject. On accept, state looks like $\sum_{\mathrm{Com}(m,d)=\mathrm{com}} |m\rangle_M |d\rangle_D$.

- If $b = 0$: return $M, D$.
- If $b = 1$: measure $M$ and return $M, D$.

# A Better Definition: Collapse-Binding [Unruh16]

$\mathrm{com}, \sum |m\rangle_M |d\rangle_D$ →

← $M, D$

**$\mathrm{Expt}_b$**

Run verifier in superposition on $M, D$ and measure its output (accept or reject); abort if reject. On accept, state looks like $\sum_{\mathrm{Com}(m,d)=\mathrm{com}} |m\rangle_M |d\rangle_D$.

- If $b = 0$: return $M, D$.
- If $b = 1$: measure $M$ and return $M, D$.

Collapse-binding: $\mathrm{Expt}_0 \approx_C \mathrm{Expt}_1$

# A Better Definition: Collapse-Binding [Unruh16]

$\mathbf{com}, \sum |m\rangle_M |d\rangle_D$ →

← $M, D$

**$\mathbf{Expt}_b$**

Run verifier in superposition on $M, D$ and measure its output (accept or reject); abort if reject. On accept, state looks like $\sum_{\mathbf{Com}(m,d)=\mathbf{com}} |m\rangle_M |d\rangle_D$.

- If $b = 0$: return $M, D$.
- If $b = 1$: measure $M$ and return $M, D$.

Collapse-binding: $\mathbf{Expt}_0 \approx_c \mathbf{Expt}_1$

**Intuition:** if $\mathbf{Com}$ is perfectly binding, $\mathbf{Expt}_0$ and $\mathbf{Expt}_1$ are perfectly indistinguishable since there is only one valid $m$ for any $\mathbf{com}$.

# A Better Definition: Collapse-Binding [Unruh16]

$\mathrm{com}, \sum |m\rangle_M |d\rangle_D$ →

← $M, D$

**$\mathrm{Expt}_b$**

Run verifier in superposition on $M, D$ and measure its output (accept or reject); abort if reject. On accept, state looks like $\sum_{\mathrm{Com}(m,d)=\mathrm{com}} |m\rangle_M |d\rangle_D$.

- If $b = 0$: return $M, D$.
- If $b = 1$: measure $M$ and return $M, D$.

Collapse-binding: $\mathrm{Expt}_0 \approx_C \mathrm{Expt}_1$

**Intuition:** if $\mathrm{Com}$ is perfectly binding, $\mathrm{Expt}_0$ and $\mathrm{Expt}_1$ are perfectly indistinguishable since there is only one valid $m$ for any $\mathrm{com}$. Collapse-binding asks for a computational version of this property.

$\mathbf{com}, \sum |m\rangle_M |d\rangle_D$

$M, D$

$\mathbf{Expt}_b$

Check if $M, D$ is valid for $\mathbf{com}$; abort if not.

- If $b = 0$, return $M, D$.
- If $b = 1$, measure $M$ and return $M, D$.

Collapse-binding: $\mathbf{Expt}_0 \approx_c \mathbf{Expt}_1$

Why this definition?

$\mathbf{com}, \sum |m\rangle_M |d\rangle_D$

$M, D$

$\mathbf{Expt}_b$

Check if $M, D$ is valid for $\mathbf{com}$; abort if not.

- If $b = 0$, return $M, D$.
- If $b = 1$, measure $M$ and return $M, D$.

Collapse-binding: $\mathbf{Expt}_0 \approx_c \mathbf{Expt}_1$

# Why this definition?

- Many good reasons: avoids [ARU14] attack, implies other proposed definitions, composable, easy to construct (implied by LWE), etc.

$\mathbf{com}, \sum |m\rangle_M |d\rangle_D$

$M, D$

$\mathbf{Expt}_b$

Check if $M, D$ is valid for $\mathbf{com}$; abort if not.

- If $b = 0$, return $M, D$.
- If $b = 1$, measure $M$ and return $M, D$.

Collapse-binding: $\mathbf{Expt}_0 \approx_c \mathbf{Expt}_1$

# Why this definition?

- Many good reasons: avoids [ARU14] attack, implies other proposed definitions, composable, easy to construct (implied by LWE), etc.
- But most importantly, this definition makes rewinding possible!

$\mathbf{com}, \sum |m\rangle_M |d\rangle_D$

$M, D$

$\mathbf{Expt}_b$

Check if $M, D$ is valid for $\mathbf{com}$; abort if not.

- If $b = 0$, return $M, D$.
- If $b = 1$, measure $M$ and return $M, D$.

Collapse-binding: $\mathbf{Expt}_0 \approx_c \mathbf{Expt}_1$

# Why this definition?

- Many good reasons: avoids [ARU14] attack, implies other proposed definitions, composable, easy to construct (implied by LWE), etc.
- But most importantly, this definition makes rewinding possible!

[U12,U16]: Blum is a post-quantum PoK if the underlying commitments are collapse-binding.*

$\mathbf{com}, \sum |m\rangle_M |d\rangle_D$

$M, D$

$\mathbf{Expt}_b$

Check if $M, D$ is valid for $\mathbf{com}$; abort if not.

- If $b = 0$, return $M, D$.
- If $b = 1$, measure $M$ and return $M, D$.

Collapse-binding: $\mathbf{Expt}_0 \approx_c \mathbf{Expt}_1$

# Why this definition?

- Many good reasons: avoids [ARU14] attack, implies other proposed definitions, composable, easy to construct (implied by LWE), etc.
- But most importantly, this definition makes rewinding possible!

[U12,U16]: Blum is a post-quantum PoK if the underlying commitments are collapse-binding.*

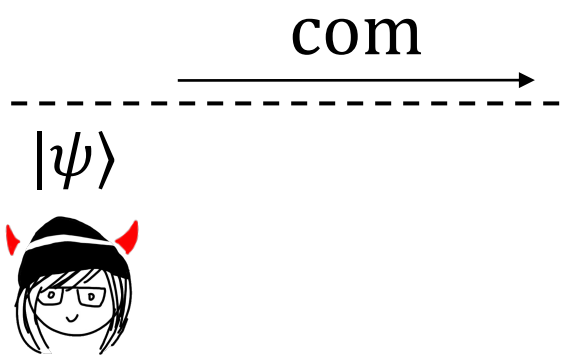
*[U12,U16] analyze a slightly modified version of Blum's protocol, but later on [LMS22] showed the original Blum protocol is post-quantum secure.

# What this talk will cover:

1. Is LWE all we need for post-quantum security? ✓
2. Review: Blum's Hamiltonicity protocol ✓
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge ✓
   - How to define post-quantum commitments ✓
   - Unruh's 1-bit rewinding lemma
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge
   - Watrous's ZK rewinding lemma

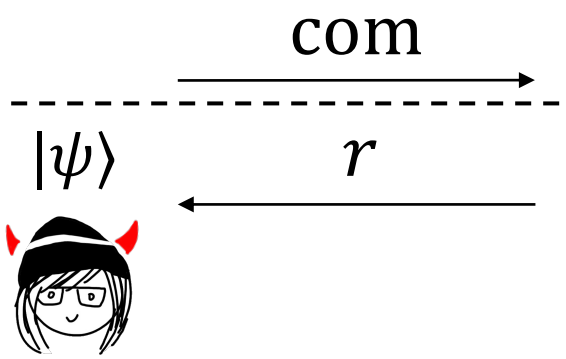
# How do collapse-binding commitments help with rewinding?

# How do collapse-binding commitments help with rewinding?



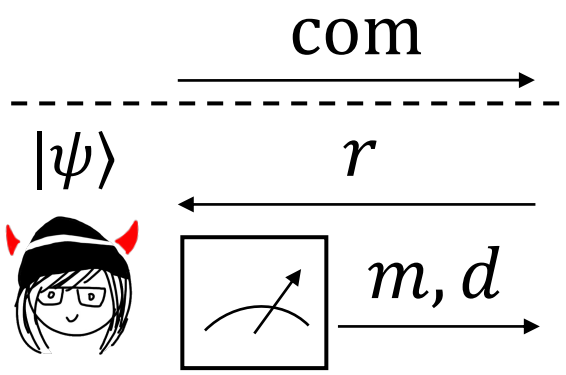

- Difficulty: recording response disturbs adversary's state.

# How do collapse-binding commitments help with rewinding?



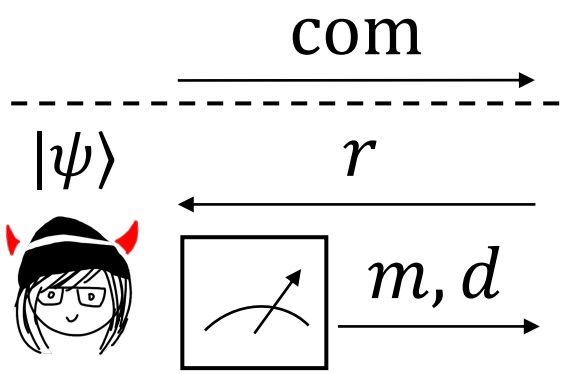

- Difficulty: recording response disturbs adversary's state.

# How do collapse-binding commitments help with rewinding?



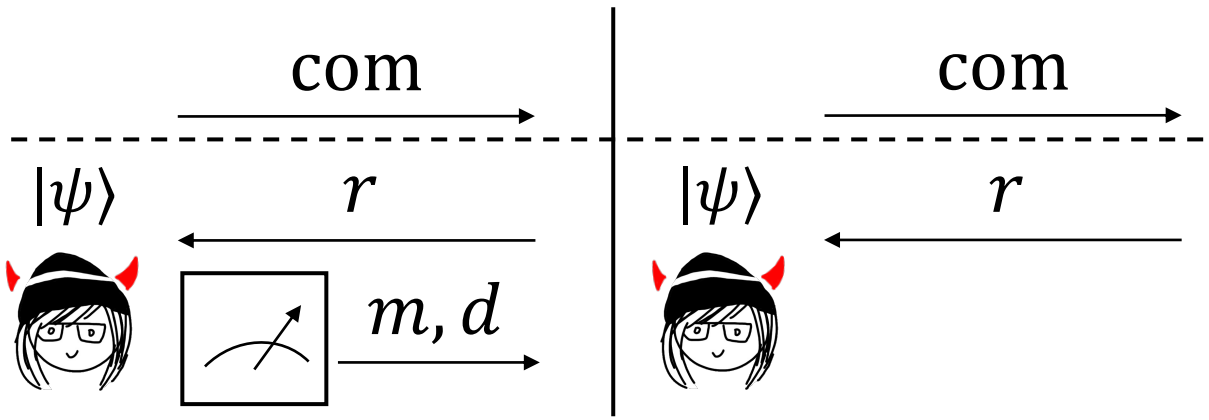

- Difficulty: recording response disturbs adversary's state.

# How do collapse-binding commitments help with rewinding?




- Difficulty: recording response disturbs adversary's state.
- But if the response is the opening to a collapse-binding commitment, we can "lazily" measure $m$.

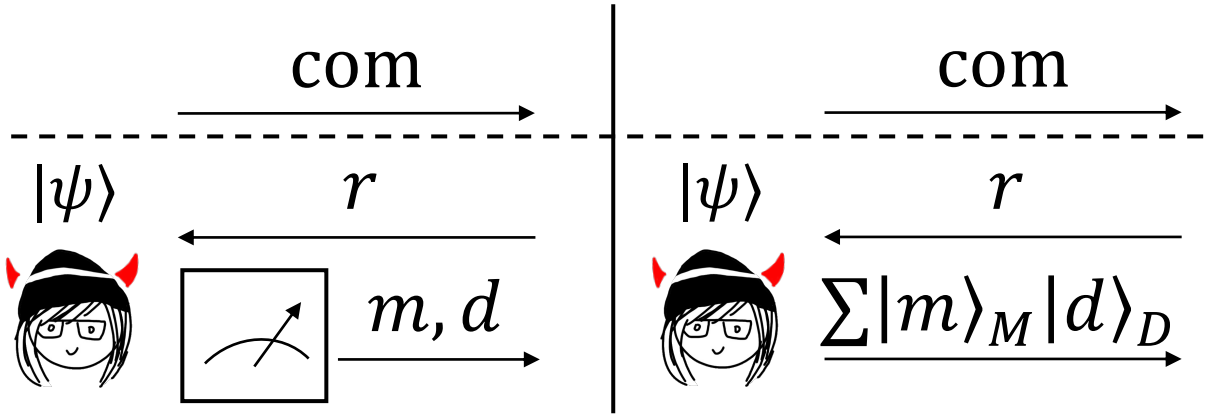
# How do collapse-binding commitments help with rewinding?




"Lazy" Measurement:

- Difficulty: recording response disturbs adversary's state.
- But if the response is the opening to a collapse-binding commitment, we can "lazily" measure $m$.

# How do collapse-binding commitments help with rewinding?

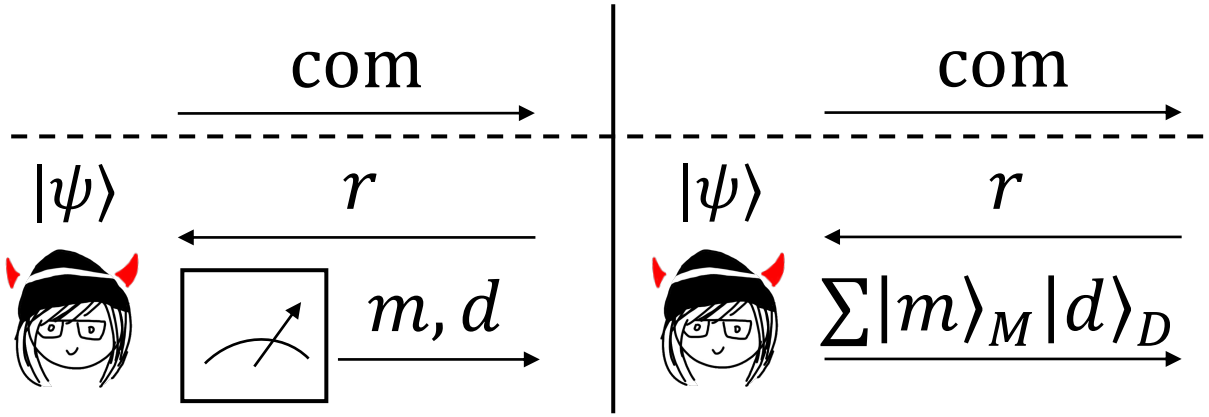



**"Lazy" Measurement:**

(1) Run adversary's unitary to generate superposition of responses on registers $M, D$.

- Difficulty: recording response disturbs adversary's state.
- But if the response is the opening to a collapse-binding commitment, we can "lazily" measure $m$.

# How do collapse-binding commitments help with rewinding?



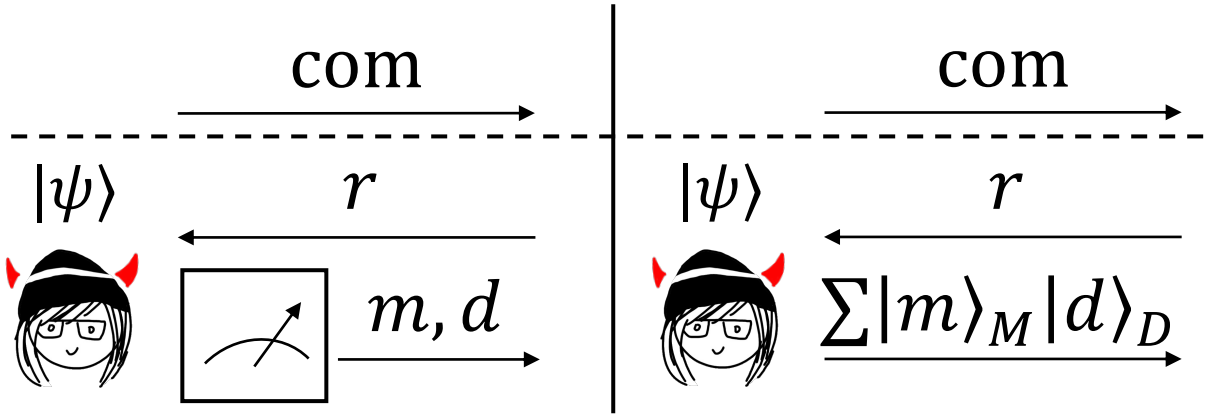

**"Lazy" Measurement:**

(1) Run adversary's unitary to generate superposition of responses on registers $M, D$.

(2) Check if $M, D$ is valid.

- Difficulty: recording response disturbs adversary's state.
- But if the response is the opening to a collapse-binding commitment, we can "lazily" measure $m$.

# How do collapse-binding commitments help with rewinding?




**"Lazy" Measurement:**

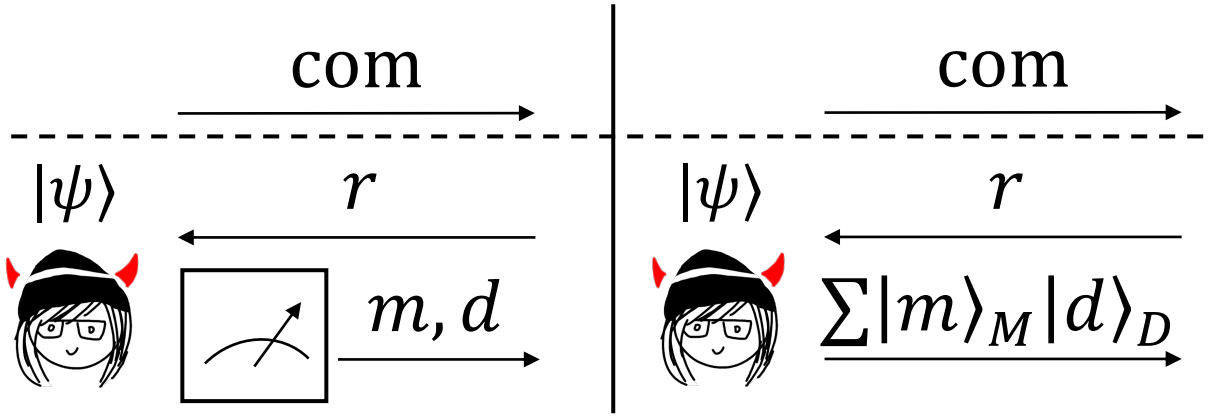
(1) Run adversary's unitary to generate superposition of responses on registers $M, D$.

(2) Check if $M, D$ is valid.

(3) If so, measure $M$.

- Difficulty: recording response disturbs adversary's state.
- But if the response is the opening to a collapse-binding commitment, we can "lazily" measure $m$.

# How do collapse-binding commitments help with rewinding?




**"Lazy" Measurement:**

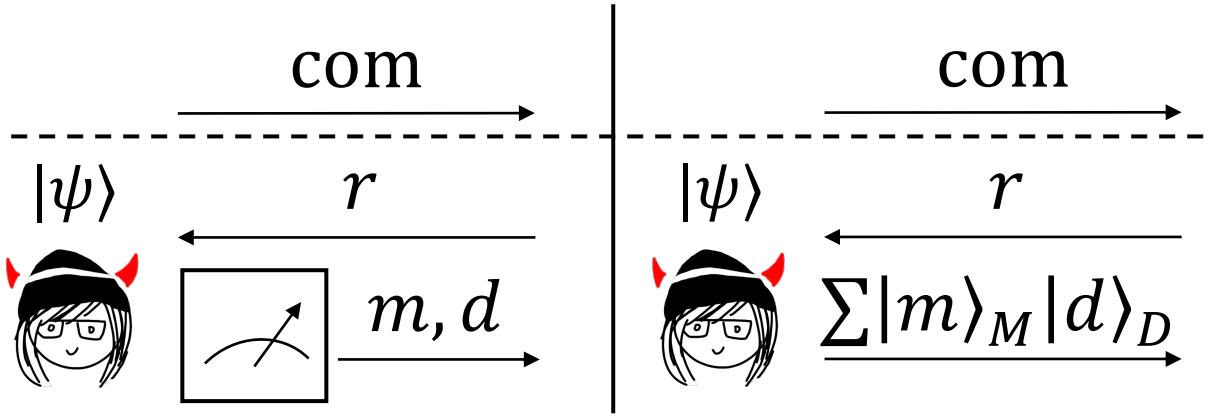
(1) Run adversary's unitary to generate superposition of responses on registers $M, D$.

