Quantum Rewinding Tutorial Part 1:

Motivation and Early Quantum Rewinding Techniques

Alex Lombardi
(MIT → Simons & Berkeley)

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)

How do cryptographers prove security?

How do cryptographers prove security?

Crypto Security Proof = (Assumed) Hard Problem + Reduction

How do cryptographers prove security?

Crypto Security Proof = (Assumed) Hard Problem + Reduction

Ex: one-way function, factoring, discrete log, etc.

How do cryptographers prove security?

Crypto Security Proof $=$ (Assumed) Hard Problem $+$ Reduction

Ex: one-way function, factoring, discrete log, etc.

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

How do cryptographers prove security?

Crypto Security Proof = (Assumed) Hard Problem + Reduction

Ex: one-way function, ~~factoring~~, ~~discrete log~~, etc.

Efficient A wins security game
→ efficient A' solves hard problem

Key point: problem must be hard for quantum computers!

How do cryptographers prove security?

Crypto Security Proof = (Assumed) 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?

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

Ex: learning with errors (LWE), isogenies, OWF

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?

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

Ex: learning with errors (LWE), isogenies, OWF

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.

Done?

Conjecture

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

Conjecture

Classical security reduction + quantum-hard problem

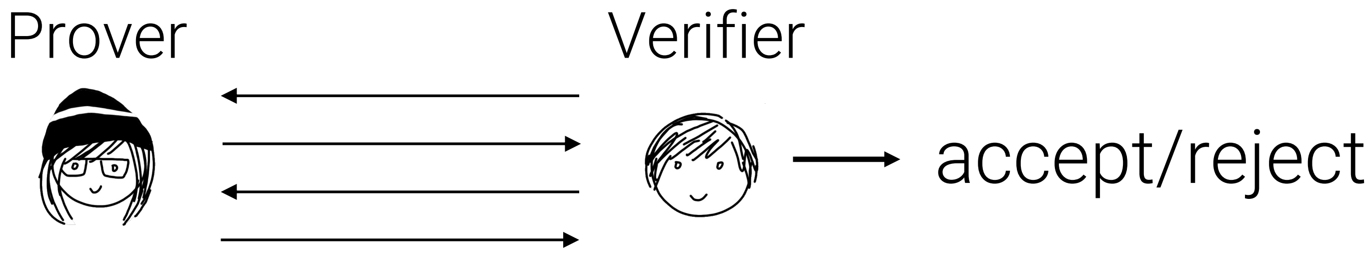
→ post-quantum security?

No!

Conjecture
Classical security reduction + quantum-hard problem
→ post-quantum security?

No!

[BCMVV18]
Protocol

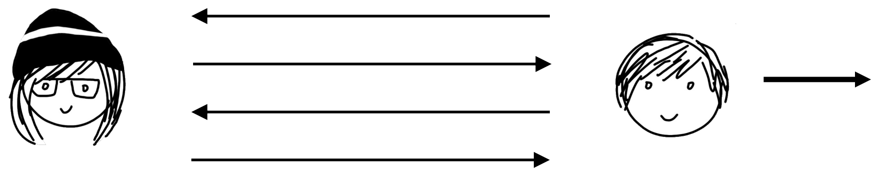


Conjecture
Classical security reduction + quantum-hard problem
→ post-quantum security?

No!

[BCMVV18]
Protocol

Prover Verifier



accept/reject

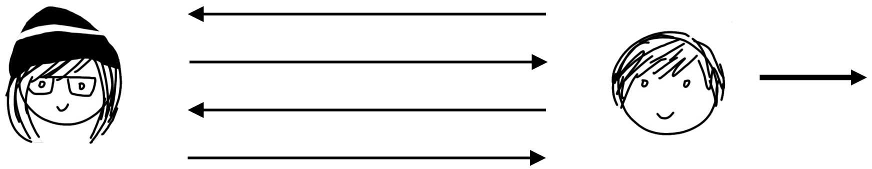
- Efficient classical P *cannot* make V accept assuming LWE

Conjecture
Classical security reduction + quantum-hard problem
→ post-quantum security?

No!

[BCMVV18] Protocol

Prover Verifier



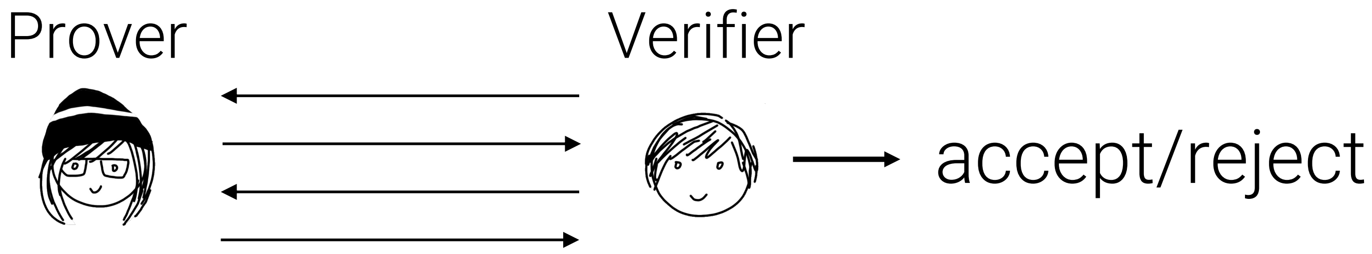
accept/reject

- 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!

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 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*

[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*

$\xrightarrow{a}$

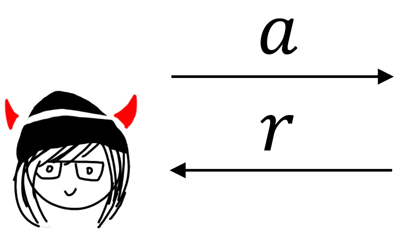
[BCMVV18] Reduction

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***



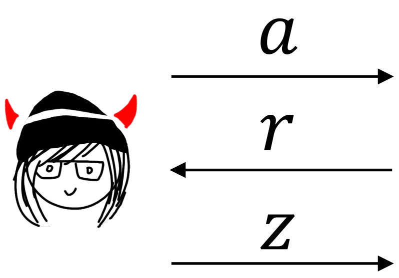
[BCMVV18] Reduction

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***



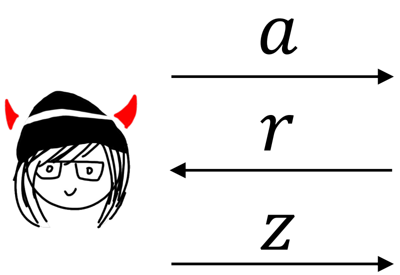
[BCMVV18] Reduction

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

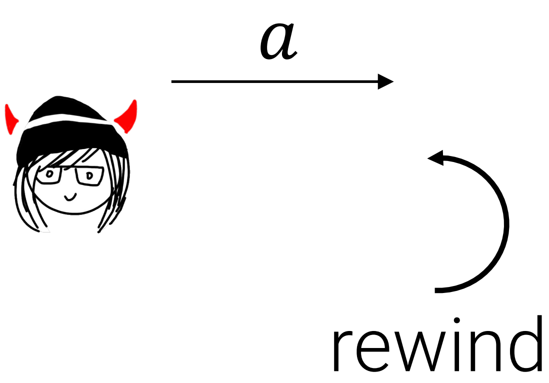
1) Record (a, r, z)

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

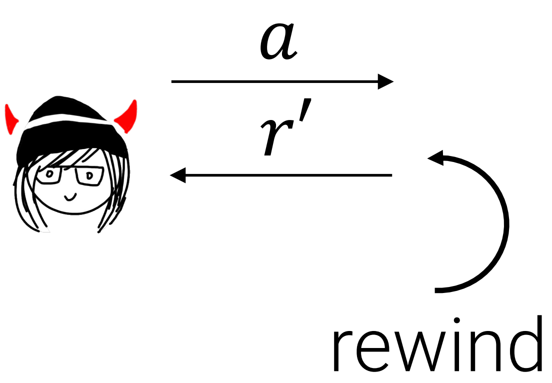
1) Record (a, r, z)
2) Rewind

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

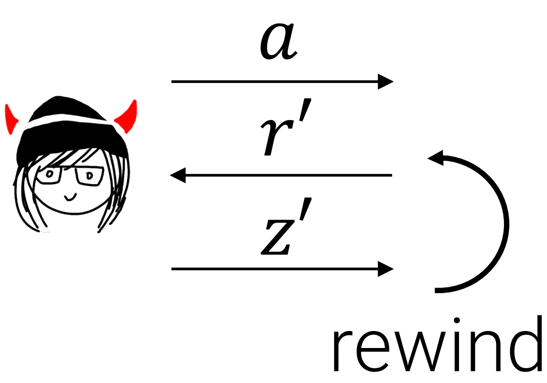
1) Record (a, r, z)
2) Rewind

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

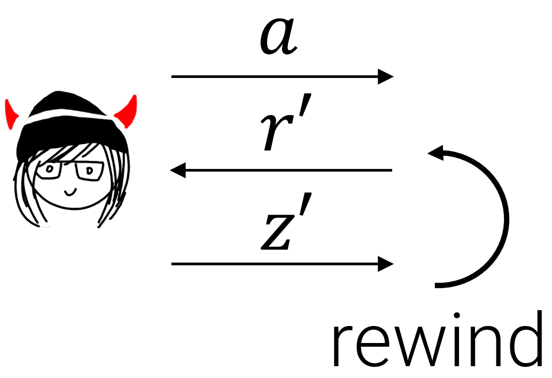
1) Record (a, r, z)
2) Rewind

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

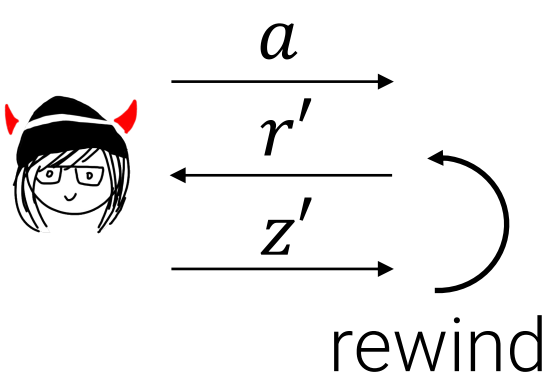
1) Record (a, r, z)
2) Rewind
3) Record (a, r', z')

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')

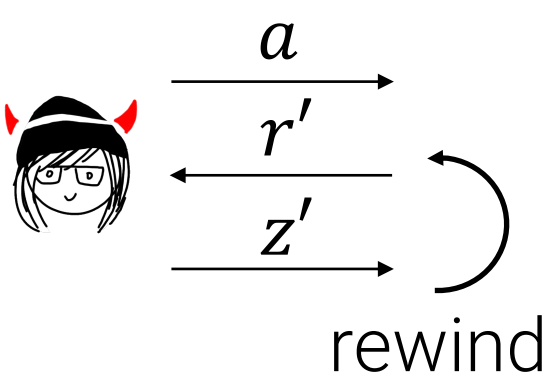
$\xrightarrow{\text{break LWE}}$

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')

$\xrightarrow{\text{break LWE}}$

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*

$\xrightarrow{a}$

$\xleftarrow{r'}$

$\xrightarrow{\cancel{z'}}$

rewind

[BCMVV18] Reduction

1) Record (a, r, z)
2) Rewind
3) ~~Record~~ $\cancel{(a, r', z')}$

~~break LWE~~ $\longrightarrow$

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

[BCMVV18] is "quantum broken"

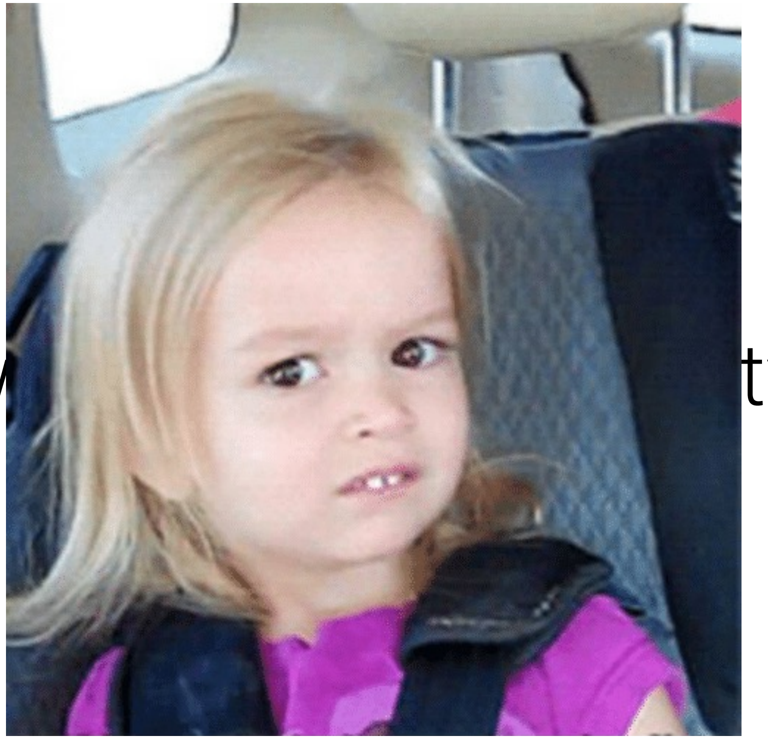
More generally, rewinding-based security proofs are not safe!

[BCMVV18] is “quantum broken”

More generally, rewinding-based security proofs are not safe!

But rewinding is one of the most common techniques in cryptography…

[BCMVV18] is "quantum broken"



More generally, rew ty proofs are not safe!

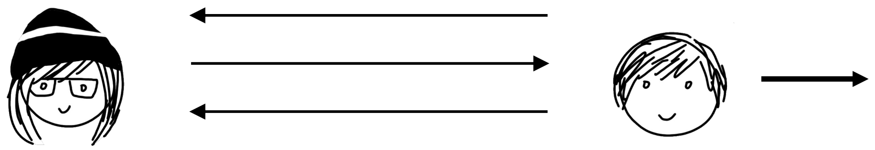
But rewinding is one of the most common techniques in cryptography…

Question for today:

When is quantum rewinding possible?

Claim: $x \in 3\text{SAT}$

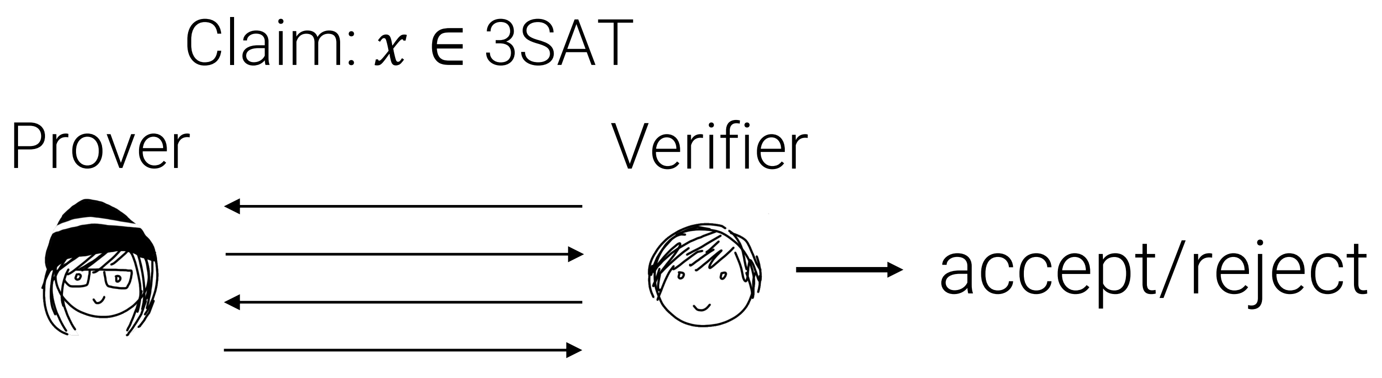
Prover Verifier



accept/reject

Question for today:

When is quantum rewinding possible?