(2) Check if $M, D$ is valid.

(3) If so, measure $M$.

- Difficulty: recording response disturbs adversary's state.
- But if the response is the opening to a collapse-binding commitment, we can "lazily" measure $m$. Collapse-binding guarantees that step (3) is computationally undetectable!

# How do collapse-binding commitments help with rewinding?




**"Lazy" Measurement:**

(1) Run adversary's unitary to generate superposition of responses on registers $M, D$.

(2) Check if $M, D$ is valid.

(3) If so, measure $M$.

- Difficulty: recording response disturbs adversary's state.
- But if the response is the opening to a collapse-binding commitment, we can "lazily" measure $m$. Collapse-binding guarantees that step (3) is computationally undetectable!

**Key point:** with collapse-binding commitments, we just need to consider measuring the 1-bit decision (accept/reject).

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\||\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.

Aside: $\Pi_r = U_r^\dagger\left(\sum_{\mathrm{Ver}(m,d)=1}|m,d\rangle\langle m,d|\right)U_r$ where $U_r$ is the adversary's unitary for challenge $r$.

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.
- If adversary's state is $|\psi\rangle$, its success probability is $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$.

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

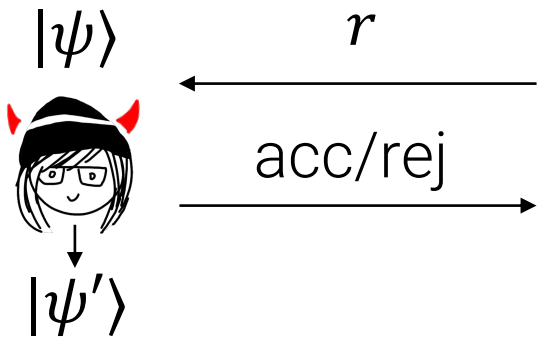
- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.
- If adversary's state is $|\psi\rangle$, its success probability is $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$.

By [U12], if we run the adversary on ***two*** random challenges, it succeeds ***twice*** w/ prob $\geq p^3$.

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.
- If adversary's state is $|\psi\rangle$, its success probability is $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$.

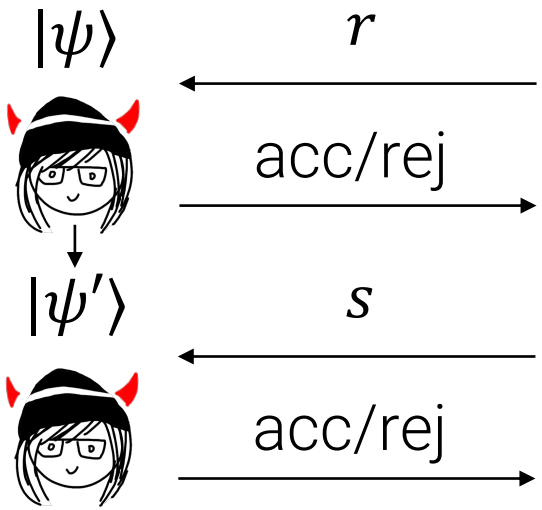
By [U12], if we run the adversary on ***two*** random challenges, it succeeds ***twice*** w/ prob $\geq p^3$.



**1-bit Rewinding Lemma [Unruh12]:** For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\||\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.
- If adversary's state is $|\psi\rangle$, its success probability is $p = \mathbb{E}_{r\leftarrow R}\||\Pi_r|\psi\rangle\|^2$.

By [U12], if we run the adversary on ***two*** random challenges, it succeeds ***twice*** w/ prob $\geq p^3$.

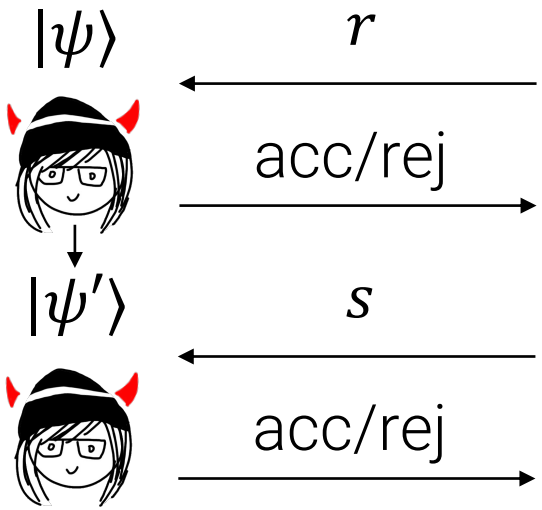


**1-bit Rewinding Lemma [Unruh12]:** For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\||\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.
- If adversary's state is $|\psi\rangle$, its success probability is $p = \mathbb{E}_{r\leftarrow R}\||\Pi_r|\psi\rangle\|^2$.

By [U12], if we run the adversary on ***two*** random challenges, it succeeds ***twice*** w/ prob $\geq p^3$.

If adversary is opening a collapse-binding commitment, then we record two accepting transcripts w/ prob $\geq p^3$.

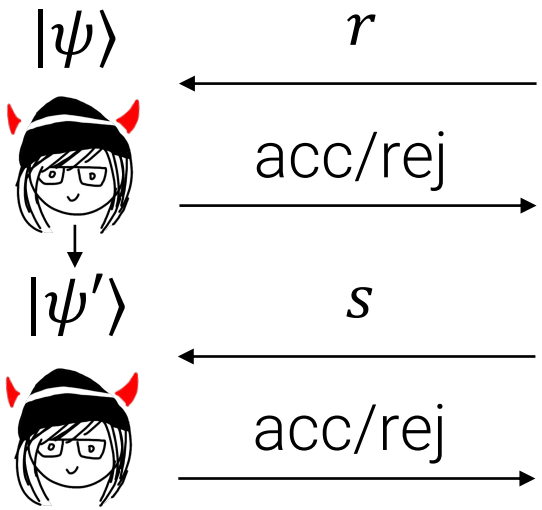


**1-bit Rewinding Lemma [Unruh12]:** For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

- Define $(\Pi_r, \mathbb{I} - \Pi_r)$ to measure whether adversary succeeds on $r$.
- If adversary's state is $|\psi\rangle$, its success probability is $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$.

By [U12], if we run the adversary on ***two*** random challenges, it succeeds ***twice*** w/ prob $\geq p^3$.

If adversary is opening a collapse-binding commitment, then we record two accepting transcripts w/ prob $\geq p^3$.




**Annoying detail:** this is only useful if $r \neq s$. For Blum ($R = \{0,1\}$), we only extract a witness with $\Omega(\varepsilon)$ probability when $p \geq 1/\sqrt{2} + \varepsilon$.

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

We won't prove this lemma, but it is reminiscent of "gentle measurement":

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\||\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

We won't prove this lemma, but it is reminiscent of "gentle measurement":

- If $p$ is close to 1, then $\Pi_r|\psi\rangle$ is not too far from $|\psi\rangle$ (in expectation).

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

We won't prove this lemma, but it is reminiscent of "gentle measurement":

- If $p$ is close to 1, then $\Pi_r|\psi\rangle$ is not too far from $|\psi\rangle$ (in expectation). So if we perform another random measurement $(\Pi_s, \mathbb{I} - \Pi_s)$, it should still have a reasonable chance of accepting.

1-bit Rewinding Lemma [Unruh12]: For any state $|\psi\rangle$ and set of projectors $\{\Pi_r\}_{r\in R}$, if $p = \mathbb{E}_{r\leftarrow R}\|\Pi_r|\psi\rangle\|^2$, then $\mathbb{E}_{r\leftarrow R,s\leftarrow R}\|\Pi_s\Pi_r|\psi\rangle\|^2 \geq p^3$

We won't prove this lemma, but it is reminiscent of "gentle measurement":

- If $p$ is close to 1, then $\Pi_r|\psi\rangle$ is not too far from $|\psi\rangle$ (in expectation). So if we perform another random measurement $(\Pi_s, \mathbb{I} - \Pi_s)$, it should still have a reasonable chance of accepting.

(However, this bound is much stronger than a gentle measurement bound)

# Putting It Together

**Step 1: Collapsing commitments** [U16]:

recording adversary's response $\approx_c$ recording 1-bit decision

+

**Step 2: 1-bit-rewinding lemma** [U12]:

If we run a $p$-successful adversary on 2 random challenges (and only measure the 1-bit decision), then:

$$\Pr[\text{succeed twice}] \geq p^3$$

# Putting It Together

**Step 1: Collapsing commitments** [U16]:

recording adversary's response $\approx_c$ recording 1-bit decision

+

**Step 2: 1-bit-rewinding lemma** [U12]:

If we run a $p$-successful adversary on 2 random challenges (and only measure the 1-bit decision), then:

$$\Pr[\text{succeed twice}] \geq p^3$$

**Theorem:** If a quantum $P^*$ convinces $V$ to accept with probability $\geq 1/\sqrt{2} + \varepsilon$, we can extract a witness with probability $\Omega(\varepsilon)$.

# Putting It Together

**Step 1: Collapsing commitments** [U16]:

recording adversary's response $\approx_c$ recording 1-bit decision

+

**Step 2: 1-bit-rewinding lemma** [U12]:

If we run a $p$-successful adversary on 2 random challenges (and only measure the 1-bit decision), then:

$$\Pr[\text{succeed twice}] \geq p^3$$

**Theorem:** If a quantum $P^*$ convinces $V$ to accept with probability $\geq 1/\sqrt{2} + \varepsilon$, we can extract a witness with probability $\Omega(\varepsilon)$.

Remember that for classical $P^*$, we just need $1/2 + \varepsilon$, and we extract with probability $\approx 1$.

# Putting It Together

**Step 1: Collapsing commitments** [U16]:

recording adversary's response $\approx_c$ recording 1-bit decision

+

**Step 2: 1-bit-rewinding lemma** [U12]:

If we run a $p$-successful adversary on 2 random challenges (and only measure the 1-bit decision), then:

$$\Pr[\text{succeed twice}] \geq p^3$$

**Theorem:** If a quantum $P^*$ convinces $V$ to accept with probability $\geq 1/\sqrt{2} + \varepsilon$, we can extract a witness with probability $\Omega(\varepsilon)$.

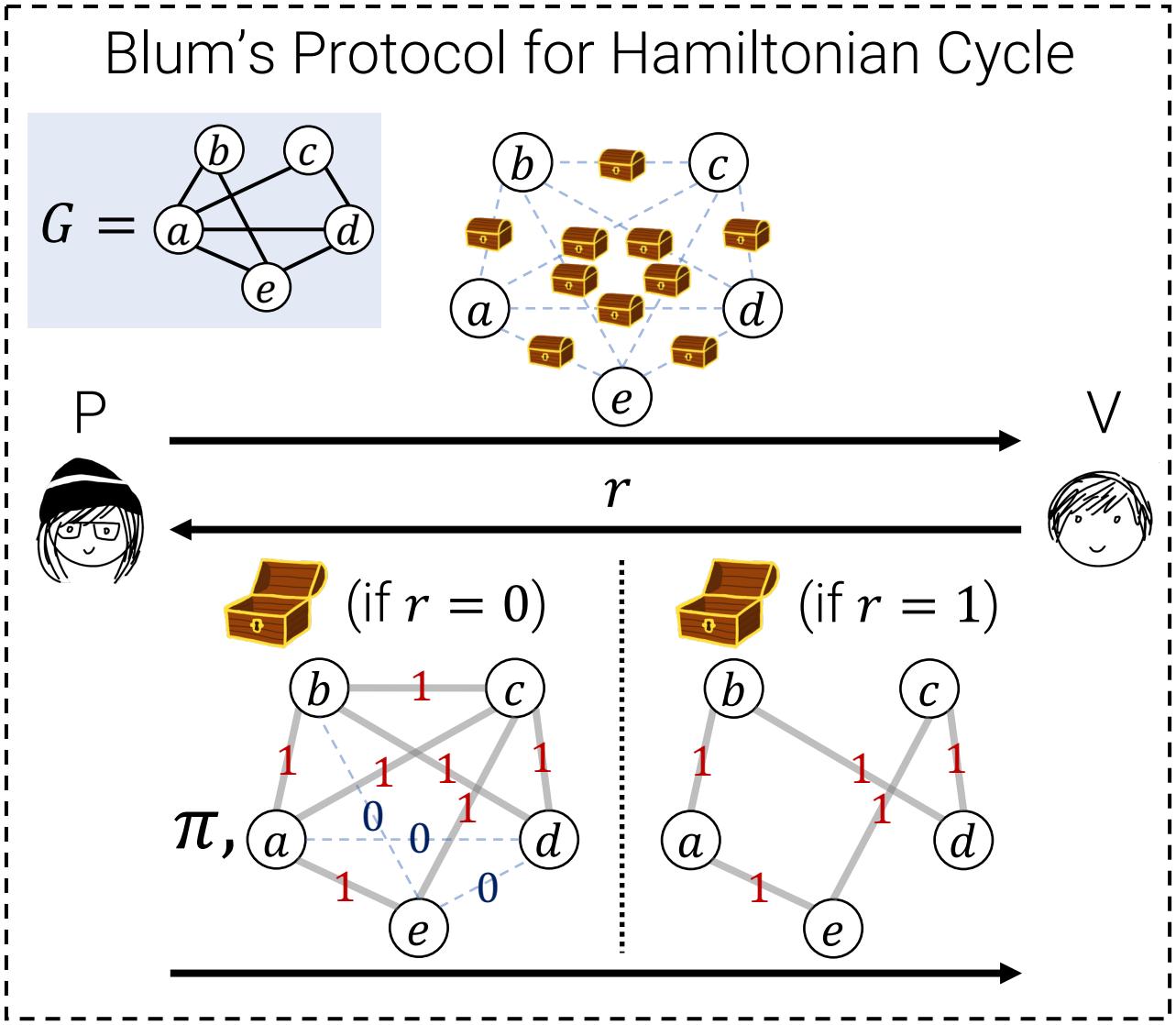
Remember that for classical $P^*$, we just need $1/2 + \varepsilon$, and we extract with probability $\approx 1$.

In the next talk, we'll see a different quantum rewinding technique that achieves the original classical guarantees.

# What this talk will cover:

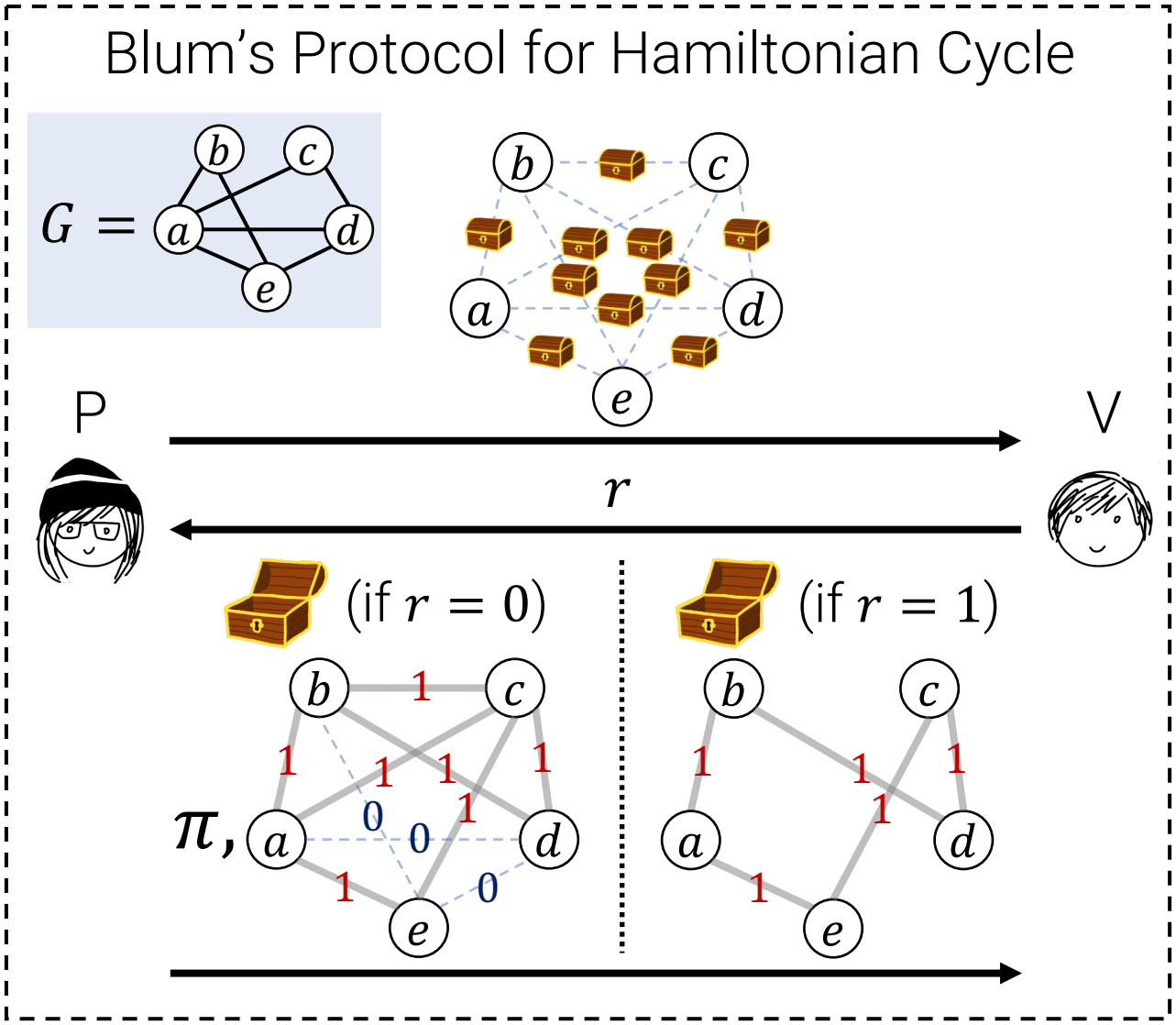
1. Is LWE all we need for post-quantum security? ✓
2. Review: Blum's Hamiltonicity protocol ✓
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge ✓
   - How to define post-quantum commitments ✓
   - Unruh's 1-bit rewinding lemma ✓
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge
   - Watrous's ZK rewinding lemma