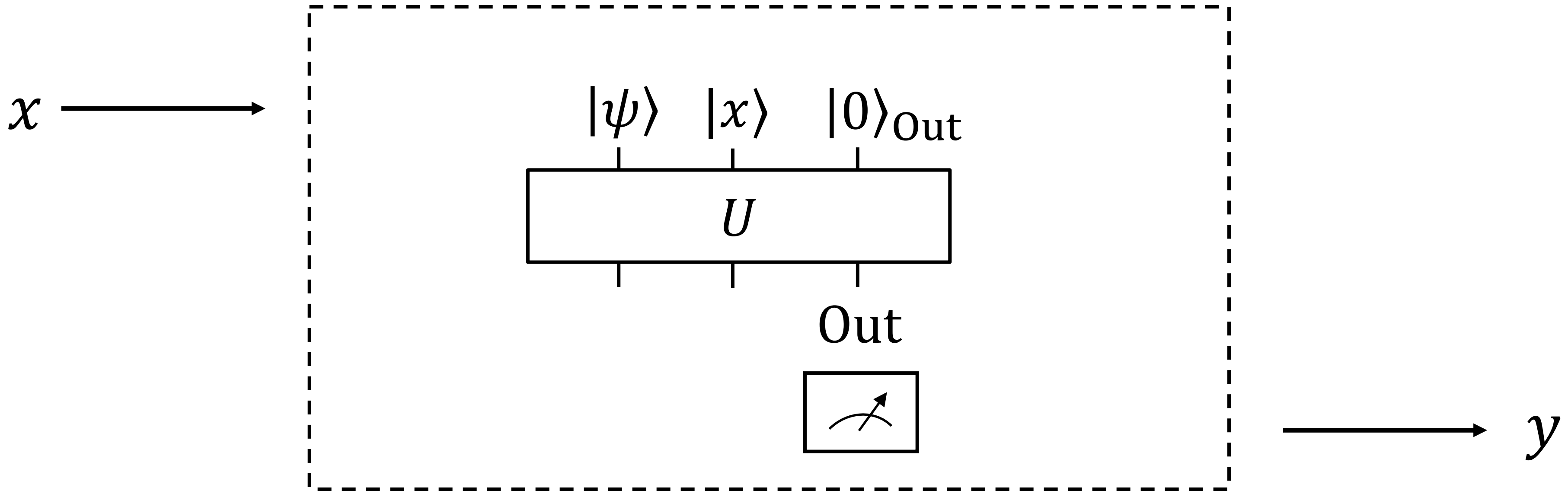


Soundness: Malicious P can't trick V into accepting a false claim.

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

Preliminaries: Quantum Adversary Model

(Non-Uniform) Quantum Adversary consists of efficiently computable and invertible U along with a measurement in the standard basis



(One-shot case) equivalent to efficient quantum circuit.

Interactive adversary will be stateful.

This Talk

1) Blum's protocol for graph Hamiltonicity

2) Post-Quantum Soundness of Blum

3) Post-Quantum Zero Knowledge of Blum

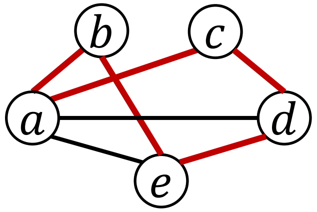
This Talk

1) Blum's protocol for graph Hamiltonicity

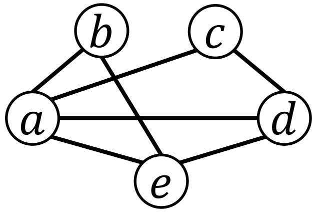
2) Post-Quantum Soundness of Blum

3) Post-Quantum Zero Knowledge of Blum

Blum's Protocol for Hamiltonian Cycles

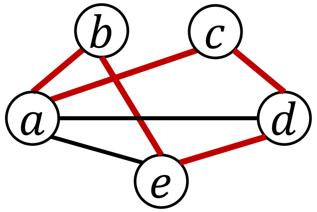
$G =$ 

Prover 

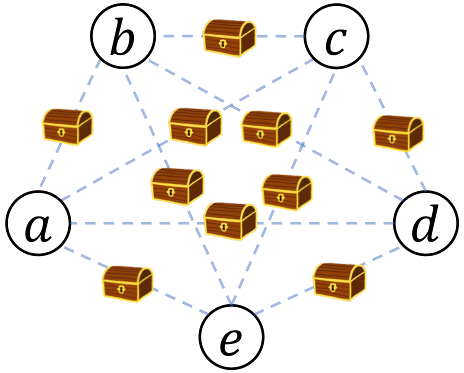
$G =$ 

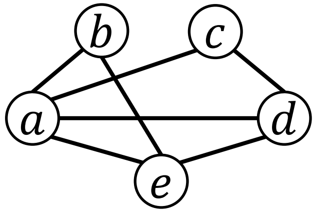
Verifier 

Blum's Protocol for Hamiltonian Cycles

$G =$ 

Prover 



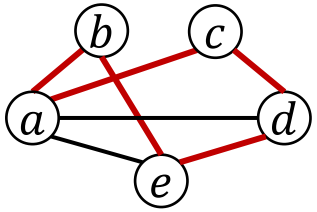
$G =$ 

Verifier 

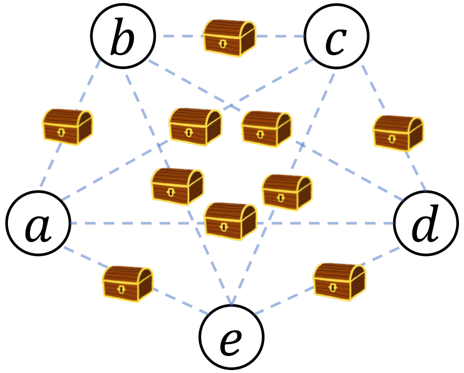
Sample $\pi \leftarrow S_V$.

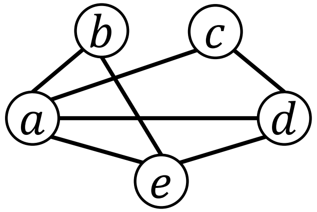
Commit to the adjacency matrix of $\pi(G)$

Blum's Protocol for Hamiltonian Cycles

$G =$ 

Prover 



$G =$ 

Verifier 

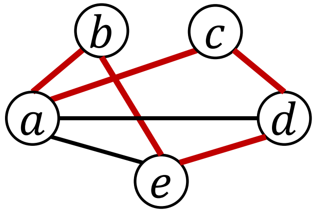
Sample $\pi \leftarrow S_V$.

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

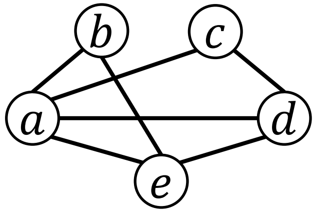
r

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

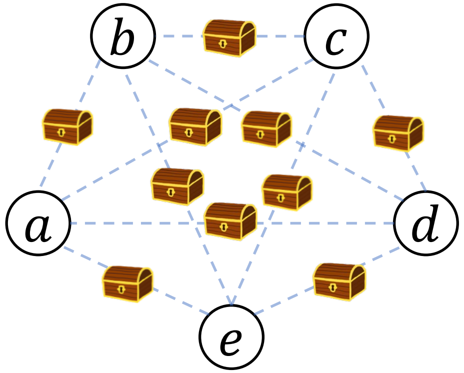
Blum's Protocol for Hamiltonian Cycles

$G =$ 

Prover 

$G =$ 

Verifier 

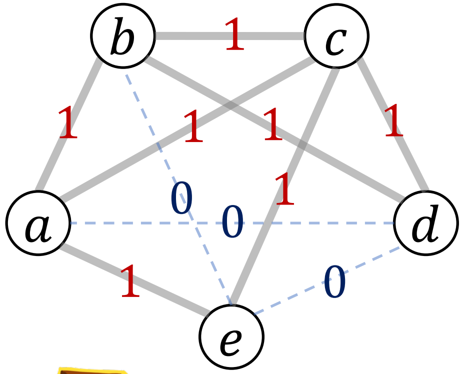


Sample $\pi \leftarrow S_V$.

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

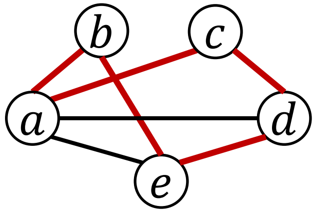
r

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

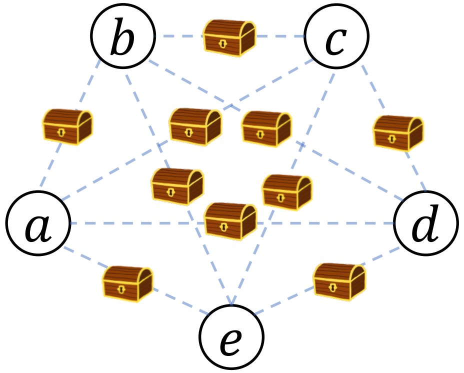
$\pi,$ 

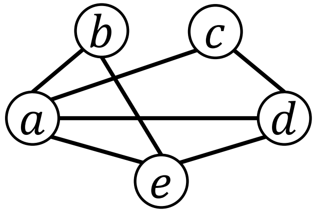
 (if $r = 0$)

Blum's Protocol for Hamiltonian Cycles

$G =$ 

Prover 



$G =$ 

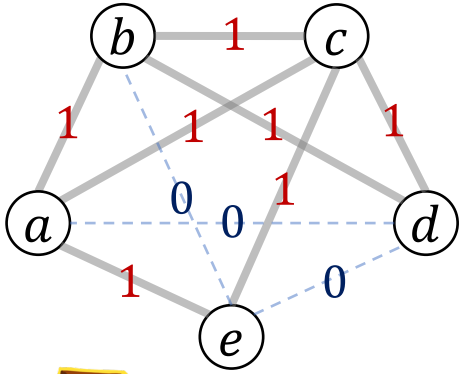
Verifier 

Sample $\pi \leftarrow S_V$.