# Classical Zero Knowledge




**Key Property**: can simulate honest verifier that sends random bit

# Classical Zero Knowledge

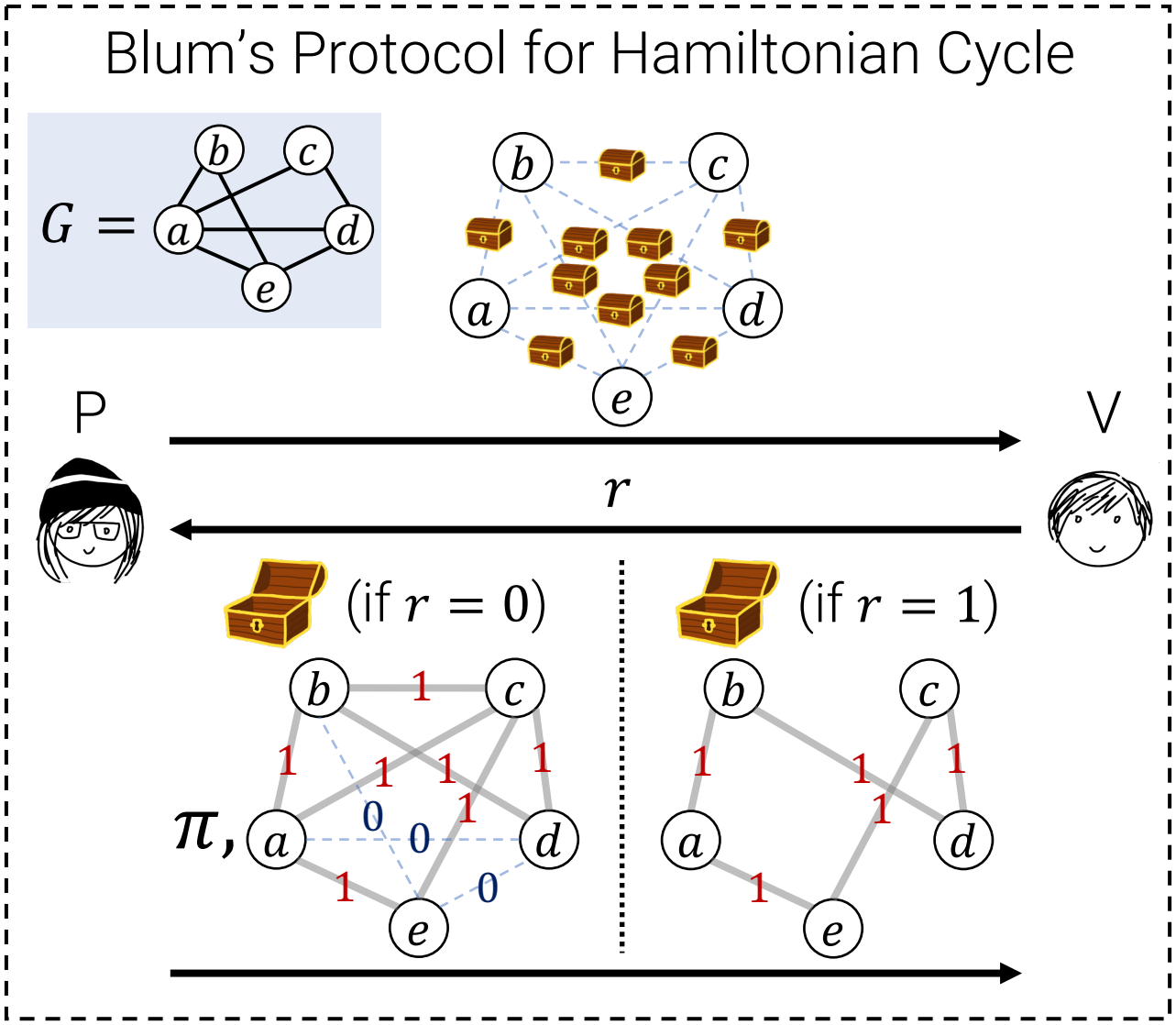



**Key Property**: can simulate honest verifier that sends random bit

**HVSim**:

1) Sample $r' \leftarrow \{0,1\}$

# Classical Zero Knowledge



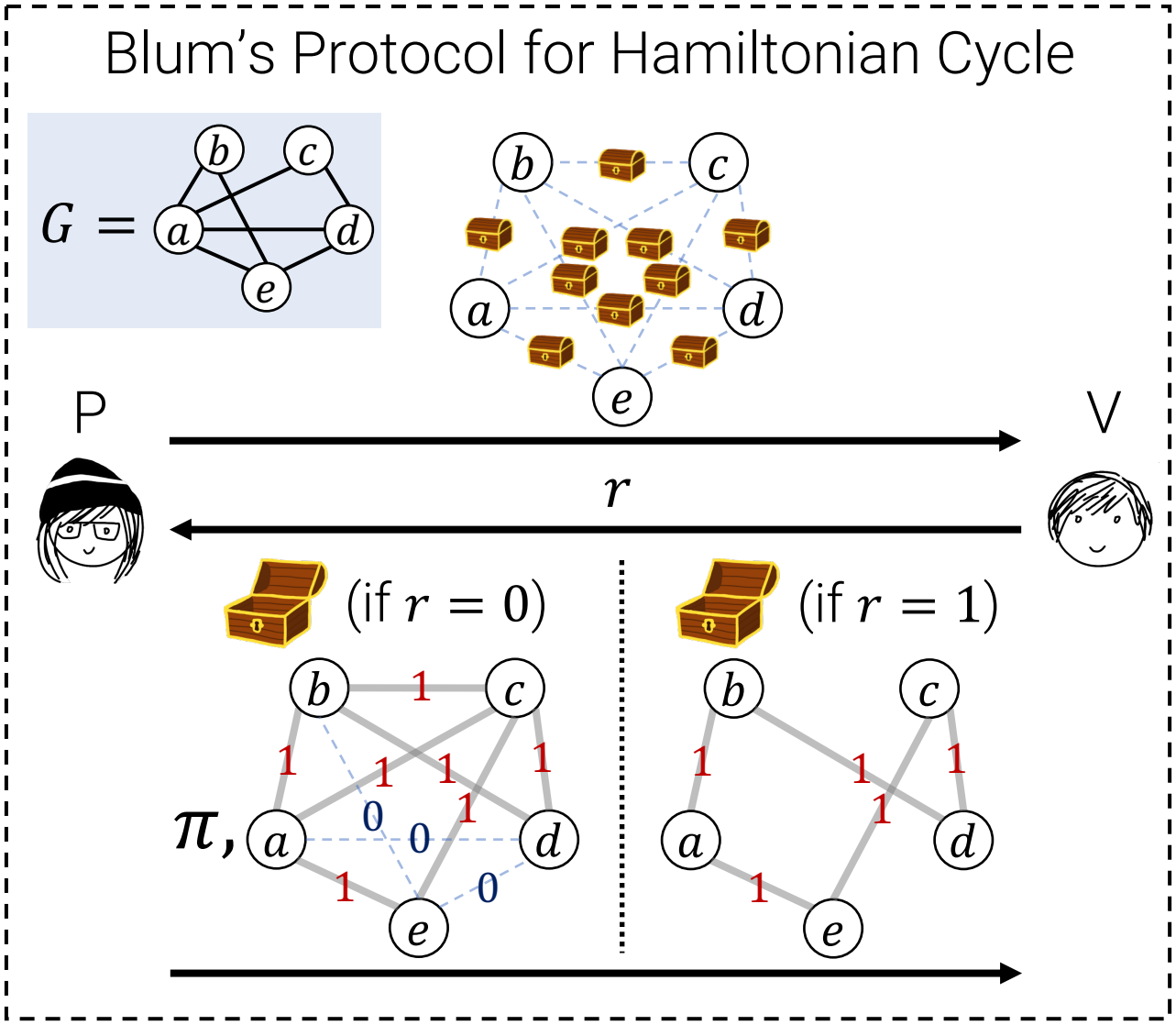

**Key Property**: can simulate honest verifier that sends random bit

**HVSim**:

1) Sample $r' \leftarrow \{0,1\}$

2) Generate transcript $(c, r', z)$:

# Classical Zero Knowledge

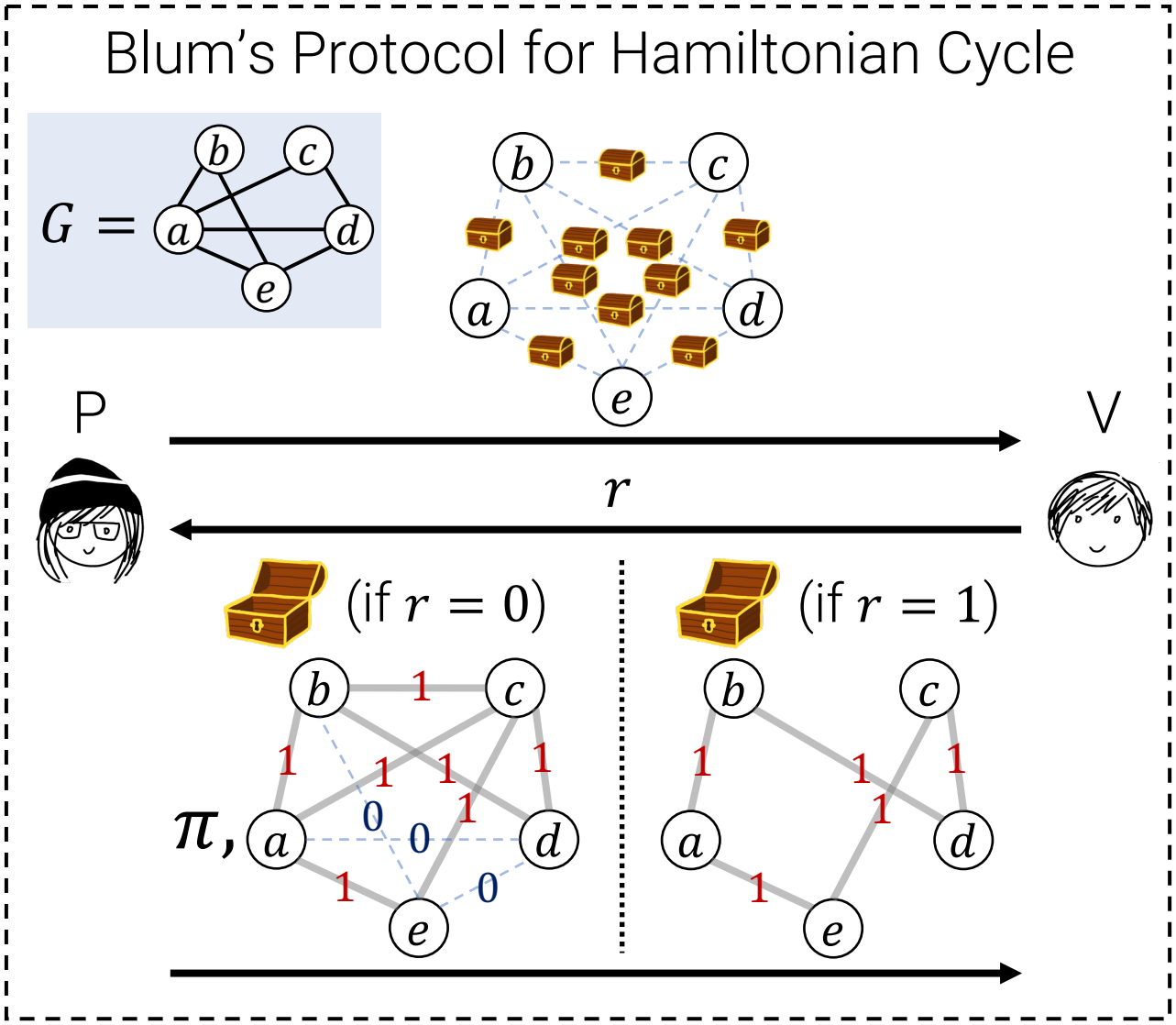



**Key Property**: can simulate honest verifier that sends random bit

**HVSim**:

1) Sample $r' \leftarrow \{0,1\}$
2) Generate transcript $(c, r', z)$:
   - If $r' = 0$, generate $c, z$ using a random permutation of $G$

# Classical Zero Knowledge

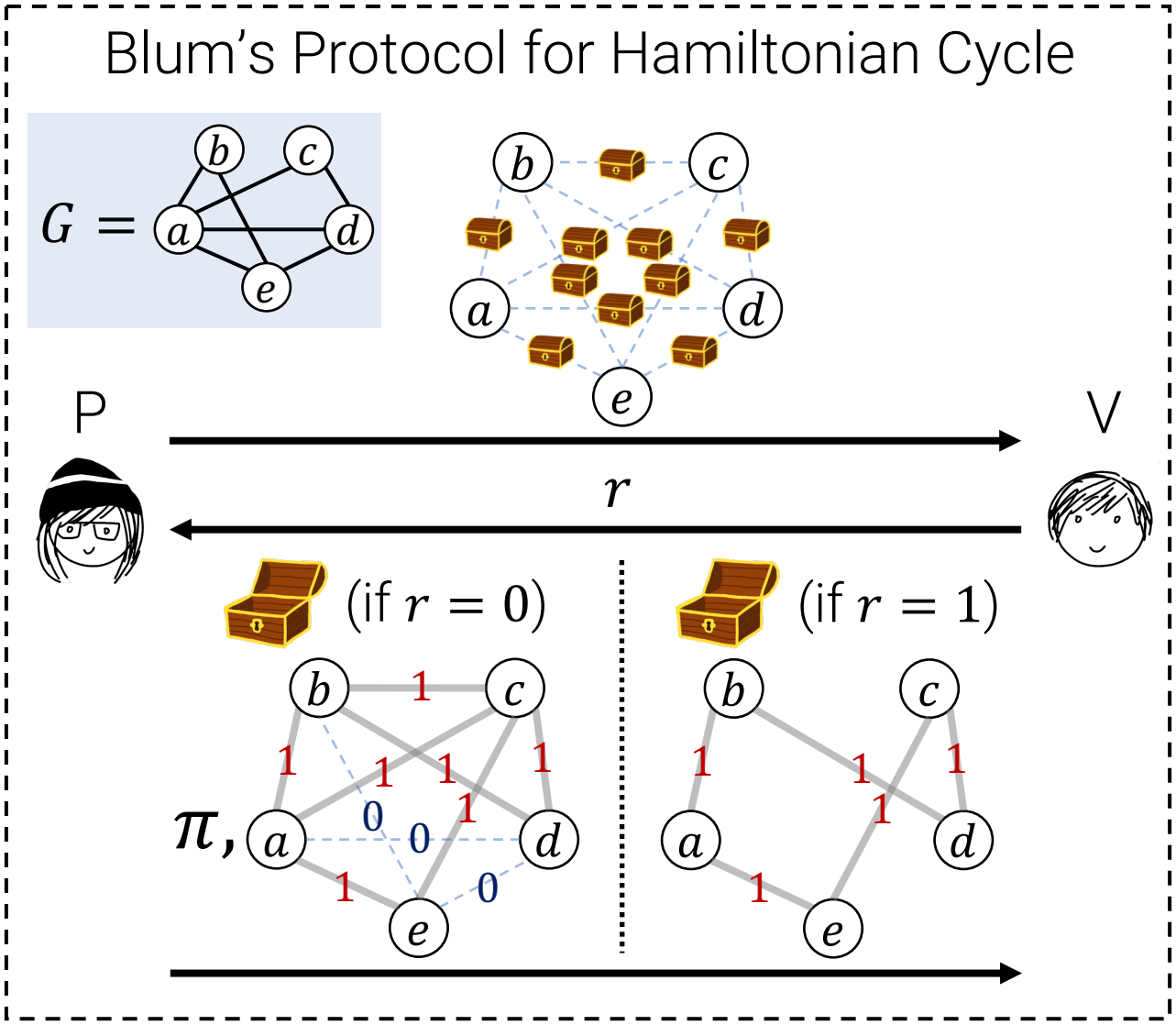



**Key Property**: can simulate honest verifier that sends random bit

**HVSim**:

1) Sample $r' \leftarrow \{0,1\}$
2) Generate transcript $(c, r', z)$:
- If $r' = 0$, generate $c, z$ using a random permutation of $G$
- If $r' = 1$, generate $c, z$ using a random cycle graph

# Classical Zero Knowledge




**Key Property**: can simulate honest verifier that sends random bit

**HVSim**:

1) Sample $r' \leftarrow \{0,1\}$
2) Generate transcript $(c, r', z)$:
   - If $r' = 0$, generate $c, z$ using a random permutation of $G$
   - If $r' = 1$, generate $c, z$ using a random cycle graph

By hiding, $(c, r', z) \leftarrow \mathbf{HVSim}$ looks like honest-verifier view.

# Classical Zero Knowledge

$\mathbf{HVSim}$ can simulate an honest verifier view, but ZK requires simulating a malicious $V^*$ that picks $r$ *adaptively* based on the first message $c$.

# Classical Zero Knowledge

$\mathbf{HVSim}$ can simulate an honest verifier view, but ZK requires simulating a malicious $V^*$ that picks $r$ *adaptively* based on the first message $c$.

Observation: can simulate malicious $V^*$ w/ prob $\approx 1/2$ by guessing $r$.

$\mathrm{Guess}(V^*)$:

$V^*$

# Classical Zero Knowledge

$\mathbf{HVSim}$ can simulate an honest verifier view, but ZK requires simulating a malicious $V^*$ that picks $r$ *adaptively* based on the first message $c$.

Observation: can simulate malicious $V^*$ w/ prob $\approx 1/2$ by guessing $r$.

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$

$V^*$

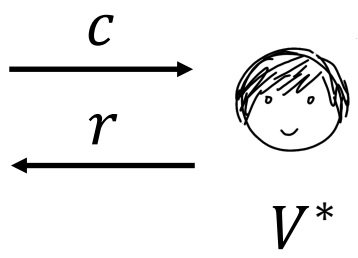
# Classical Zero Knowledge

$\mathbf{HVSim}$ can simulate an honest verifier view, but ZK requires simulating a malicious $V^*$ that picks $r$ *adaptively* based on the first message $c$.

Observation: can simulate malicious $V^*$ w/ prob $\approx 1/2$ by guessing $r$.

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$



# Classical Zero Knowledge

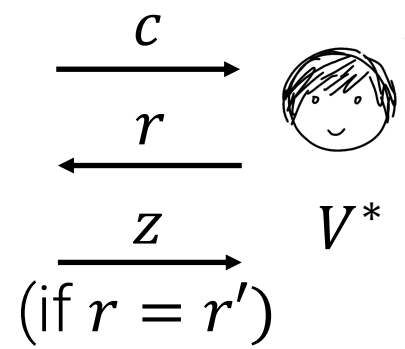
$\mathbf{HVSim}$ can simulate an honest verifier view, but ZK requires simulating a malicious $V^*$ that picks $r$ *adaptively* based on the first message $c$.

**Observation:** can simulate malicious $V^*$ w/ prob $\approx 1/2$ by guessing $r$.

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$

2) If $r = r'$, output $(c, r', z)$.
Otherwise, output $\perp$.



# Classical Zero Knowledge

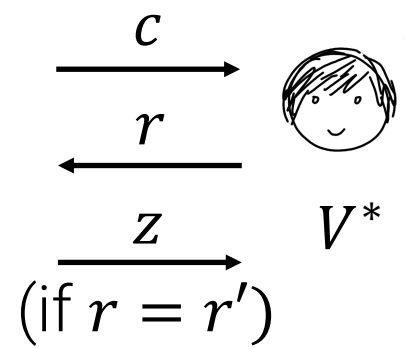
$\mathbf{HVSim}$ can simulate an honest verifier view, but ZK requires simulating a malicious $V^*$ that picks $r$ *adaptively* based on the first message $c$.

**Observation:** can simulate malicious $V^*$ w/ prob $\approx 1/2$ by guessing $r$.

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$

2) If $r = r'$, output $(c, r', z)$.
Otherwise, output $\perp$.




Since $c$ is hiding, $\Pr[r = r'] \approx 1/2$

# Classical Zero Knowledge

$\mathbf{HVSim}$ can simulate an honest verifier view, but ZK requires simulating a malicious $V^*$ that picks $r$ *adaptively* based on the first message $c$.

**Observation:** can simulate malicious $V^*$ w/ prob $\approx 1/2$ by guessing $r$.

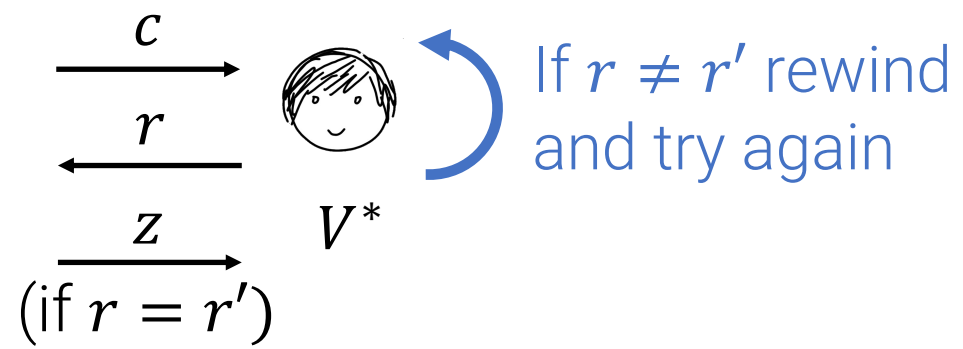
We combine this with rewinding to get the full ZK simulator:

$\mathbf{Sim}(V^*)$

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$

2) If $r = r'$, output $(c, r', z)$. Otherwise, output $\perp$.




Since $c$ is hiding, $\Pr[r = r'] \approx 1/2$

# What this talk will cover:

1. Is LWE all we need for post-quantum security? ✓
2. Review: Blum's Hamiltonicity protocol ✓
3. Post-quantum proof of knowledge (PoK):
   - Review: classical proof of knowledge ✓
   - How to define post-quantum commitments ✓
   - Unruh's 1-bit rewinding lemma ✓
4. Post-quantum ZK for Blum's protocol
   - Review: classical zero knowledge ✓
   - Watrous's ZK rewinding lemma

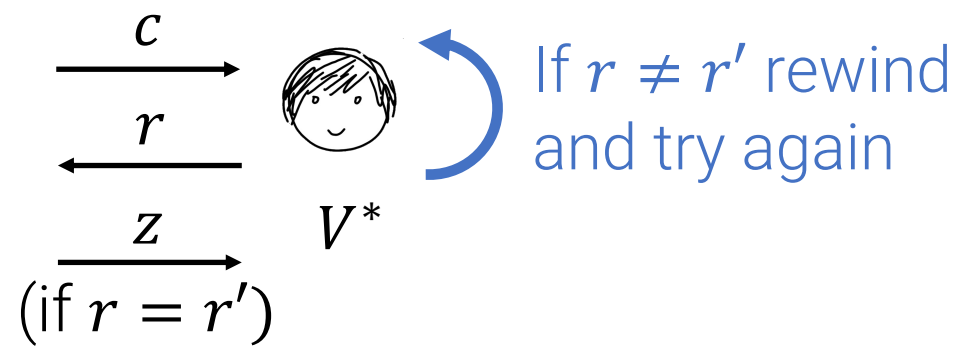
Unfortunately, this simulator won't suffice for post-quantum ZK! If a malicious $V^*$ has an unknown initial state $|\psi\rangle$ running $\mathbf{Guess}(V^*, |\psi\rangle)$ may irreversibly disturb it.

$\mathbf{Sim}(V^*)$

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$

2) If $r = r'$, output $(c, r', z)$. Otherwise, output $\perp$.




Since $c$ is hiding, $\Pr[r = r'] \approx 1/2$

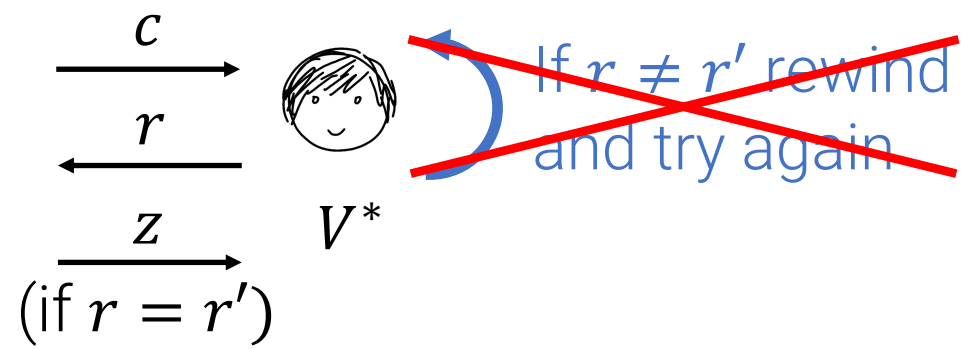
Unfortunately, this simulator won't suffice for post-quantum ZK! If a malicious $V^*$ has an unknown initial state $|\psi\rangle$ running $\mathbf{Guess}(V^*, |\psi\rangle)$ may irreversibly disturb it.

$\mathbf{Sim}(V^*)$

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$

2) If $r = r'$, output $(c, r', z)$. Otherwise, output $\perp$.




Since $c$ is hiding, $\Pr[r = r'] \approx 1/2$

Unfortunately, this simulator won't suffice for post-quantum ZK! If a malicious $V^*$ has an unknown initial state $|\psi\rangle$ running $\mathbf{Guess}(V^*, |\psi\rangle)$ may irreversibly disturb it.

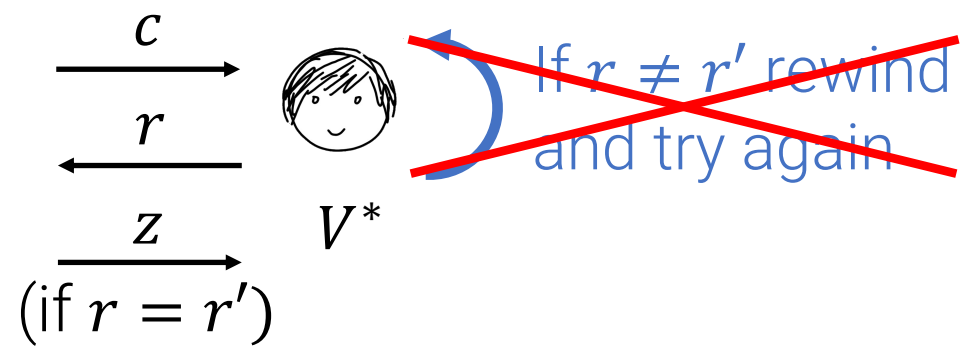
But there is a different simulator due to [Watrous05] that works.

$\mathbf{Sim}(V^*)$

$\mathbf{Guess}(V^*)$:

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$

2) If $r = r'$, output $(c, r', z)$. Otherwise, output $\perp$.

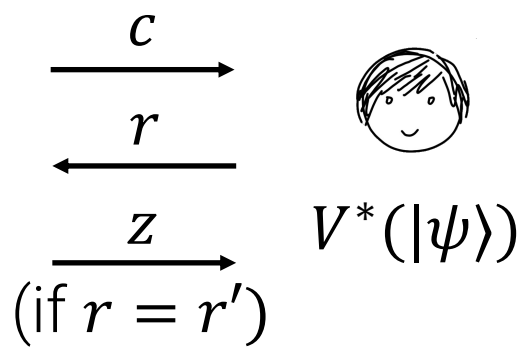



Since $c$ is hiding, $\Pr[r = r'] \approx 1/2$

[Watrous05]: If commitment scheme is hiding, then the Blum protocol is post-quantum ZK.

# Post-Quantum ZK of Blum [Watrous05]

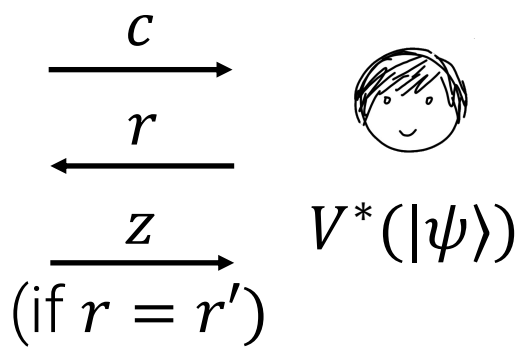
$\mathbf{Guess}(V^*, |\psi\rangle)$:
1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$
2) If $r = r'$, output $(c, r, z)$. Otherwise $\perp$.




If commitments are hiding, can still simulate with probability $1/2$.

# Post-Quantum ZK of Blum [Watrous05]

$\mathbf{Guess}(V^*, |\psi\rangle)$:
1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$
2) If $r = r'$, output $(c, r, z)$. Otherwise $\perp$.

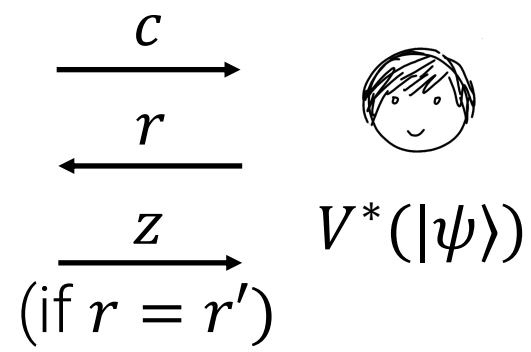



If commitments are hiding, can still simulate with probability $1/2$.

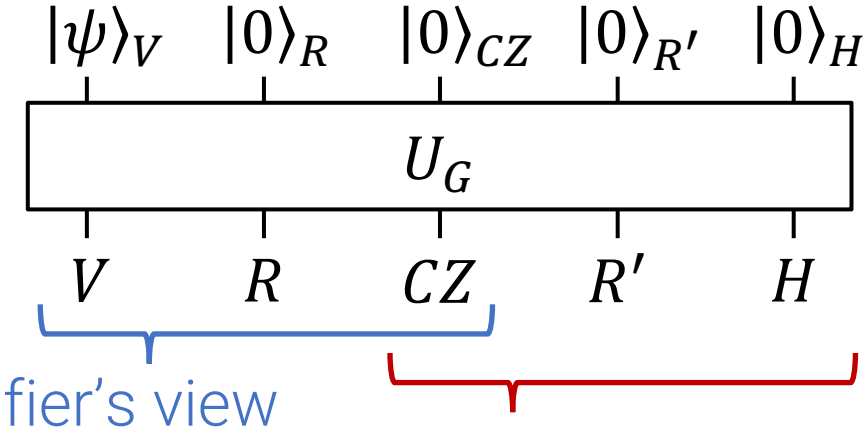
We'll write this process as a quantum circuit on $|\psi\rangle$.

# Post-Quantum ZK of Blum [Watrous05]

$\mathbf{Guess}(V^*, |\psi\rangle)$:
1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$
2) If $r = r'$, output $(c, r, z)$. Otherwise $\perp$.



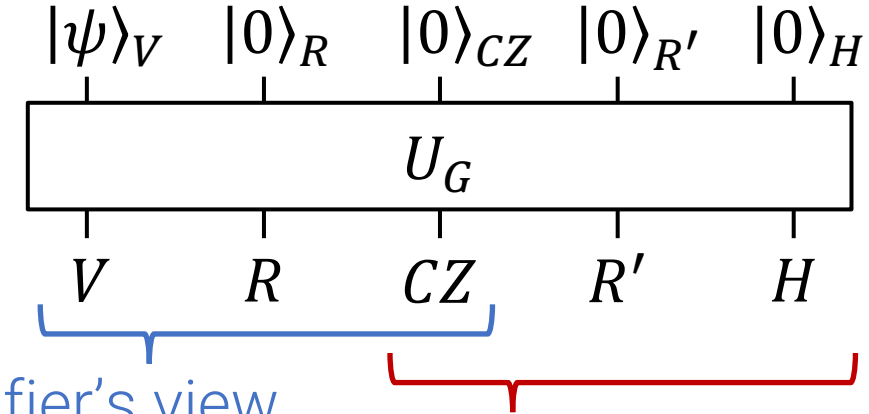

$C, R, Z, R'$ correspond to $c, r, z, r'$




- Computing $U_G|\psi\rangle|0\rangle$ and checking if $R = R'$ is the same as running $\mathbf{Guess}(V^*, |\psi\rangle)$.

# Post-Quantum ZK of Blum [Watrous05]

$C, R, Z, R'$ correspond to $c, r, z, r'$



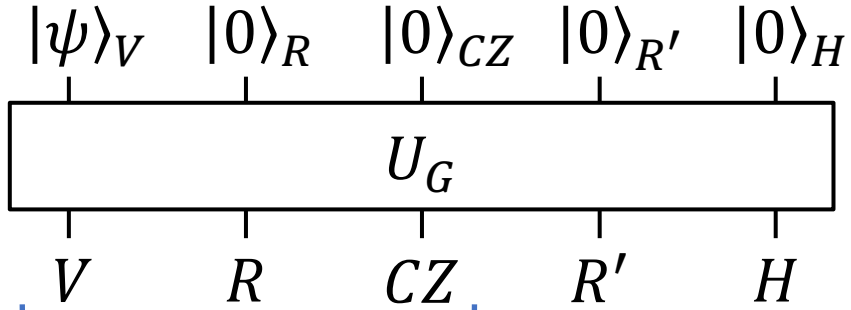

- Computing $U_G|\psi\rangle|0\rangle$ and checking if $R = R'$ is the same as running $\mathbf{Guess}(V^*, |\psi\rangle)$.

# Post-Quantum ZK of Blum [Watrous05]

Define projector $\Pi_G := U_G^\dagger \Pi_{R=R'} U_G$.

**Intuition:** $(\Pi_G, \mathbb{I} - \Pi_G)$ measures whether simulation succeeds.

$C, R, Z, R'$ correspond to $c, r, z, r'$




Verifier's view (state + transcript)

**HVSim** (workspace + output)

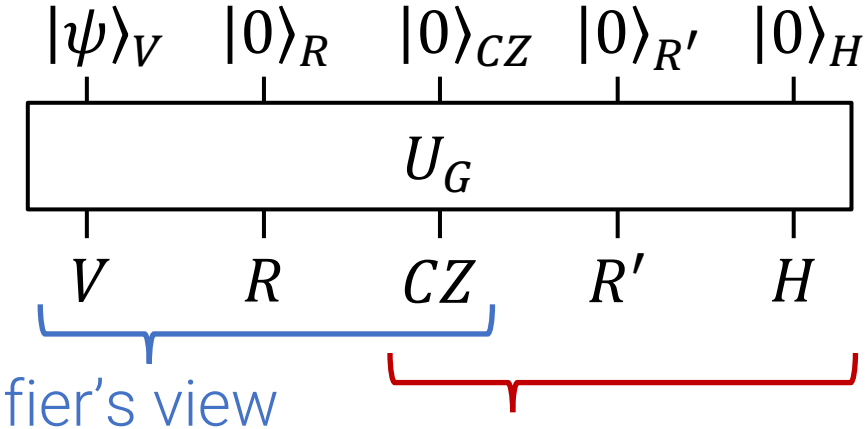
- Computing $U_G|\psi\rangle|0\rangle$ and checking if $R = R'$ is the same as running $\mathbf{Guess}(V^*, |\psi\rangle)$.

# Post-Quantum ZK of Blum [Watrous05]

Define projector $\Pi_G := U_G^\dagger \Pi_{R=R'} U_G$.
**Intuition:** $(\Pi_G, \mathbb{I} - \Pi_G)$ measures whether simulation succeeds.

**Our goal:** Produce the state $\Pi_G |\psi\rangle_V |0\rangle_{Aux}$.

$C, R, Z, R'$ correspond to $c, r, z, r'$




- Computing $U_G|\psi\rangle|0\rangle$ and checking if $R = R'$ is the same as running $\mathbf{Guess}(V^*, |\psi\rangle)$.

# Post-Quantum ZK of Blum [Watrous05]

Define projector $\Pi_G \coloneqq U_G^\dagger \Pi_{R=R'} U_G$.
Intuition: $(\Pi_G, \mathbb{I} - \Pi_G)$ measures whether simulation succeeds.

**Our goal**: Produce the state $\Pi_G |\psi\rangle_V |0\rangle_{Aux}$.

Rough Intuition:

- Each $(\Pi_G, \mathbb{I} - \Pi_G)$ measurement is one simulation attempt.

# Post-Quantum ZK of Blum [Watrous05]

Define projector $\Pi_G \coloneqq U_G^\dagger \Pi_{R=R'} U_G$.
Intuition: $(\Pi_G, \mathbb{I} - \Pi_G)$ measures whether simulation succeeds.

**Our goal**: Produce the state $\Pi_G |\psi\rangle_V |0\rangle_{Aux}$.

Rough Intuition:

- Each $(\Pi_G, \mathbb{I} - \Pi_G)$ measurement is one simulation attempt.
- Applying $(\Pi_G, \mathbb{I} - \Pi_G)$ *twice in a row* gives the same outcome (no help).

# Post-Quantum ZK of Blum [Watrous05]

Define projector $\Pi_G := U_G^\dagger \Pi_{R=R'} U_G$.
Intuition: $(\Pi_G, \mathbb{I} - \Pi_G)$ measures whether simulation succeeds.

**Our goal**: Produce the state $\Pi_G |\psi\rangle_V |0\rangle_{Aux}$.

Rough Intuition:

- Each $(\Pi_G, \mathbb{I} - \Pi_G)$ measurement is one simulation attempt.
- Applying $(\Pi_G, \mathbb{I} - \Pi_G)$ ***twice in a row*** gives the same outcome (no help).
- We'll write down an $M_0$ measurement to "reset" each attempt.

# The Post-Quantum ZK Simulator [MW05, W05]

# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.

# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.

# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.

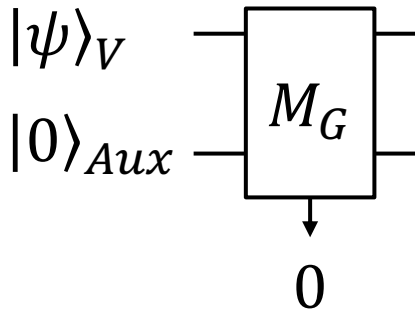
$|\psi\rangle_V$ –

$|0\rangle_{Aux}$ –

# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

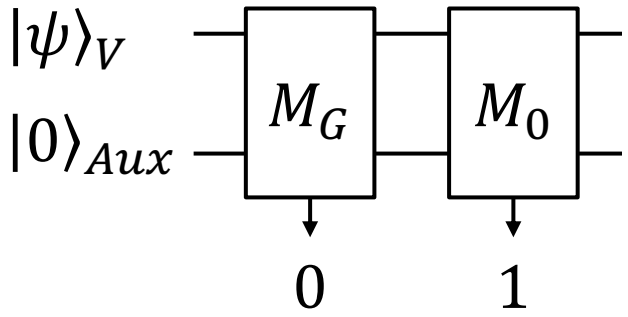
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

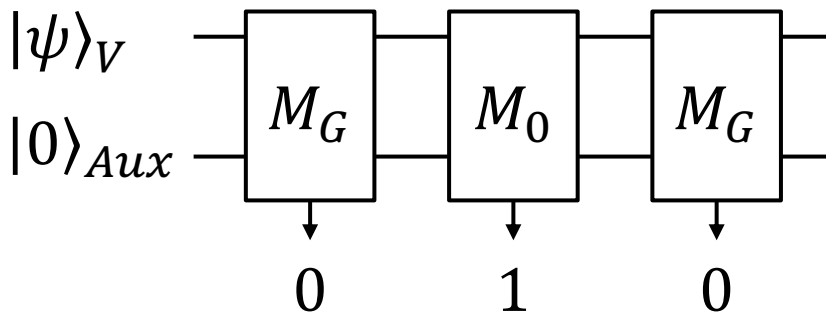
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

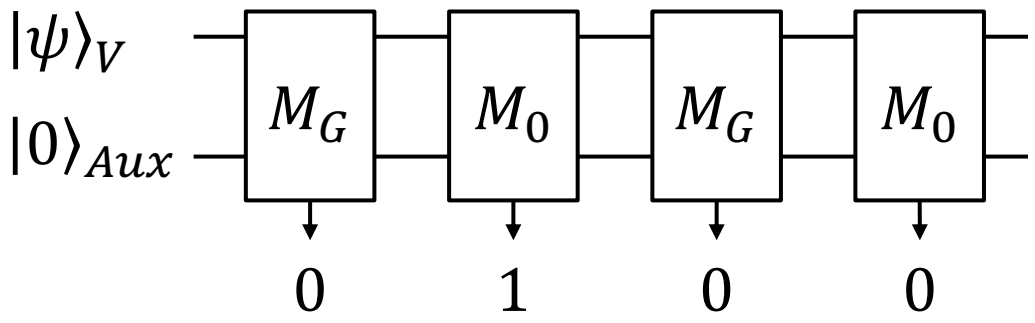
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

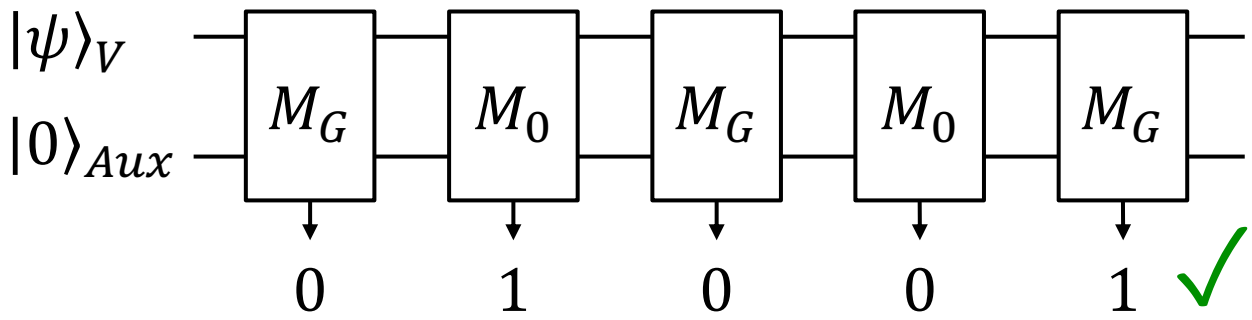
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