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

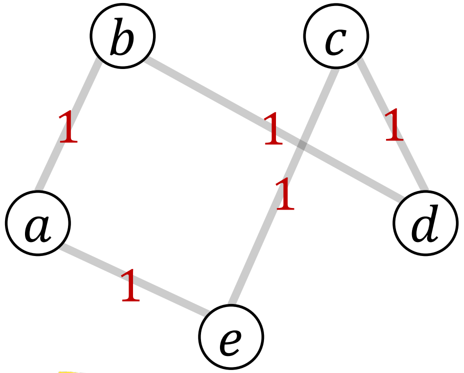
r

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

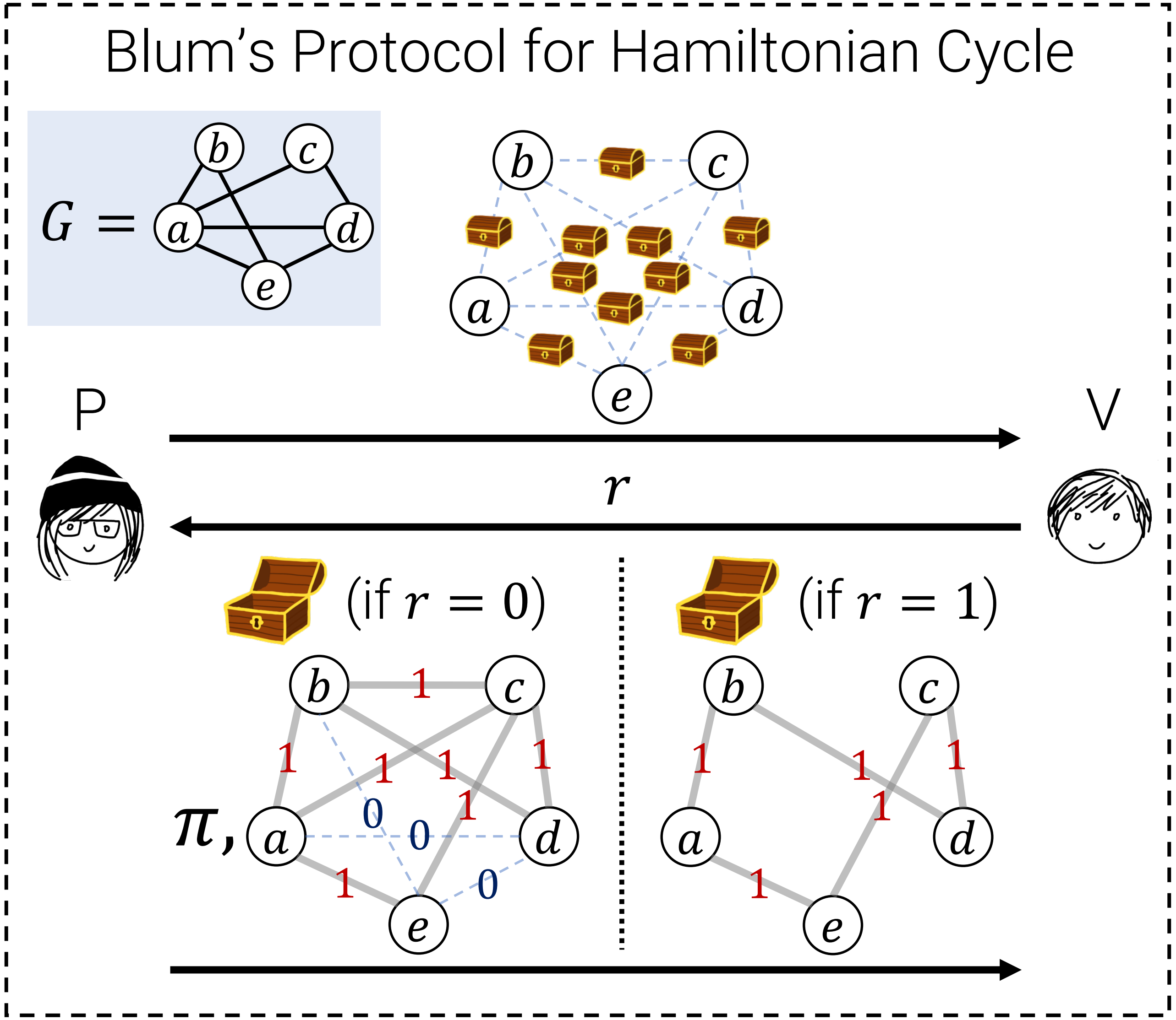
π, 

 (if $r = 0$)

or



 (if $r = 1$)

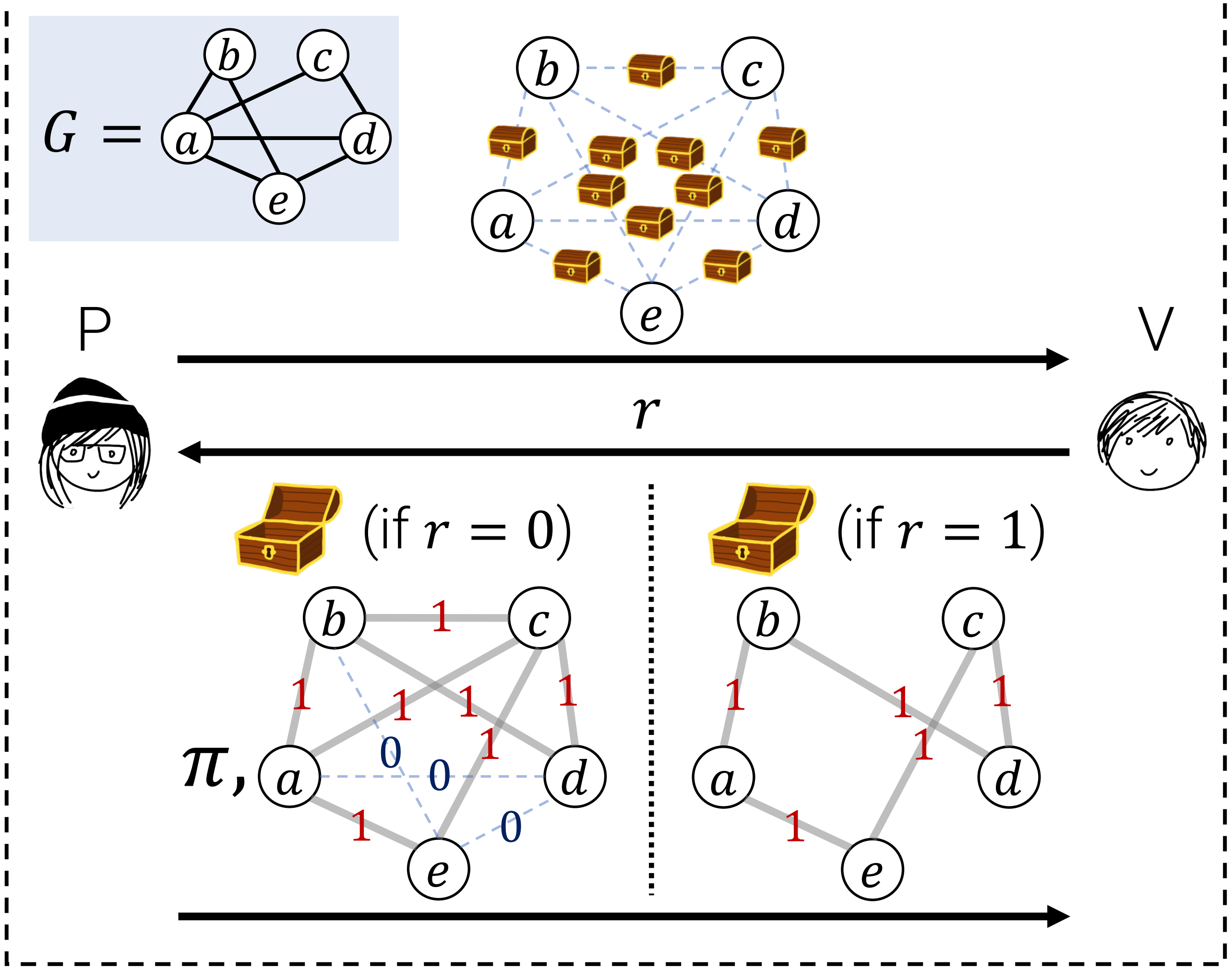


Soundness (intuition)