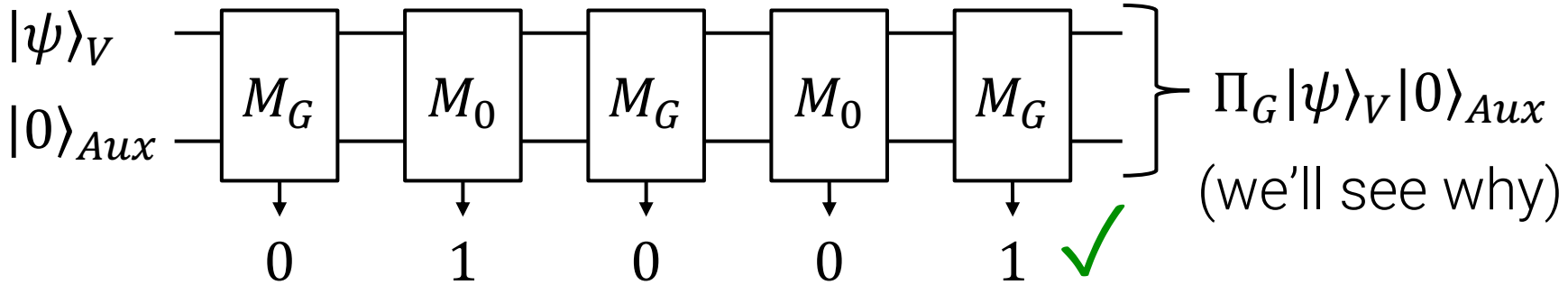
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

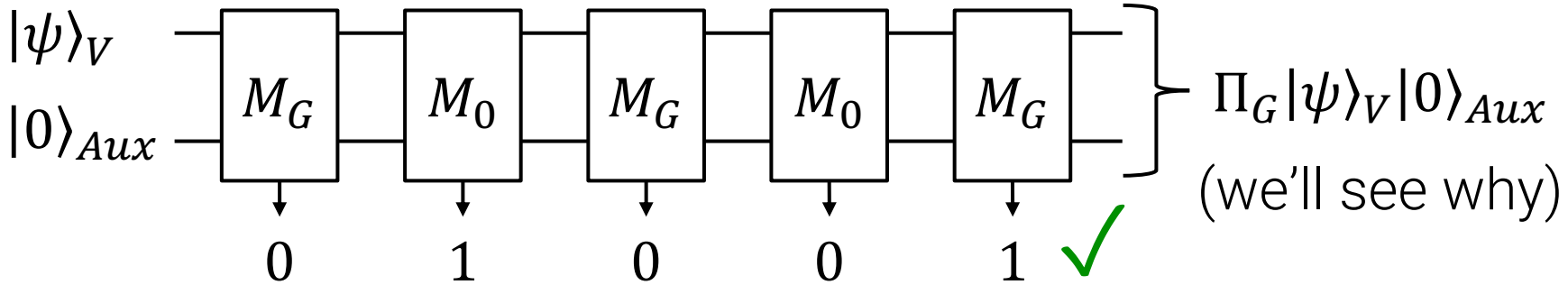
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

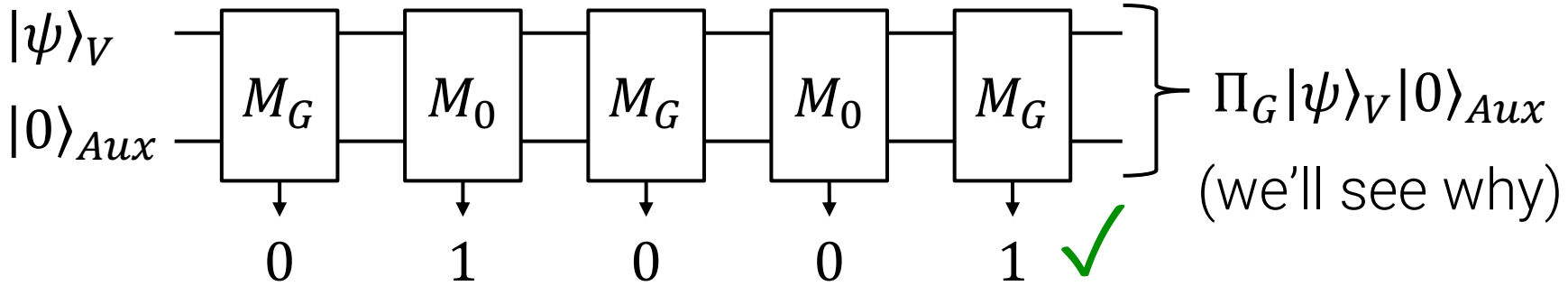
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.
3) Generate verifier's view (apply $U_G$).



# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.
3) Generate verifier's view (apply $U_G$).

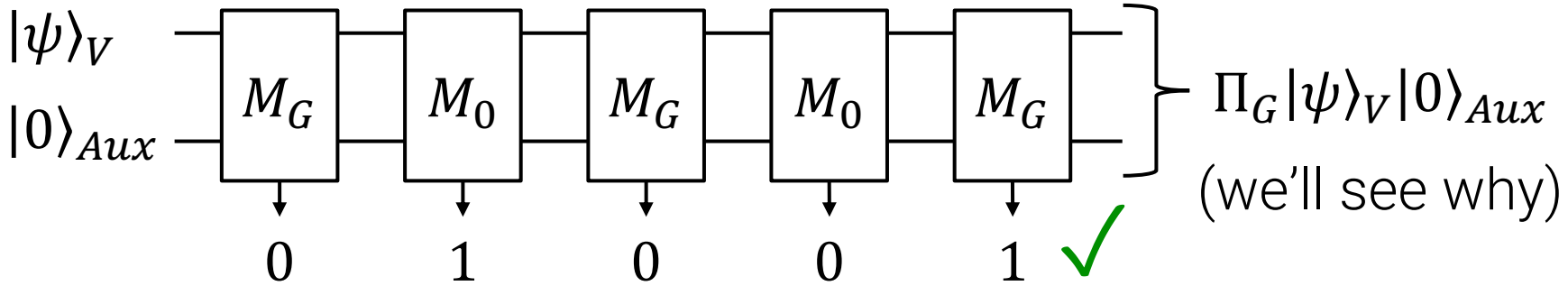



But why does this simulator work? Need to resolve:

# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.
3) Generate verifier's view (apply $U_G$).



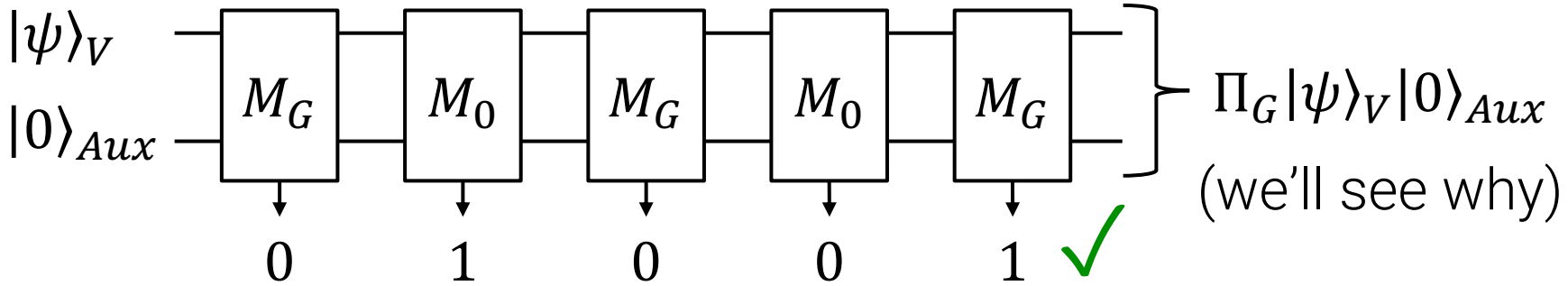

But why does this simulator work? Need to resolve:

- **Efficiency**: How long (if ever) until $M_G \to 1$?

# The Post-Quantum ZK Simulator [MW05, W05]

$\mathbf{Sim}(V^*, |\psi\rangle)$

1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.
3) Generate verifier's view (apply $U_G$).




But why does this simulator work? Need to resolve:

- **Efficiency**: How long (if ever) until $M_G \to 1$?
- **Simulation**: After $M_G \to 1$, why is the state is $\Pi_G|\psi\rangle_V|0\rangle_{Aux}$?

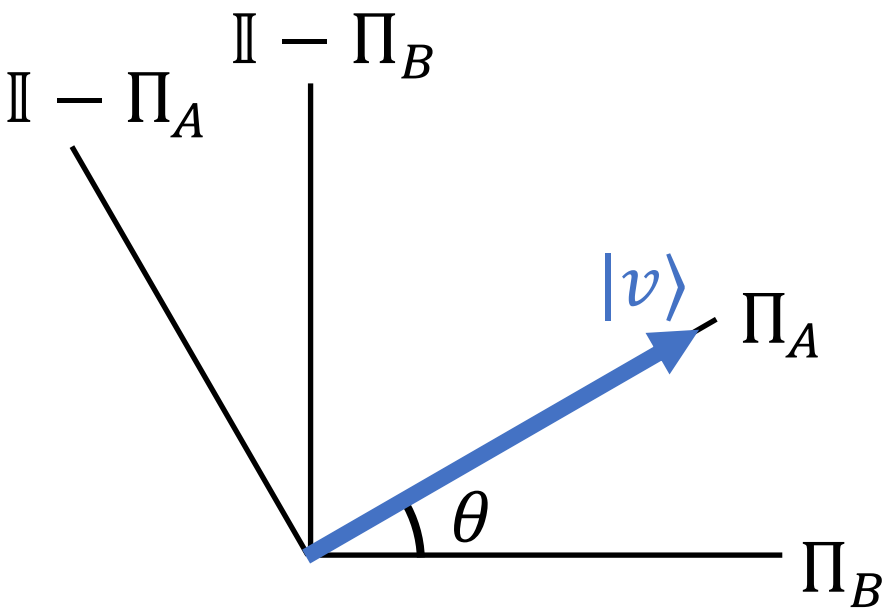
# Understanding Alternating Measurements [MW05]

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

# Understanding Alternating Measurements [MW05]

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

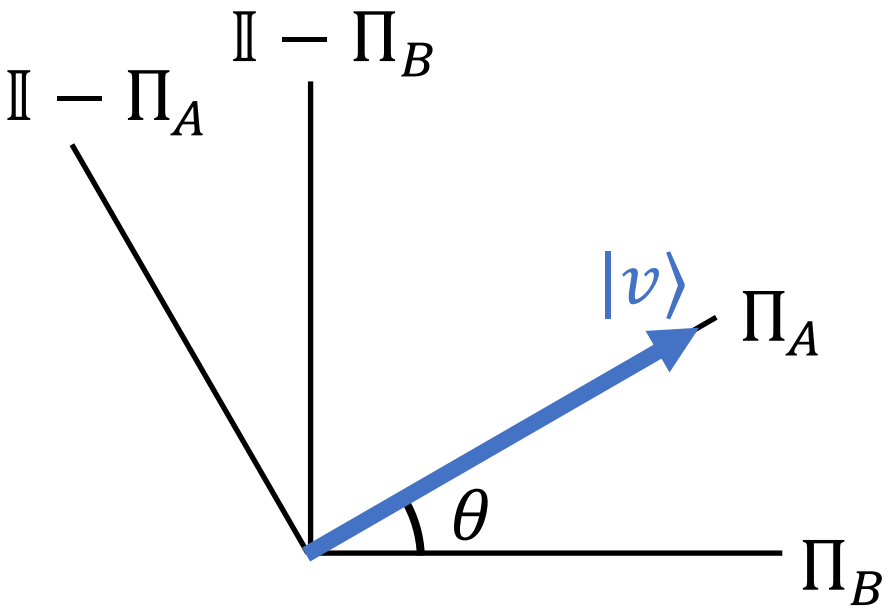
Easy case: $\Pi_A, \Pi_B$ live in 2D



# Understanding Alternating Measurements [MW05]

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D

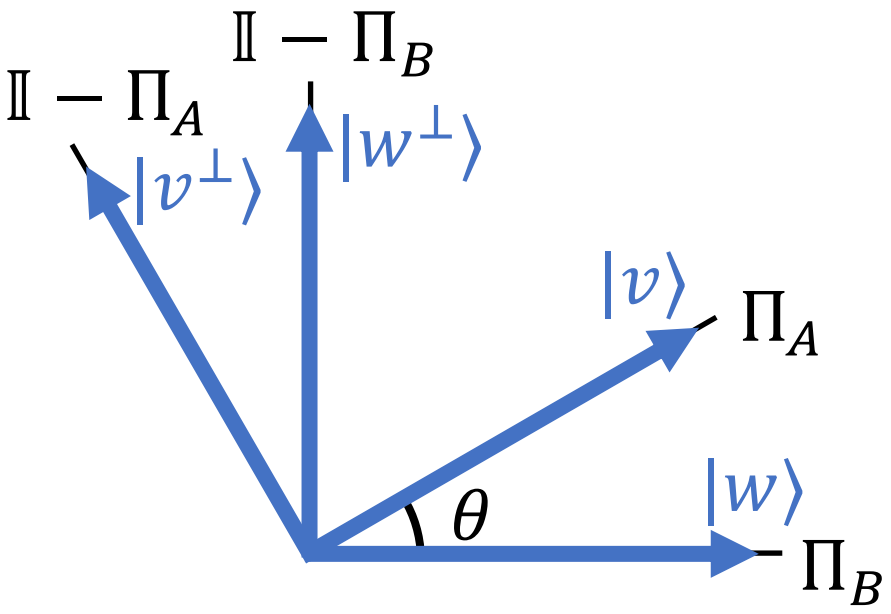



When we alternate measurements, we jump between four states

# Understanding Alternating Measurements [MW05]

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D



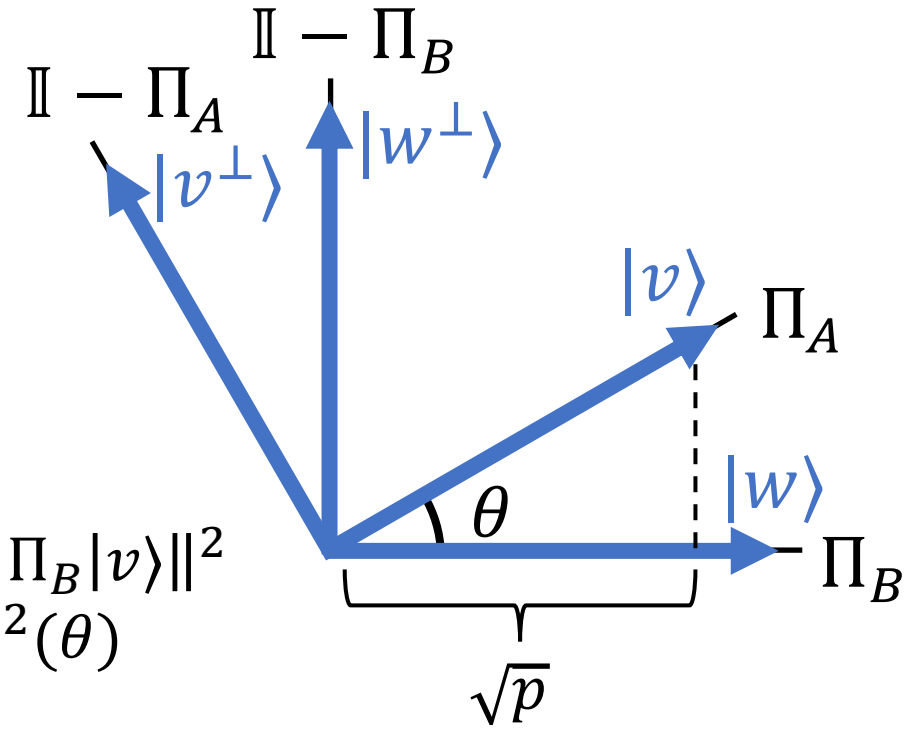

When we alternate measurements, we jump between four states

# Understanding Alternating Measurements [MW05]

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D

When we alternate measurements, we jump between four states

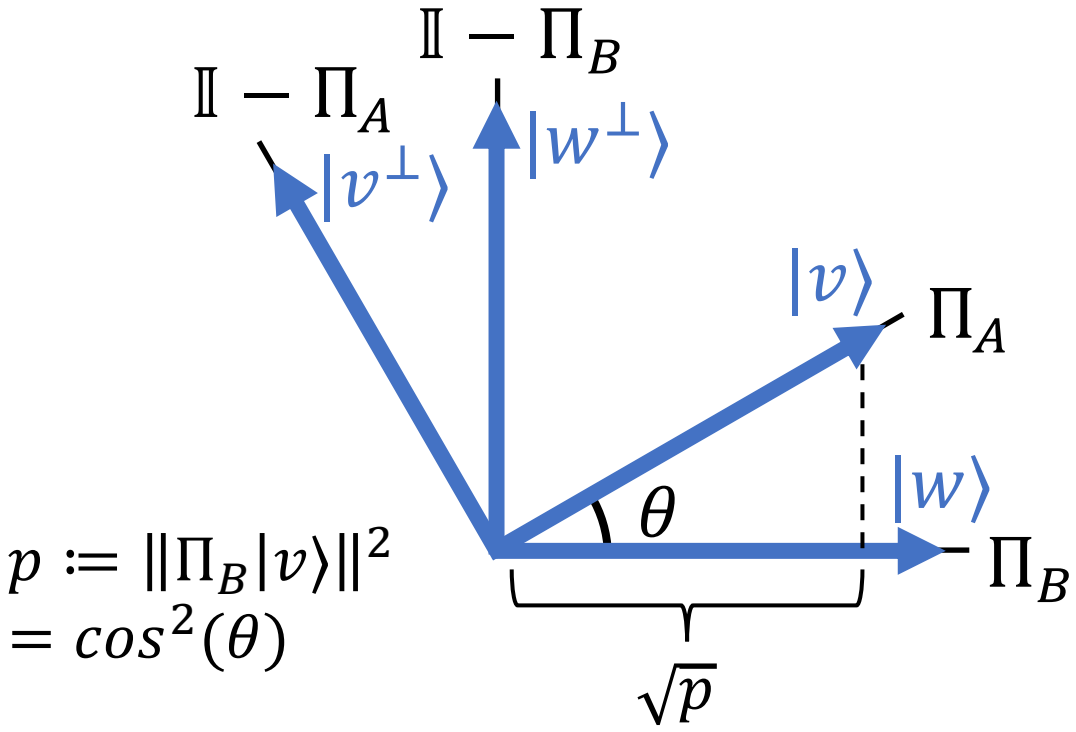



$p \coloneqq \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

# Understanding Alternating Measurements [MW05]

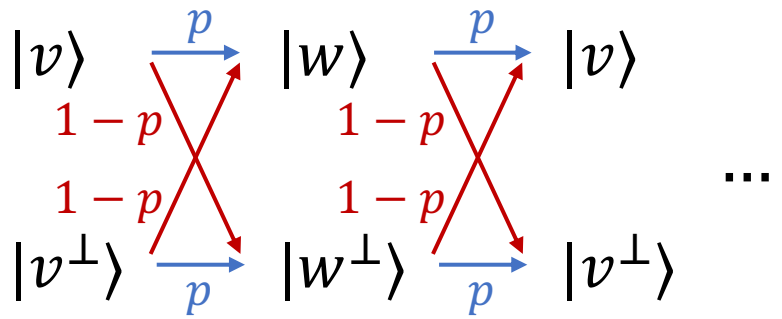
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