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



Soundness (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

This Talk

1) Blum's protocol for graph Hamiltonicity ✓

2) Post-Quantum Soundness of Blum

3) Post-Quantum Zero Knowledge of Blum

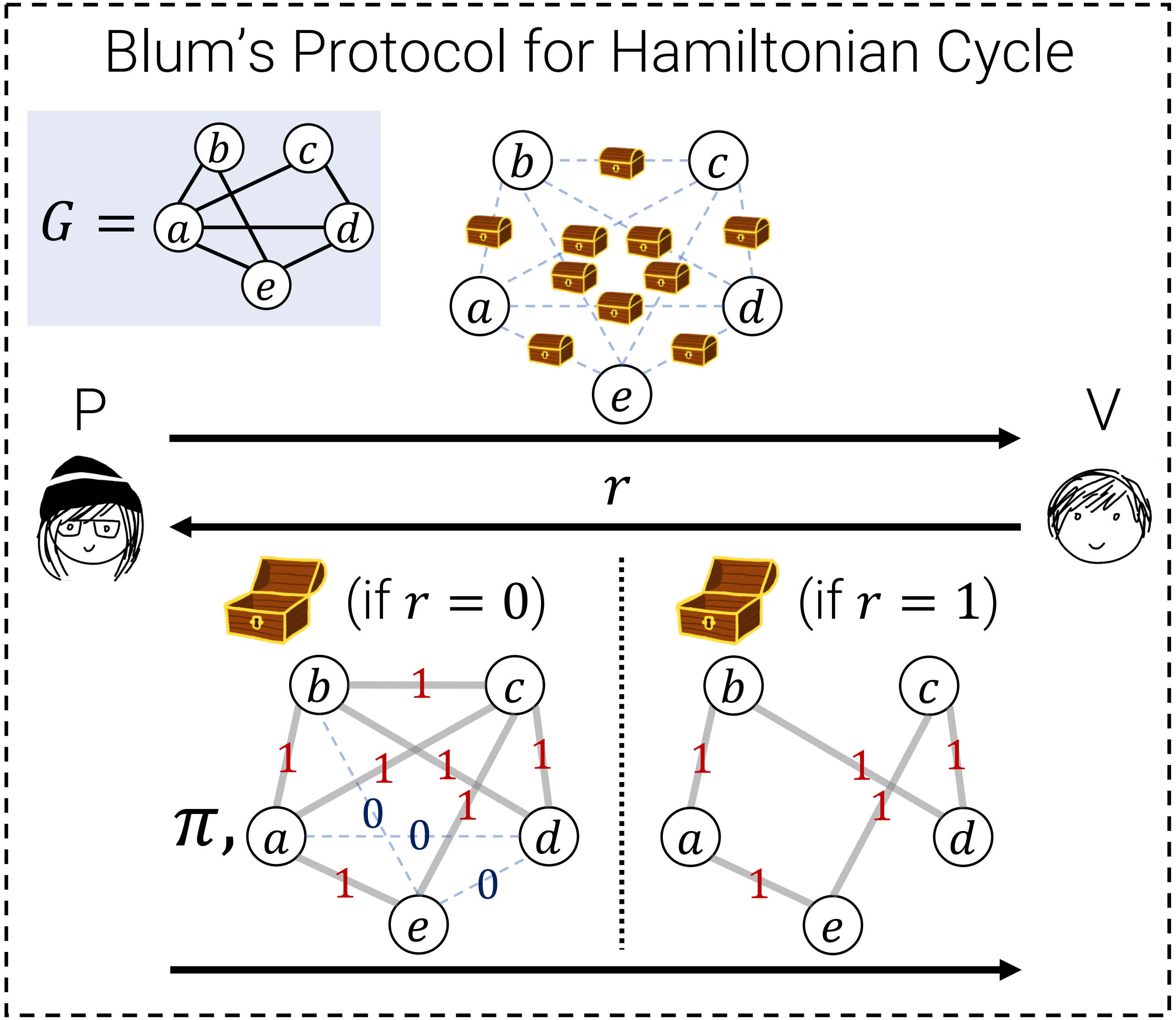
This Talk

1) Blum's protocol for graph Hamiltonicity ✓

2) Post-Quantum Soundness of Blum

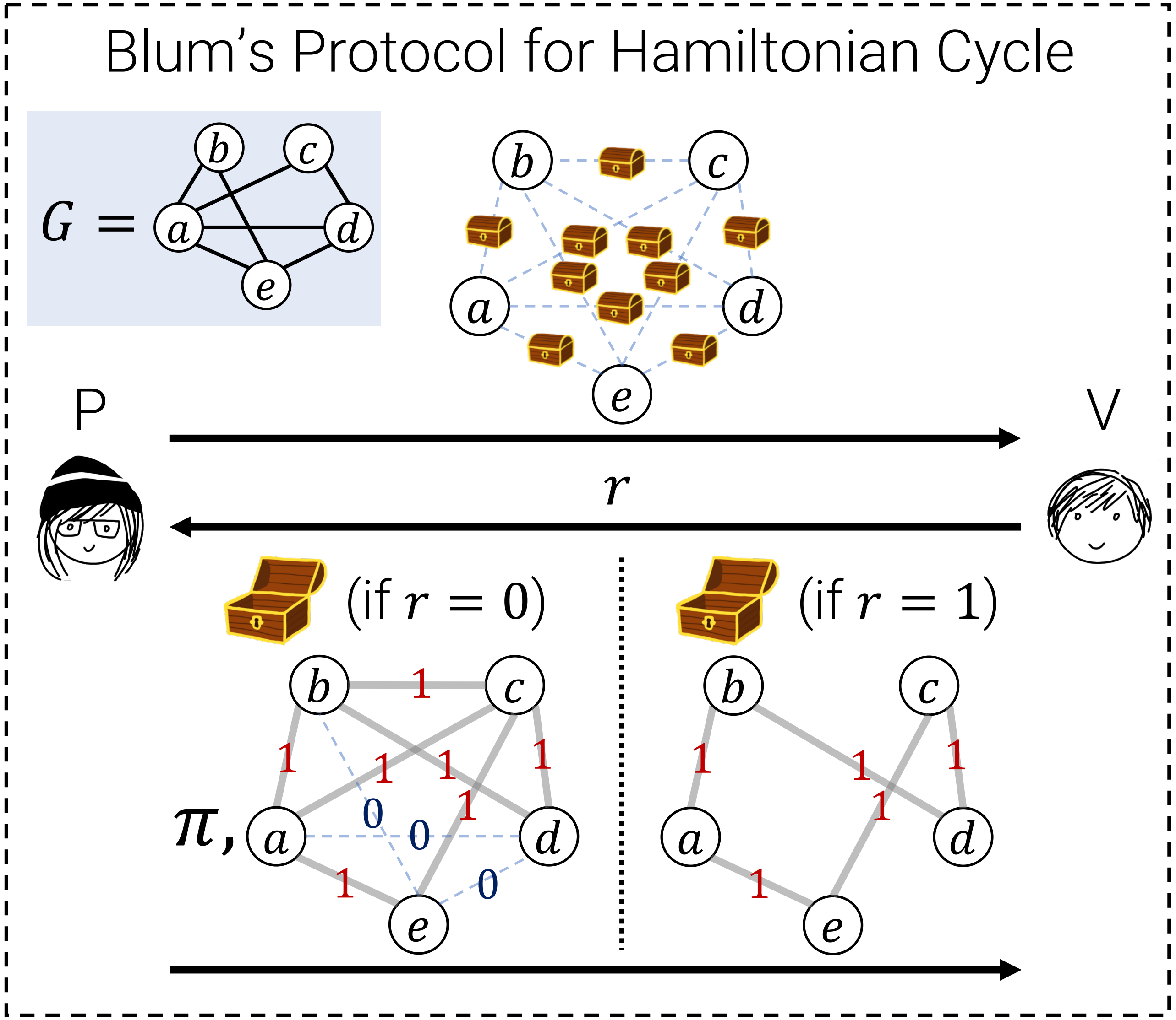
- Classical soundness
- Collapse-binding commitments
- Unruh's rewinding lemma

3) Post-Quantum Zero Knowledge of Blum



Classical Soundness

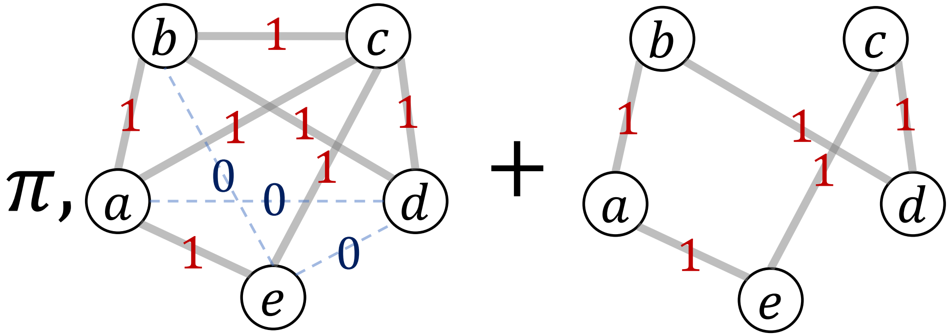
Soundness: If efficient classical P* convinces V with prob $\frac{1}{2} + \varepsilon$, then G must have a Ham cycle.

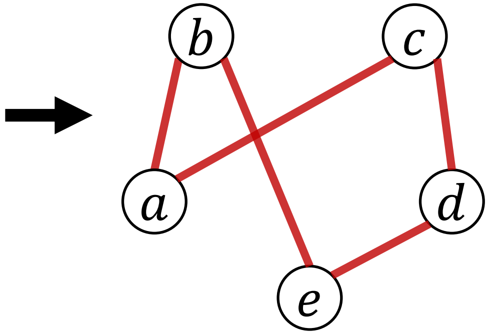


Classical Soundness

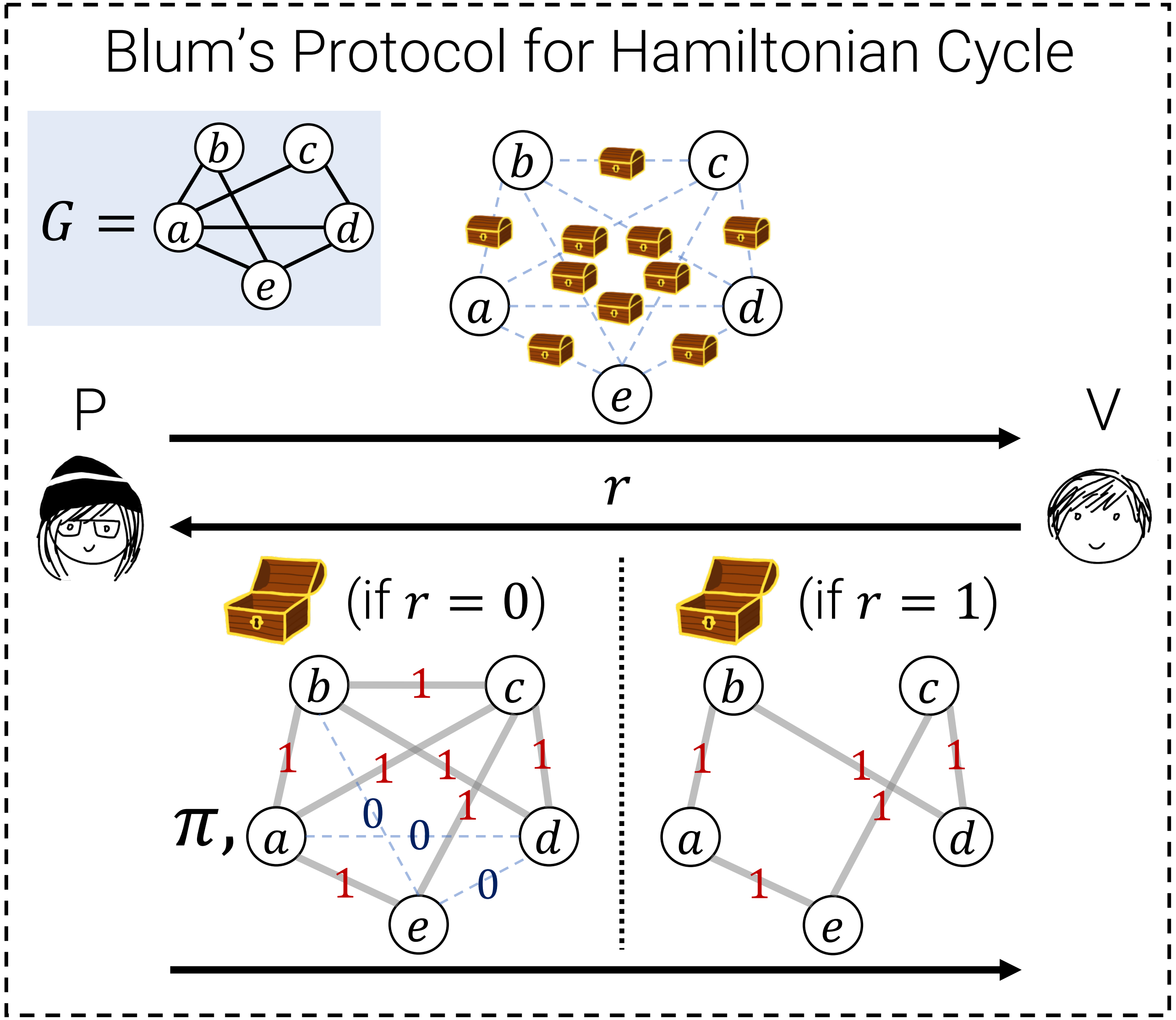
Soundness: If efficient classical P* convinces V with prob $\frac{1}{2} + \varepsilon$, then G must have a Ham cycle.

2-special soundness: Two valid transcripts → Ham cycle





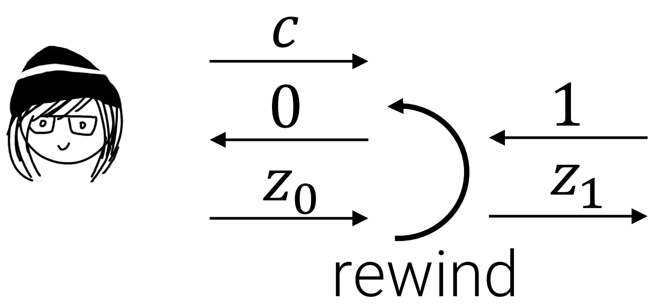
Ham cycle for original G



Classical Soundness

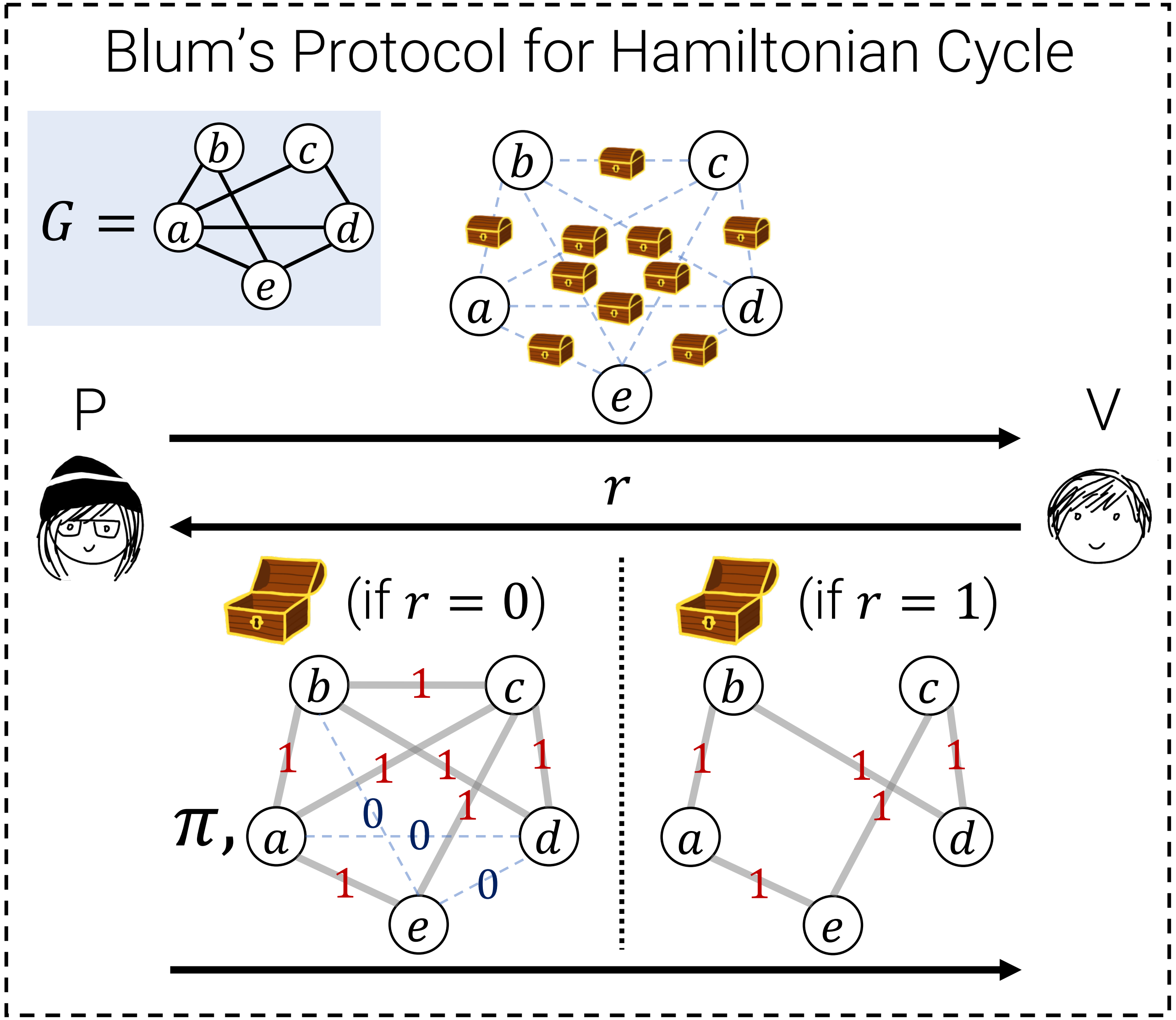
Soundness: If efficient classical P* convinces V with prob $\frac{1}{2} + \varepsilon$, then G must have a Ham cycle.