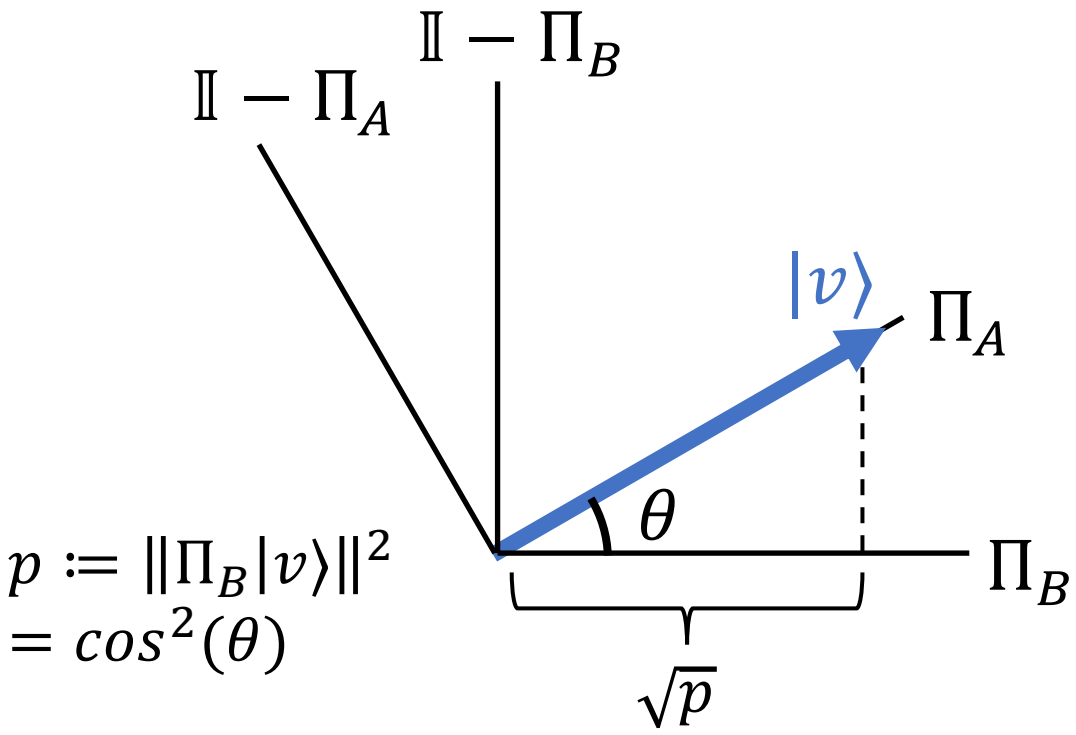
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

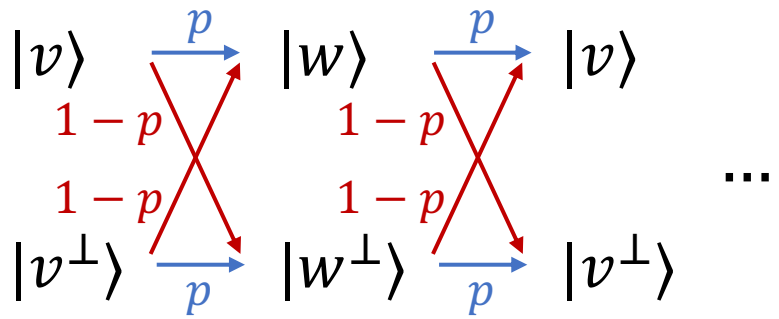
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

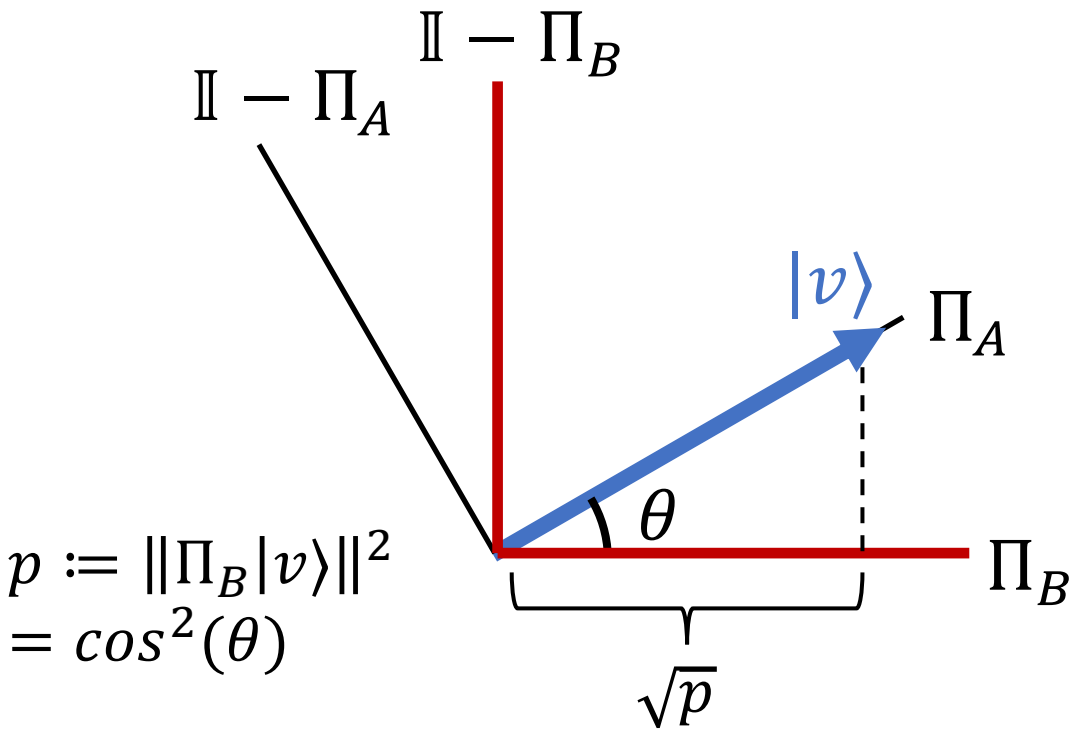
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

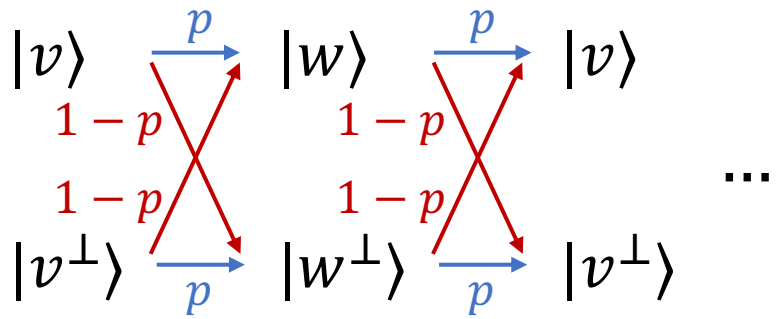
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

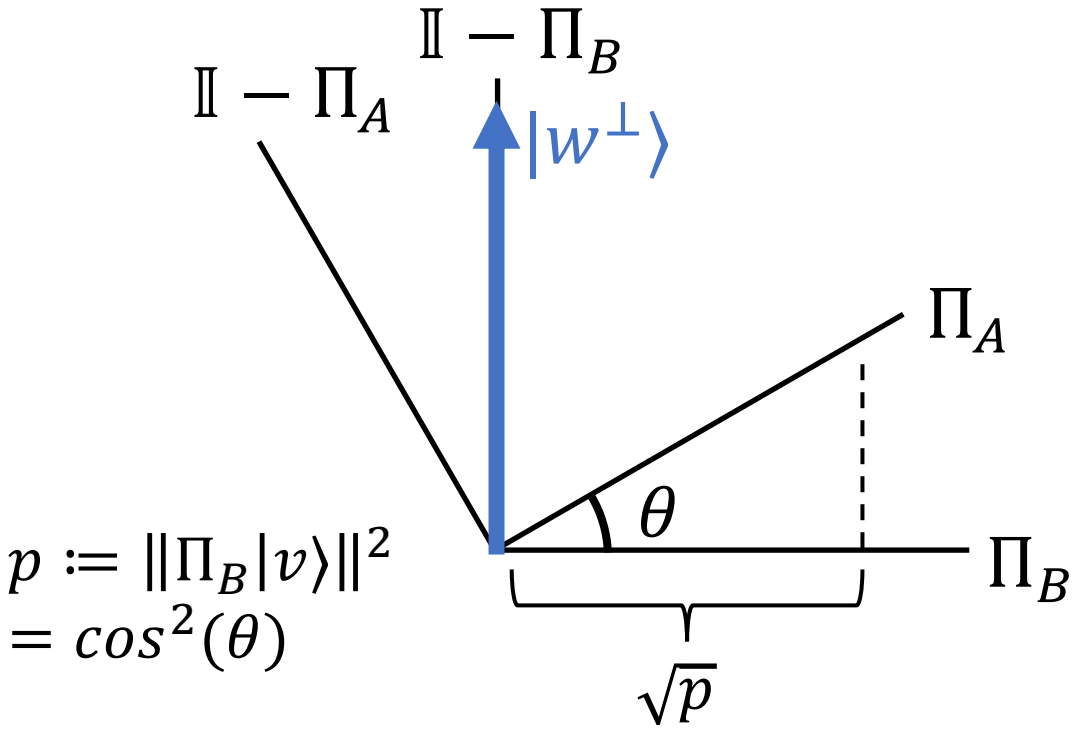
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

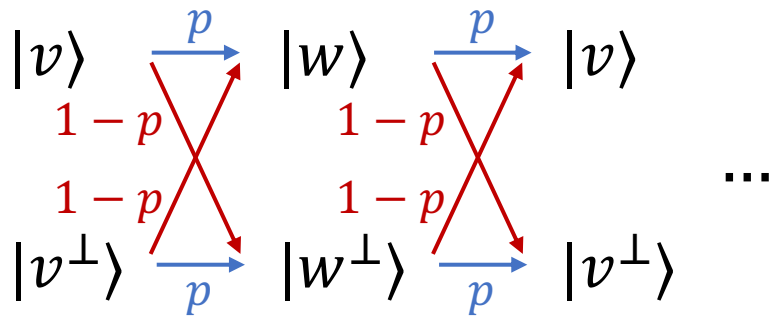
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

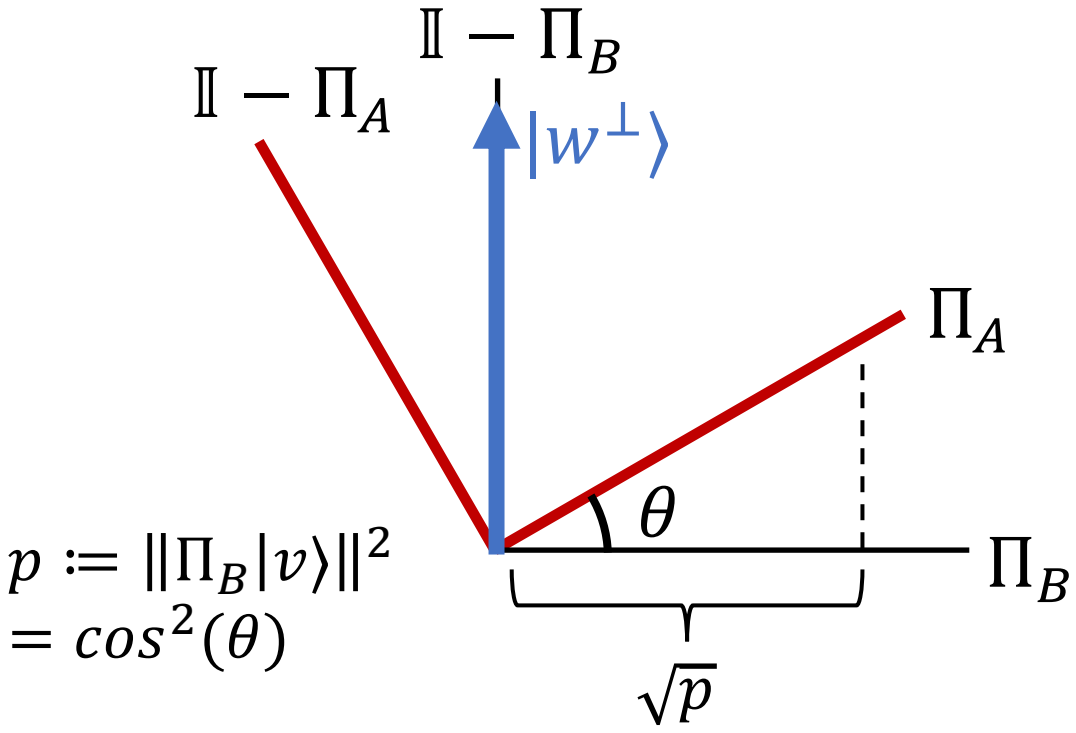
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

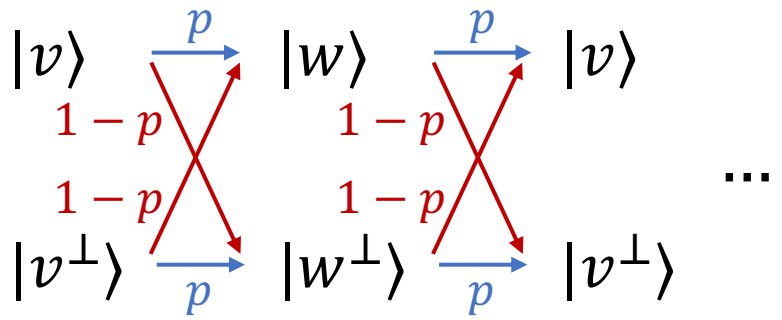
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

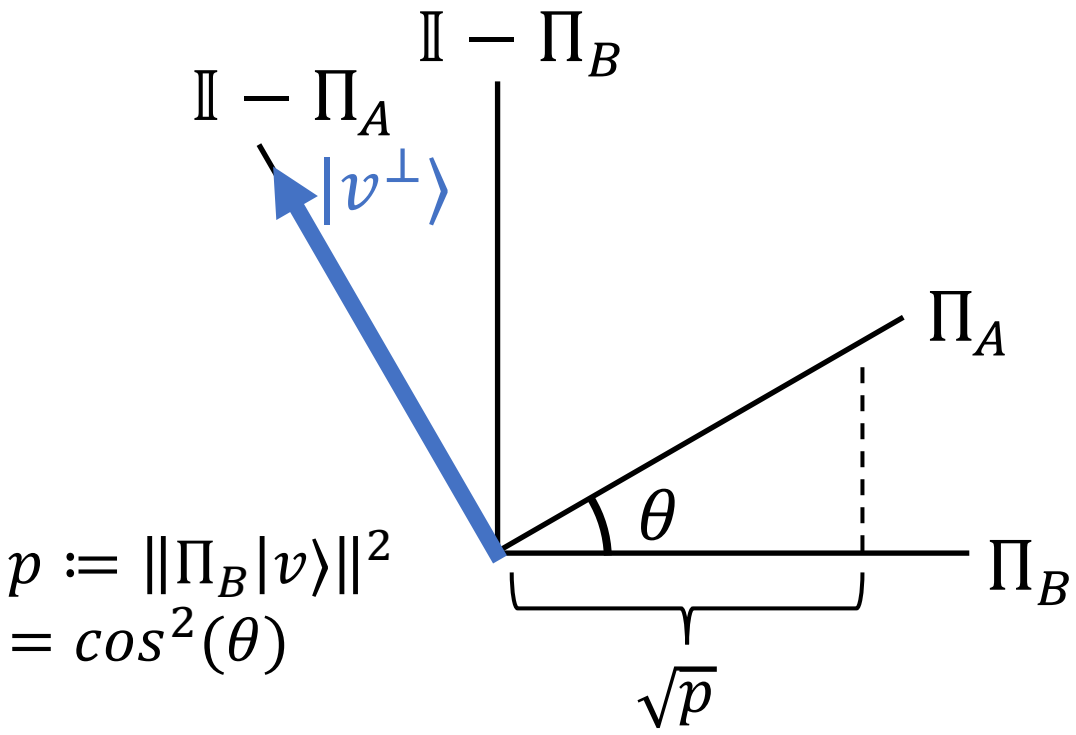
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

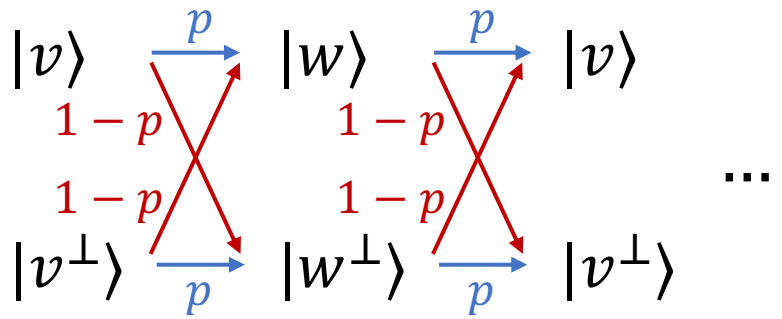
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

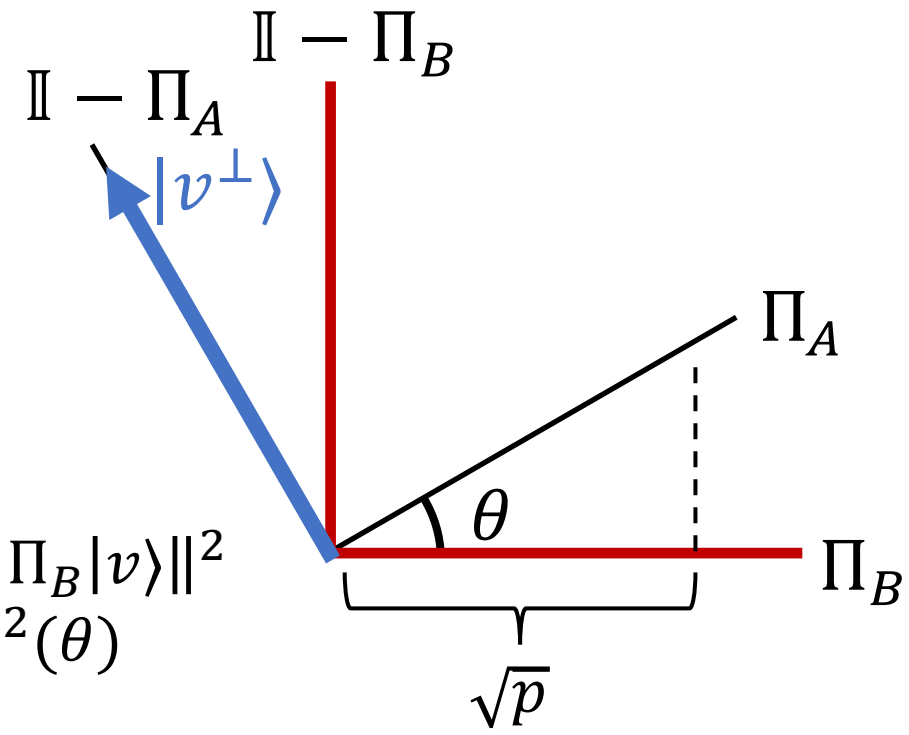
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

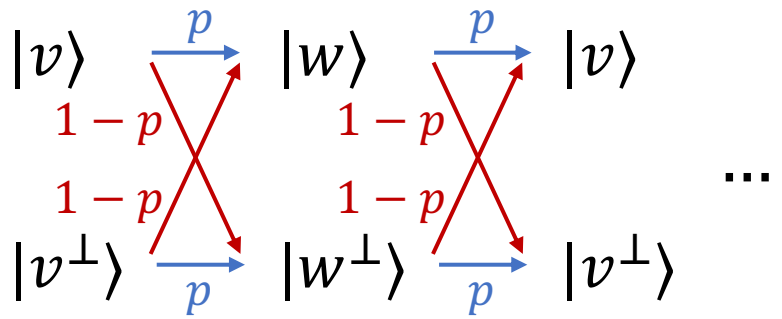
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

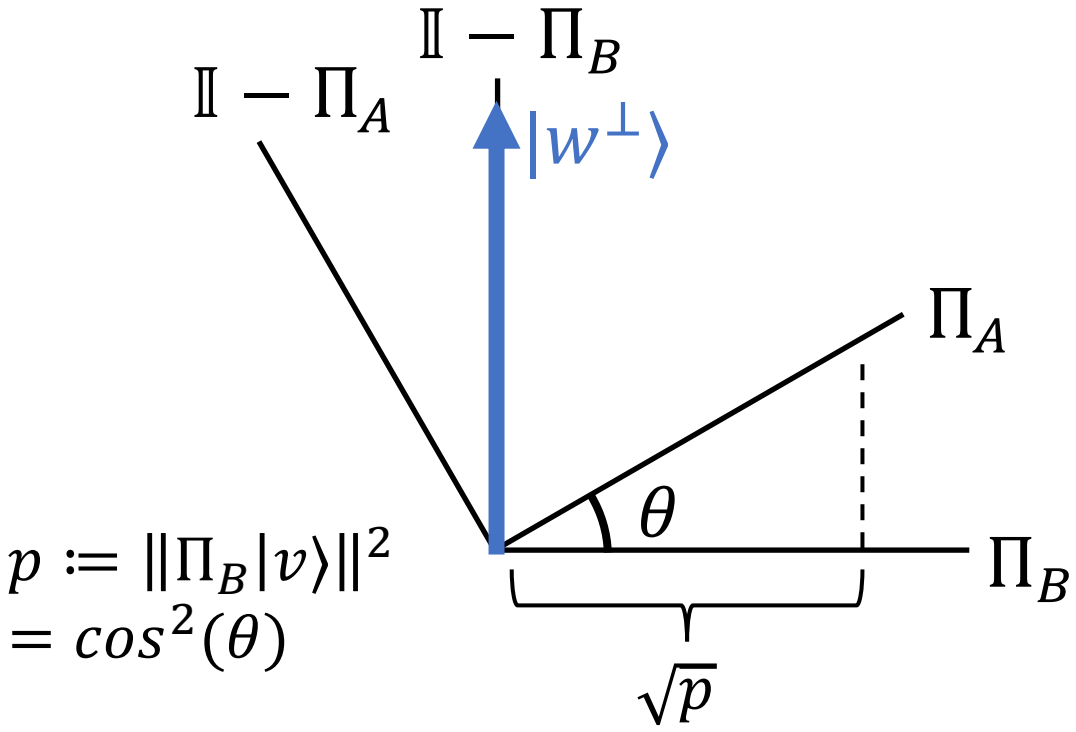
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

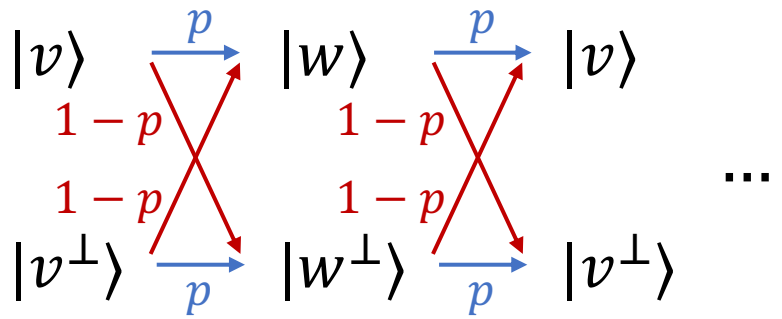
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

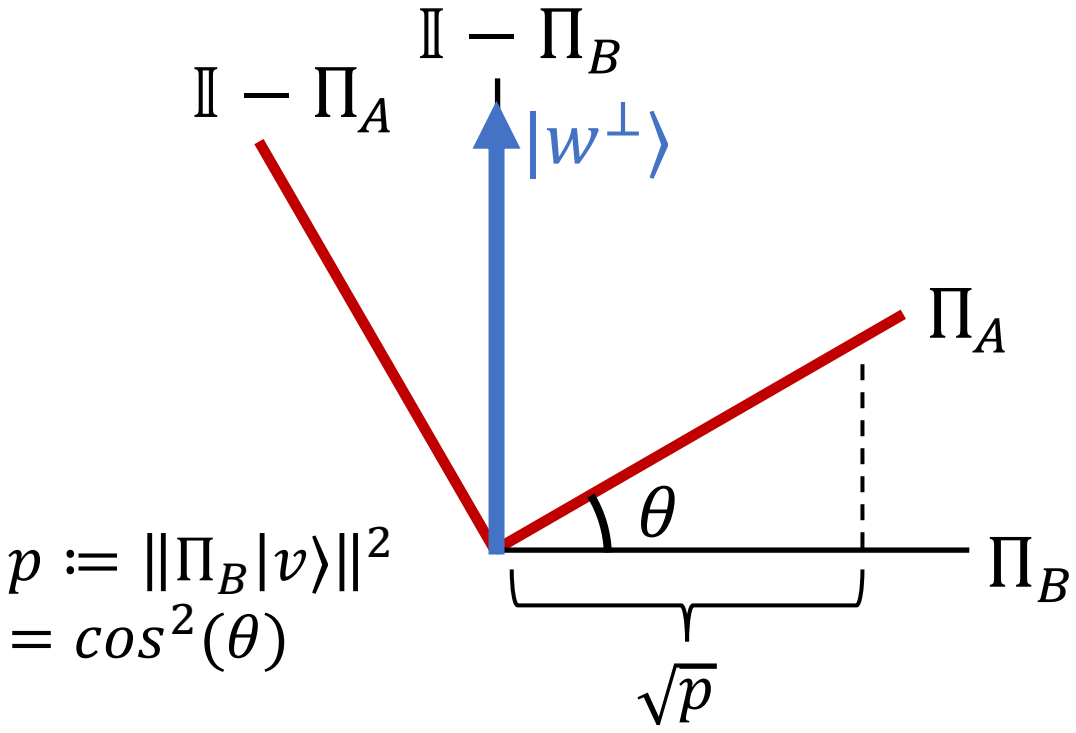
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

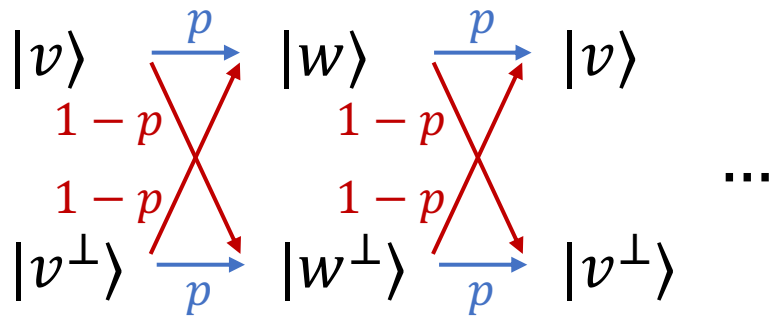
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

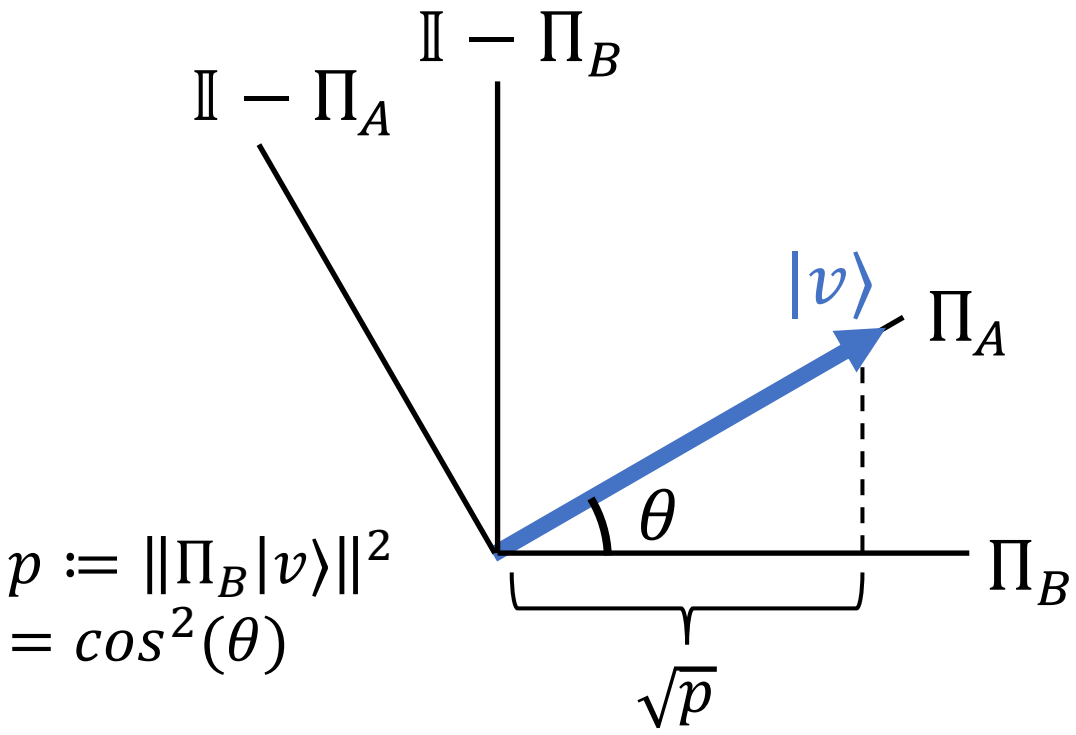
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

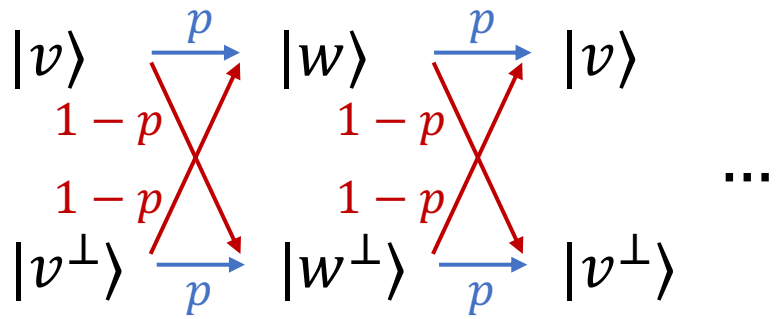
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

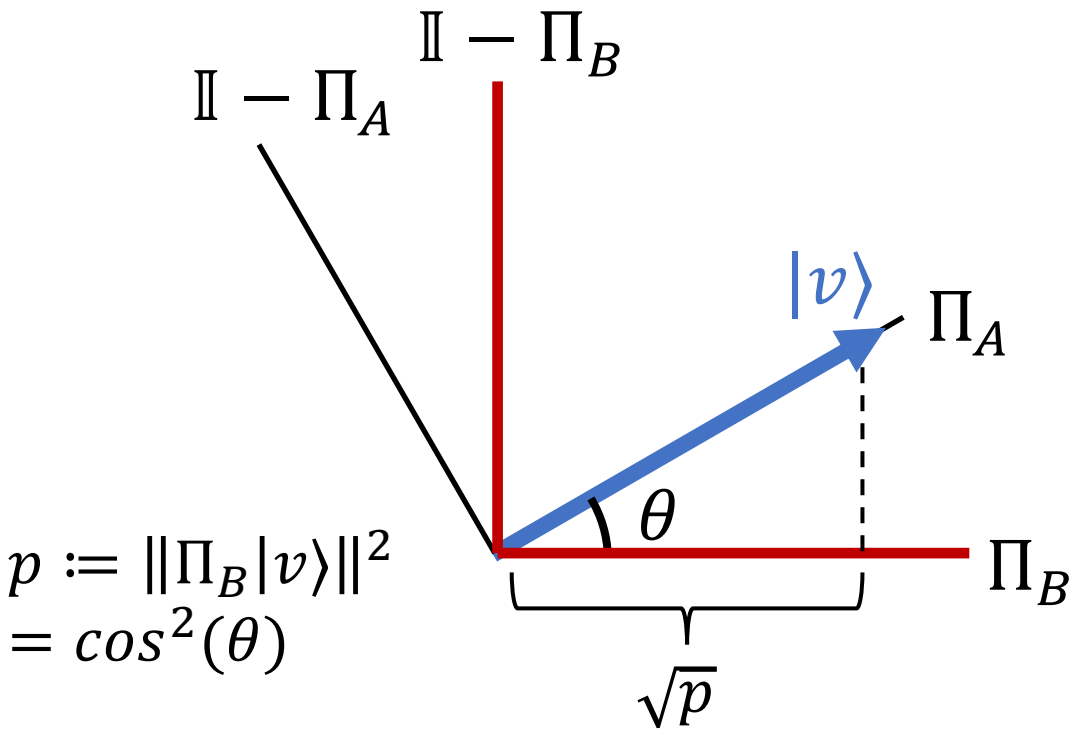
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

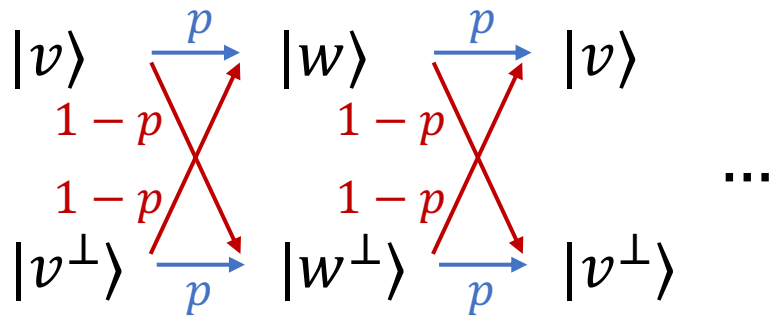
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

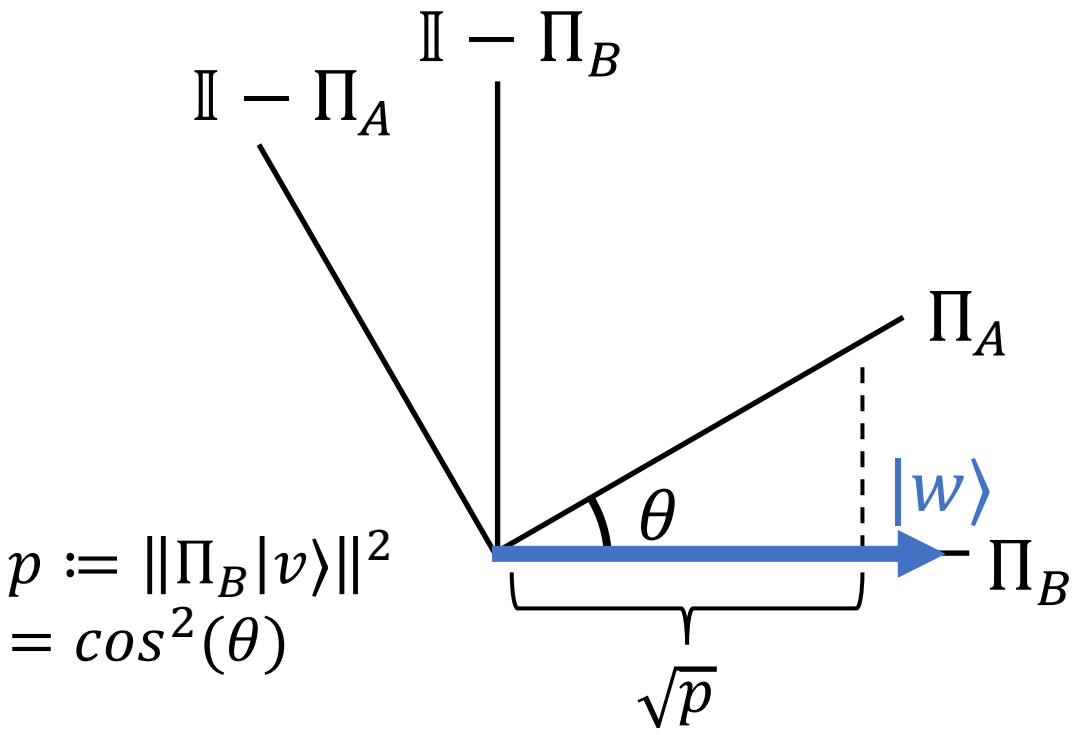
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

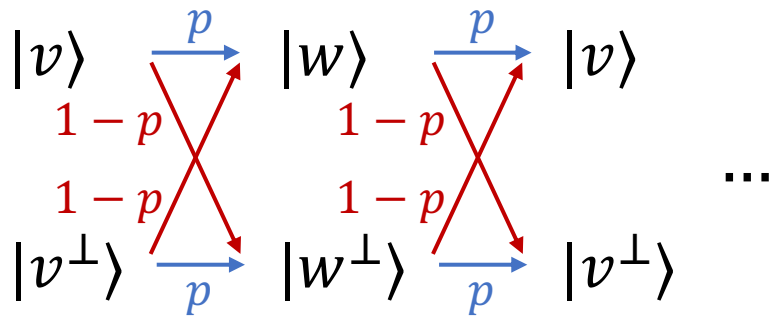
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

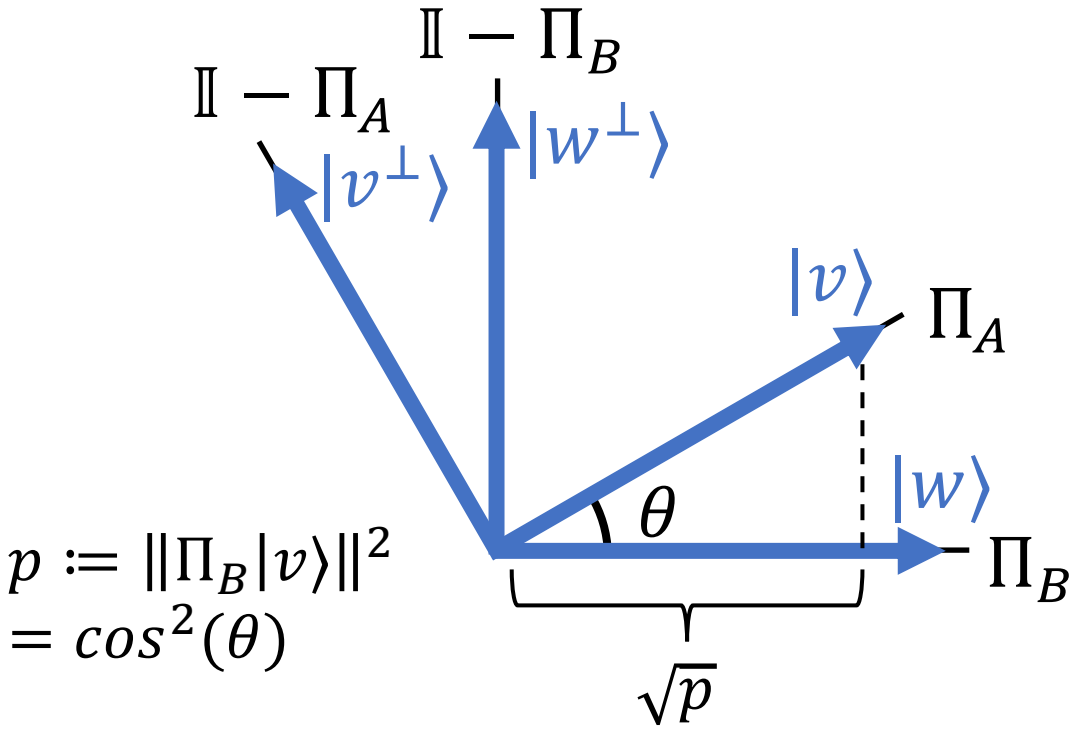
When we alternate measurements, we jump between four states



# Understanding Alternating Measurements [MW05]

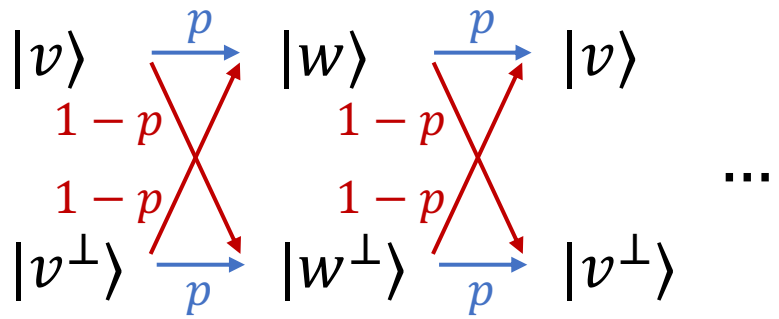
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

When we alternate measurements, we jump between four states

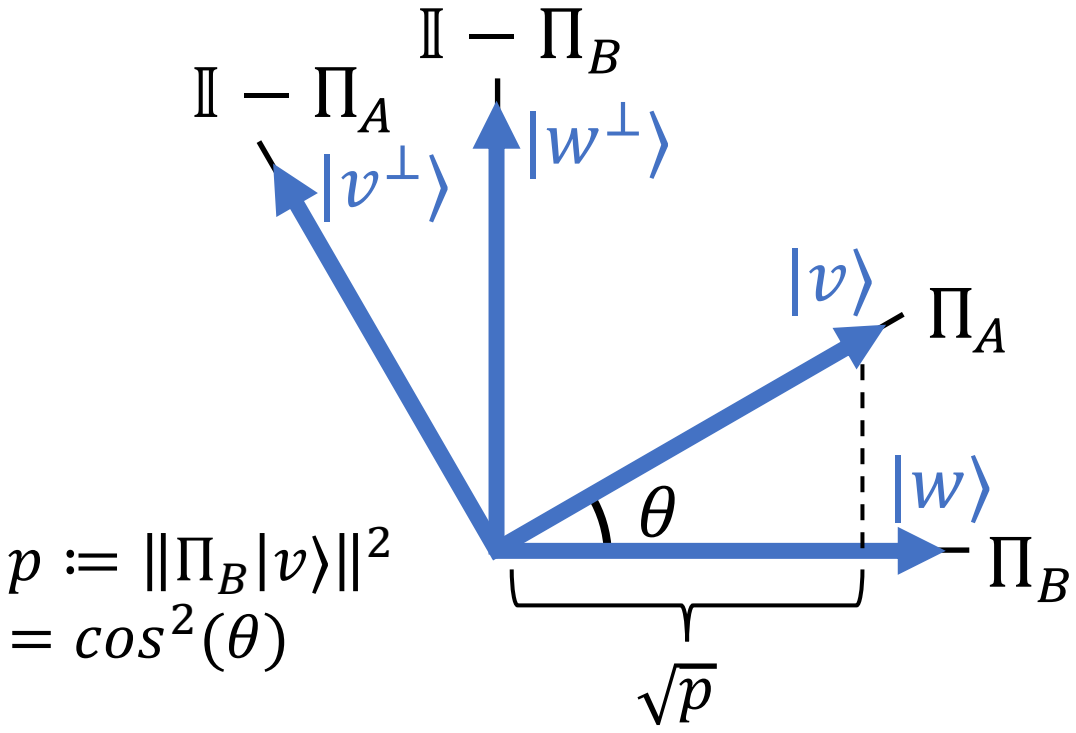



Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-o(\lambda)}$.