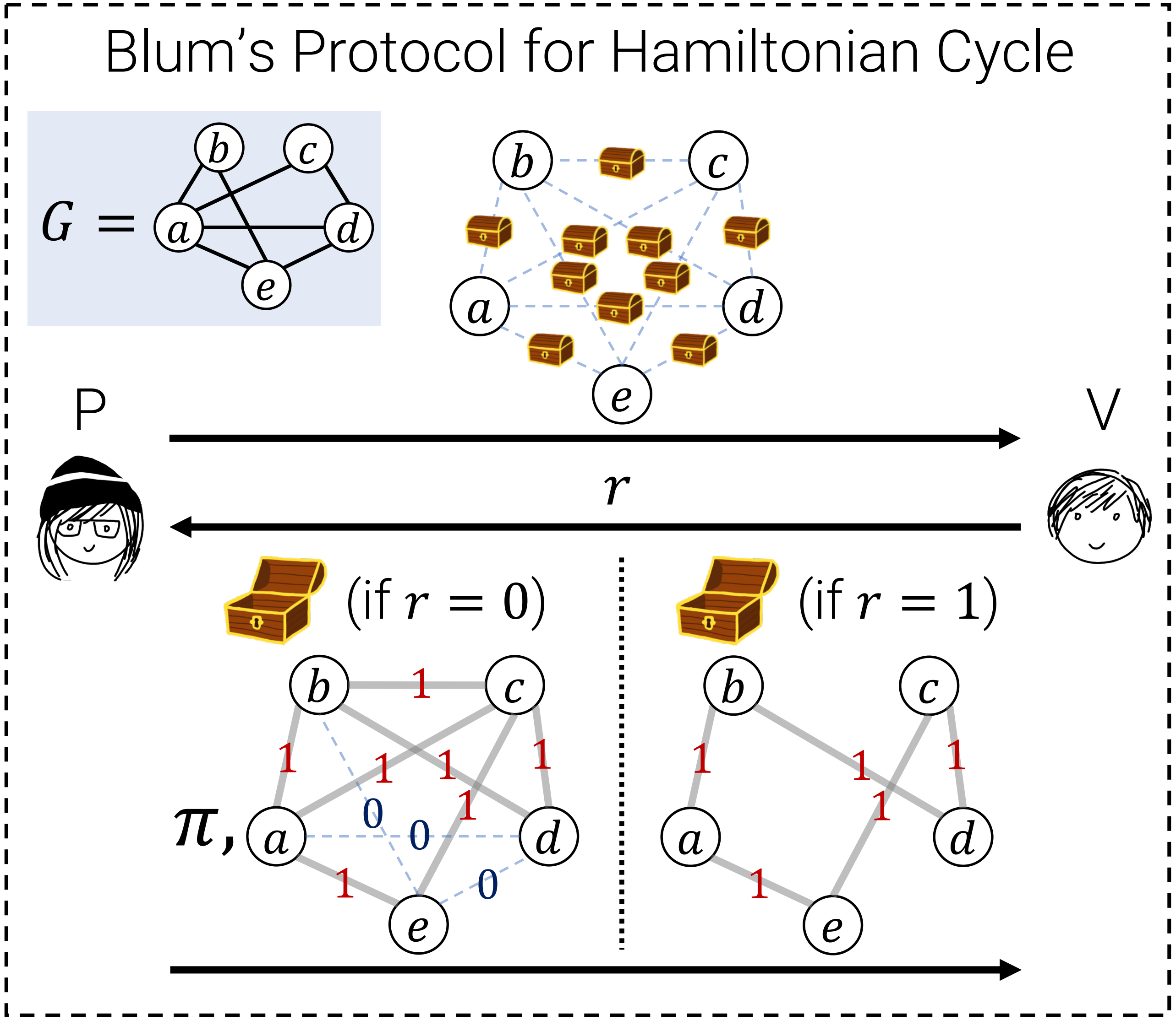
Rewinding argument: query P* once on $r = 0$ and once on $r = 1$



Probability at least $\Omega(\varepsilon)$ of two accepting responses.

Post-Quantum Soundness

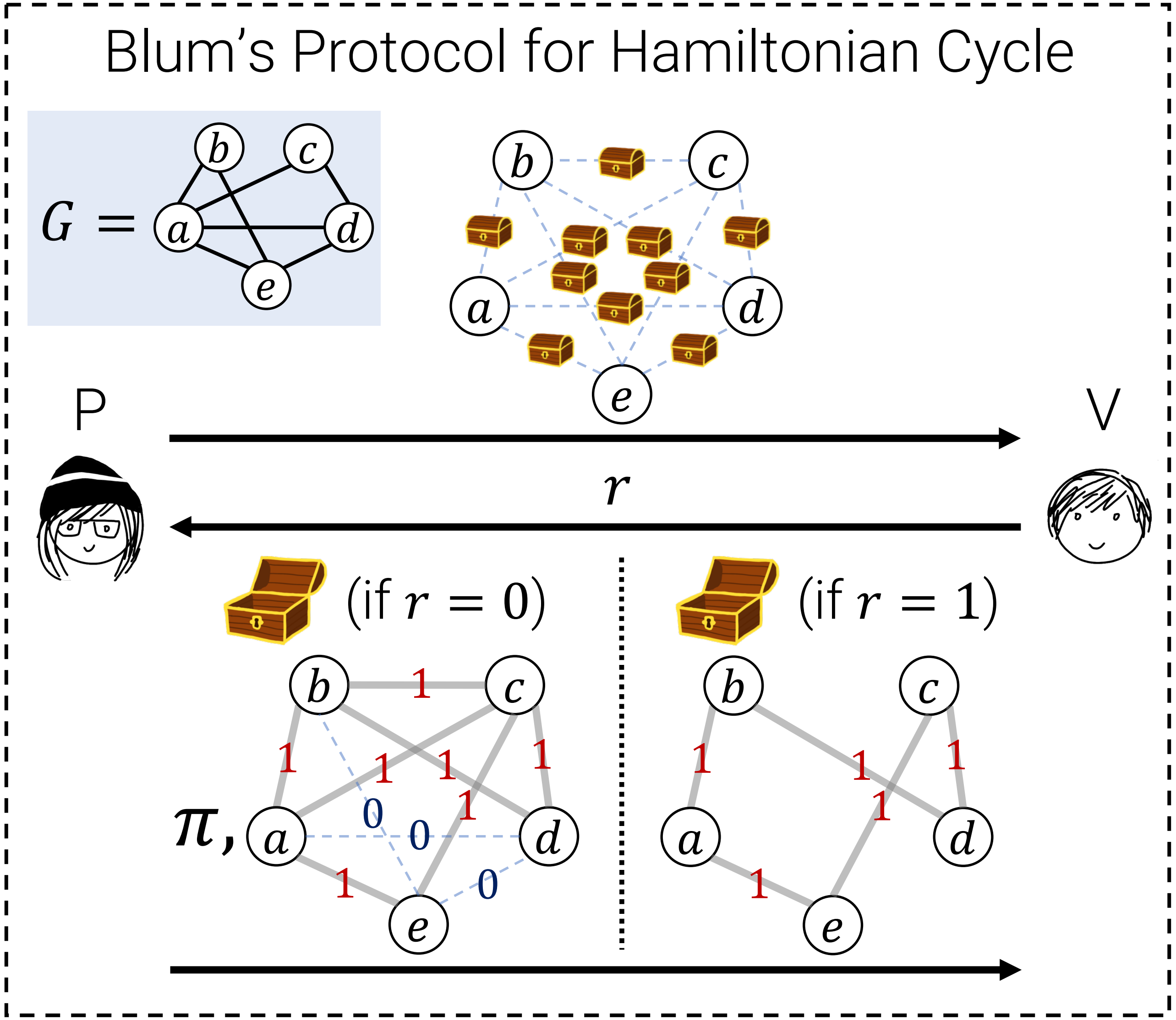




Post-Quantum Soundness

Easy case: statistically binding commitments

Soundness holds against unbounded attackers (and hence quantum)



Post-Quantum Soundness

Easy case: statistically binding commitments

Soundness holds against unbounded attackers (and hence quantum)

Interesting case: what if the commitments are only computationally binding?