# Understanding Alternating Measurements [MW05]

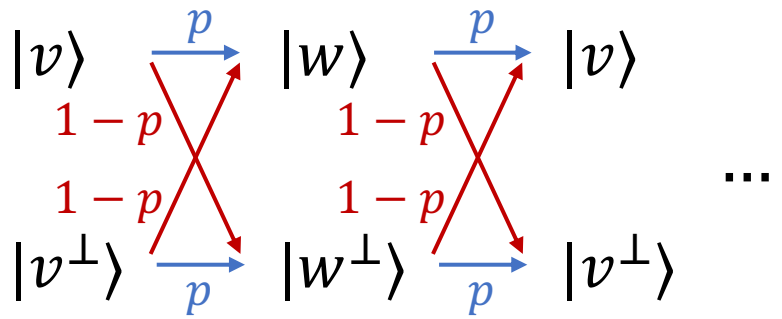
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

When we alternate measurements, we jump between four states



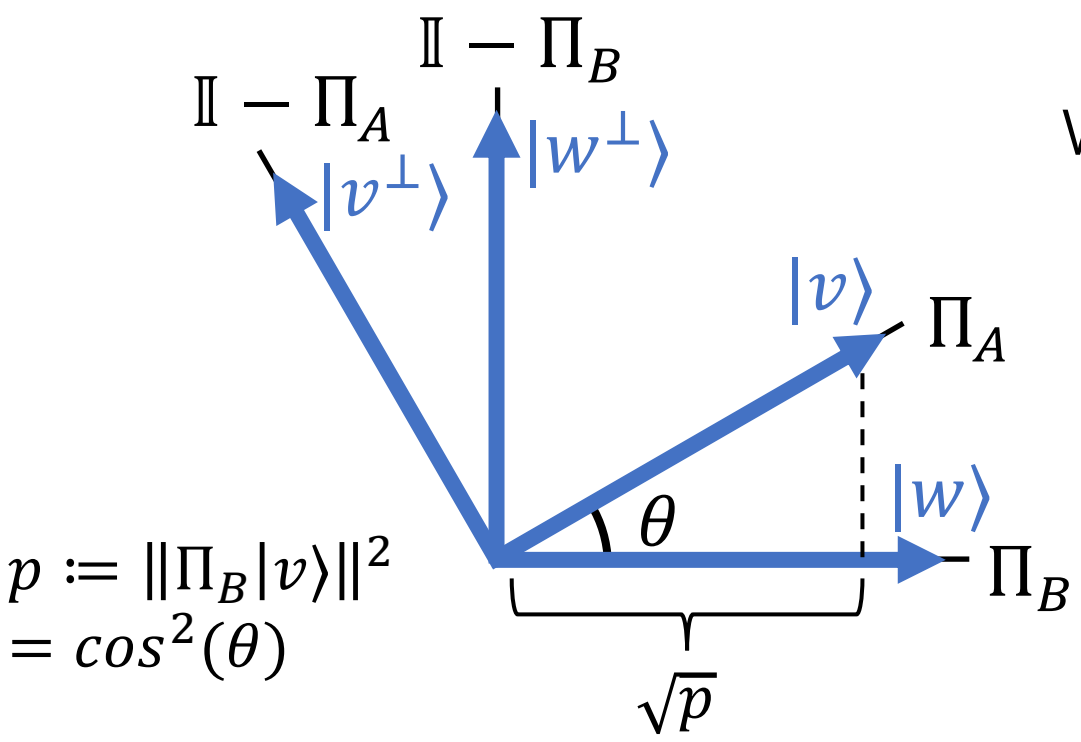

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-o(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

# Understanding Alternating Measurements [MW05]

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: $\Pi_A, \Pi_B$ live in 2D




$p := \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

These are the guarantees we want, but $\Pi_0, \Pi_G$ don't live in 2D!

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-o(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If $\Pi_A, \Pi_B$ live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If $\Pi_A, \Pi_B$ live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Do these claims extend to higher dimensions?

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If $\Pi_A, \Pi_B$ live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Do these claims extend to higher dimensions?

- For general $\Pi_A, \Pi_B$: no!

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If $\Pi_A, \Pi_B$ live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Do these claims extend to higher dimensions?

- For general $\Pi_A, \Pi_B$: no!
- For $\Pi_0, \Pi_G$: yes!

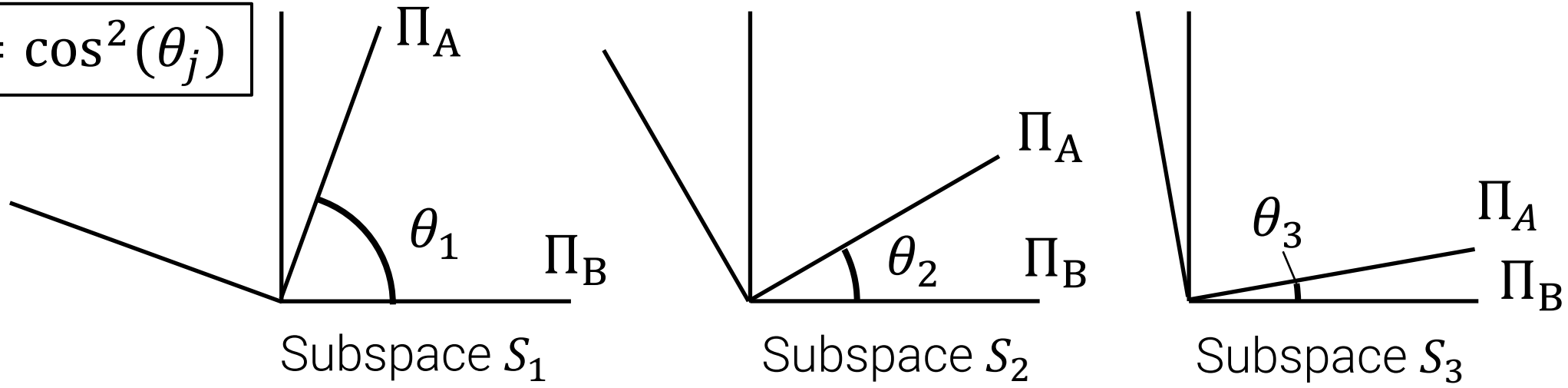
# Extremely Useful Tool

Jordan's Lemma: For any $\Pi_A, \Pi_B$, we can decompose space into 2-dim invariant subspaces $\{S_j\}$ where $\Pi_A$, $\Pi_B$ are rank-one projectors in each $S_j$.

# Extremely Useful Tool

Jordan's Lemma: For any $\Pi_A, \Pi_B$, we can decompose space into 2-dim invariant subspaces $\{S_j\}$ where $\Pi_A$, $\Pi_B$ are rank-one projectors in each $S_j$.

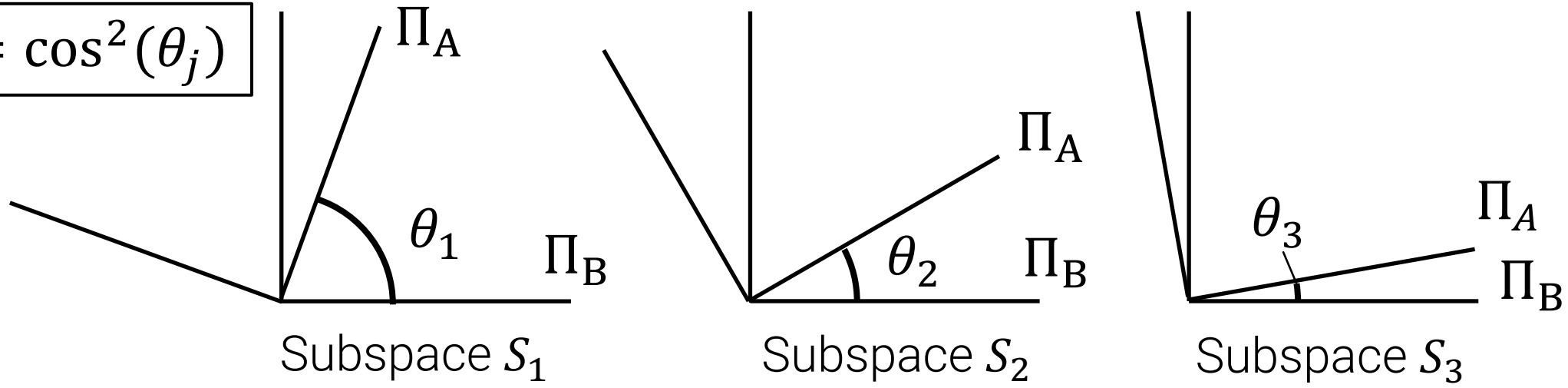
$$p_j = \cos^2(\theta_j)$$



# Extremely Useful Tool

Jordan's Lemma: For any $\Pi_A, \Pi_B$, we can decompose space into 2-dim invariant subspaces $\{S_j\}$ where $\Pi_A$, $\Pi_B$ are rank-one projectors in each $S_j$.

$$p_j = \cos^2(\theta_j)$$




To analyze our simulator, it will be helpful to understand the Jordan subspace decomposition for $\Pi_0, \Pi_G$.

**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

Why? This is an immediate consequence of hiding.

**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

Why? This is an immediate consequence of hiding.

1) Since $\Pi_0 = |0\rangle\langle 0|_{Aux}$, can write $|\phi\rangle = |\psi\rangle_V|0\rangle_{Aux}$.

**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

Why? This is an immediate consequence of hiding.

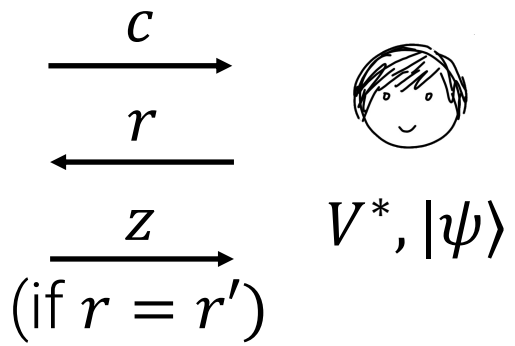
1) Since $\Pi_0 = |0\rangle\langle 0|_{Aux}$, can write $|\phi\rangle = |\psi\rangle_V|0\rangle_{Aux}$.
2) $\|\Pi_G|\psi\rangle_V|0\rangle_{Aux}\|^2$ is the probability $\mathbf{Guess}(V^*, |\psi\rangle)$ succeeds:

**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

Why? This is an immediate consequence of hiding.

1) Since $\Pi_0 = |0\rangle\langle 0|_{Aux}$, can write $|\phi\rangle = |\psi\rangle_V|0\rangle_{Aux}$.
2) $\|\Pi_G|\psi\rangle_V|0\rangle_{Aux}\|^2$ is the probability $\mathbf{Guess}(V^*, |\psi\rangle)$ succeeds:

$\mathbf{Guess}(V^*, |\psi\rangle)$:
1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$
2) If $r = r'$, output $(c, r, z)$. Otherwise $\perp$.

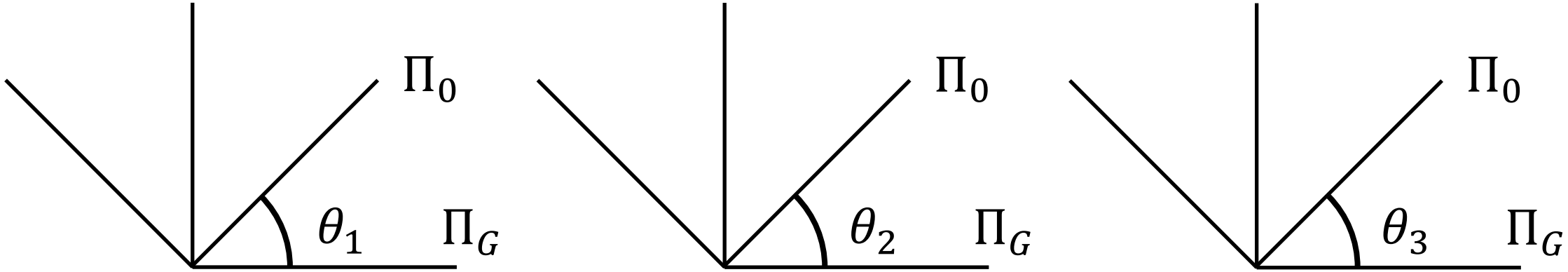


**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

Equivalently, $p_j \approx 1/2$ in every Jordan subspace $S_j$ (so $\theta_j \approx \pi/4$).

**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

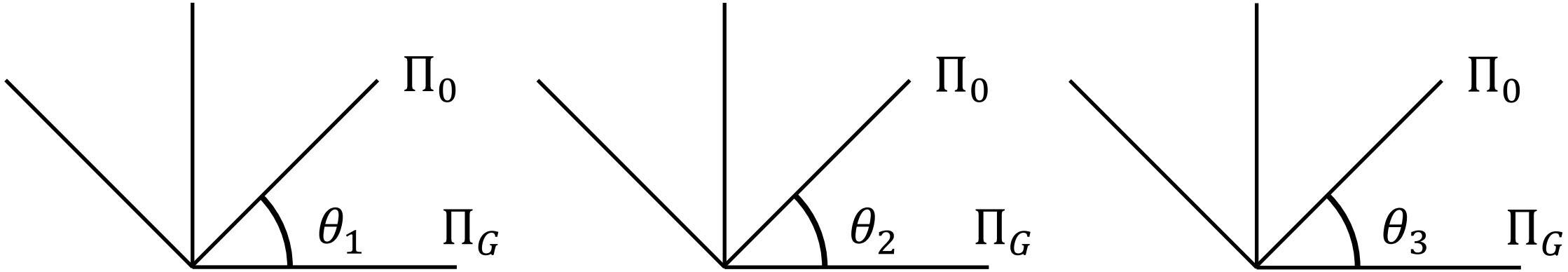
Equivalently, $p_j \approx 1/2$ in every Jordan subspace $S_j$ (so $\theta_j \approx \pi/4$).




$$p_j = \cos^2(\theta_j)$$

**Key Fact:** for any $|\phi\rangle \in \mathbf{image}(\Pi_0)$, we have $\|\Pi_G|\phi\rangle\|^2 \approx 1/2$.

Equivalently, $p_j \approx 1/2$ in every Jordan subspace $S_j$ (so $\theta_j \approx \pi/4$).




$$p_j = \cos^2(\theta_j)$$

We can now extend the 2-D analysis to our simulator!

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Previously, we claimed the following for $\Pi_A, \Pi_B$ in 2-D:

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Previously, we claimed the following for $\Pi_A, \Pi_B$ in 2-D:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-o(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Previously, we claimed the following for $\Pi_A, \Pi_B$ in 2-D:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

These claims extend to high-dim if all $(\Pi_A, \Pi_B)$-Jordan subspaces have roughly equal $p_j$.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\approx \lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\approx \lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Intuition for Claim 1: the 2-D runtime analysis extends to higher dimensions because the $\Pi_A, \Pi_B$ measurements act independently on each Jordan subspace.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\approx \lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Intuition for Claim 2:

- Consider $|v\rangle = \sum_j \alpha_j |v_j\rangle$. In each $S_j$, the state after $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts is $\propto \Pi_B|v_j\rangle$ by our analysis of the 2-D case.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\approx \lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Intuition for Claim 2:

- Consider $|v\rangle = \sum_j \alpha_j |v_j\rangle$. In each $S_j$, the state after $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts is $\propto \Pi_B|v_j\rangle$ by our analysis of the 2-D case.
- Alternating measurement results only depend on $p_j$, but since all $p_j \approx p$, the measurement outcomes give no signal about $j$.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\approx \lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Intuition for Claim 2:

- Consider $|v\rangle = \sum_j \alpha_j |v_j\rangle$. In each $S_j$, the state after $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts is $\propto \Pi_B|v_j\rangle$ by our analysis of the 2-D case.
- Alternating measurement results only depend on $p_j$, but since all $p_j \approx p$, the measurement outcomes give no signal about $j$.
- So the final state is $\propto \sum_j \alpha_j \Pi_B |v_j\rangle = \Pi_B|v\rangle$.

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\approx \lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Since $\Pi_0$ and $\Pi_G$ satisfy $p_j \approx 1/2$ in all Jordan subspaces, we can set $\Pi_A = \Pi_0$ and $\Pi_B = \Pi_G$ to analyze the alternating measurements simulator:

What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

If all $(\Pi_A, \Pi_B)$-Jordan subspaces have $p_j \approx p$, then:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in $\approx \lambda/p$ steps with prob $1 - 2^{-O(\lambda)}$.

Claim 2: When $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts, state is $|w\rangle \propto \Pi_B|v\rangle$.

Since $\Pi_0$ and $\Pi_G$ satisfy $p_j \approx 1/2$ in all Jordan subspaces, we can set $\Pi_A = \Pi_0$ and $\Pi_B = \Pi_G$ to analyze the alternating measurements simulator:

- By Claim 1, the simulator is efficient.
- By Claim 2, when $M_G \to 1$, the state is $\propto \Pi_G|\psi\rangle|0\rangle$ as desired.

# Technical Recap

We showed that Blum's protocol is post-quantum PoK and ZK.

# Technical Recap

We showed that Blum's protocol is post-quantum PoK and ZK.

Proof of knowledge:

- Collapse-binding commitments enable "lazy" measurement

# Technical Recap

We showed that Blum's protocol is post-quantum PoK and ZK.

Proof of knowledge:

- Collapse-binding commitments enable "lazy" measurement
- Unruh's lemma: if protocol is collapsing, can record ***two*** accepting transcripts given a $p$-successful adversary (with probability $p^3$)

# Technical Recap

We showed that Blum's protocol is post-quantum PoK and ZK.

Proof of knowledge:

- Collapse-binding commitments enable "lazy" measurement
- Unruh's lemma: if protocol is collapsing, can record ***two*** accepting transcripts given a $p$-successful adversary (with probability $p^3$)

Zero knowledge:

- Key tool: obtain a quantum analogue of the classical "repeated-guessing" simulator using alternating projectors.

# Technical Recap

We showed that Blum's protocol is post-quantum PoK and ZK.

Proof of knowledge:

- Collapse-binding commitments enable "lazy" measurement
- Unruh's lemma: if protocol is collapsing, can record ***two*** accepting transcripts given a $p$-successful adversary (with probability $p^3$)

Zero knowledge:

- Key tool: obtain a quantum analogue of the classical "repeated-guessing" simulator using alternating projectors.
- Analyze alternating projectors via Jordan's lemma

Thank You!

Questions?