Binding Against Quantum Attack

Before we can analyze soundness, we need to answer a basic question:

Binding Against Quantum Attack

Before we can analyze soundness, we need to answer a basic question:

What does it mean for a commitment to be *computationally binding*?

Binding Against Quantum Attack

Before we can analyze soundness, we need to answer a basic question:

What does it mean for a commitment to be *computationally binding*?

Commitment Syntax

sender

receiver

$$\xleftarrow{\quad ck \quad}$$

$$\xrightarrow{\quad c \,=\, \mathrm{Com}_{ck}(m;d) \quad}$$

$$\xrightarrow{\quad m,d \quad}$$

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

Binding Against Quantum Attack

Before we can analyze soundness, we need to answer a basic question:

What does it mean for a commitment to be *computationally binding*?

Commitment Syntax

sender  receiver 

$\xleftarrow{\;ck\;}$

$\xrightarrow{\;c \,=\, \mathrm{Com}_{ck}(m;d)\;}$

$\xrightarrow{\;m,d\;}$

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

Classical definition:

PPT adversary can't output c and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

Binding Against Quantum Attack

Before we can analyze soundness, we need to answer a basic question:

What does it mean for a commitment to be *computationally binding*?

Commitment Syntax

sender 

receiver 

$\xleftarrow{\quad ck \quad}$

$\xrightarrow{\; c = \mathrm{Com}_{ck}(m; d) \;}$

$\xrightarrow{\quad m, d \quad}$

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

Classical definition:

PPT adversary can't output c 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

Before we can analyze soundness, we need to answer a basic question:

What does it mean for a commitment to be *computationally binding*?

Commitment Syntax

sender

receiver

$\xleftarrow{ck}$

$\xrightarrow{c = \mathrm{Com}_{ck}(m; d)}$

$\xrightarrow{m, d}$

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

Classical definition:

PPT adversary can't output c 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 c 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 c and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

[ARU14]: Quantum attacker* might produce $c, |\psi\rangle$ such that:

- Can use $|\psi\rangle$ to open c to any m

malicious sender

$\xrightarrow{c}$

$\downarrow$

$|\psi\rangle$

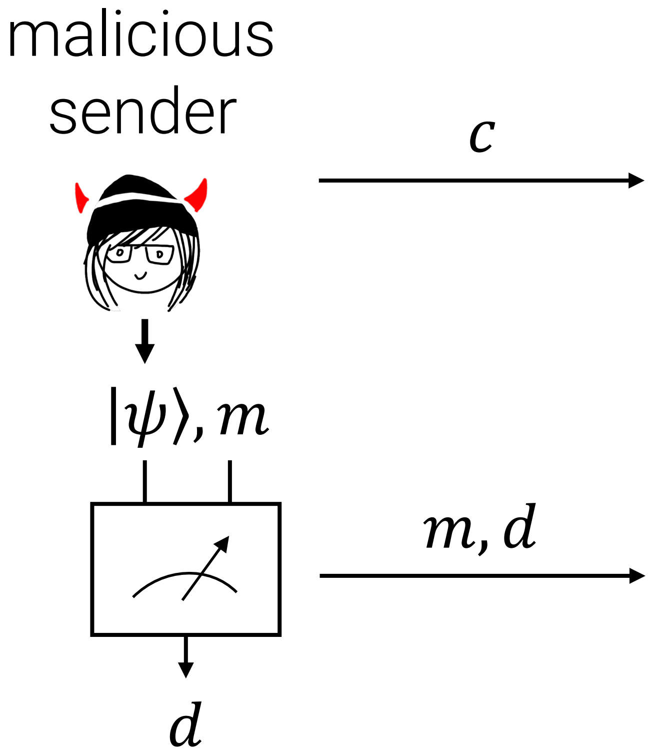
What's wrong with this definition?

Naïve post-quantum binding def:

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

[ARU14]: Quantum attacker* might produce $c, |\psi\rangle$ such that:

- Can use $|\psi\rangle$ to open c to any m

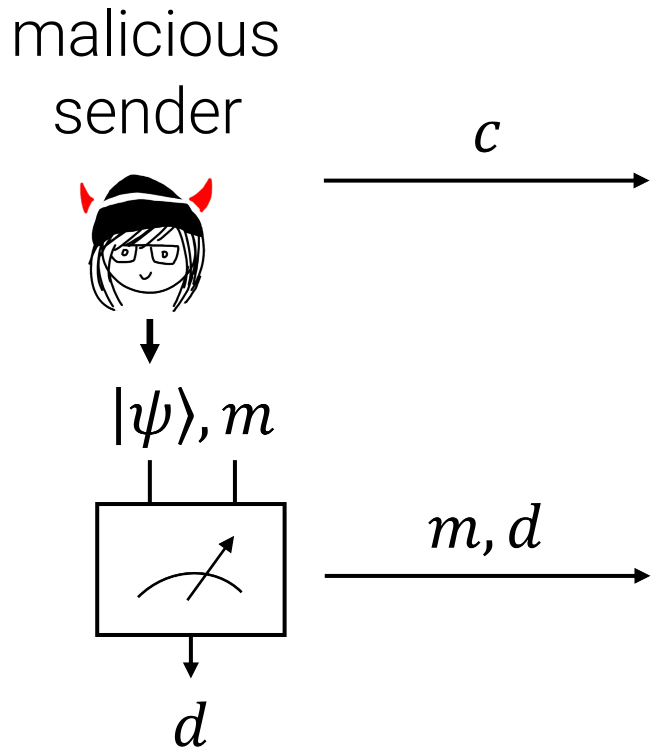


What's wrong with this definition?

Naïve post-quantum binding def:
QPT attacker can't output c and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

[ARU14]: Quantum attacker* might produce $c, |\psi\rangle$ such that:

- Can use $|\psi\rangle$ to open c to any m
- But can only do this once!

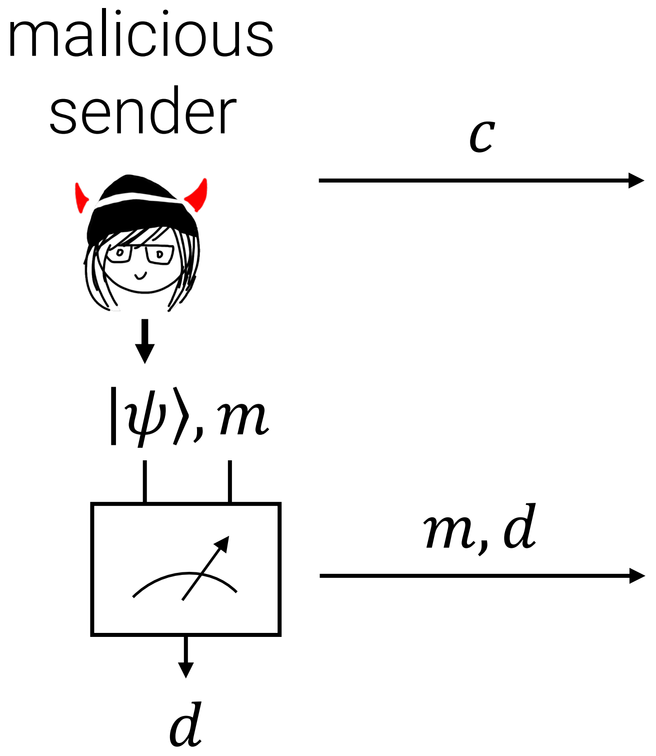


What's wrong with this definition?

Naïve post-quantum binding def:
QPT attacker can't output c and valid $(m_0, d_0), (m_1, d_1)$ for $m_0 \neq m_1$.

[ARU14]: Quantum attacker* might produce $c, |\psi\rangle$ such that:

- Can use $|\psi\rangle$ to open c to any m
- But can only do this once!



*Caveat: assuming a quantum oracle

**Open: construct example without oracles

A Better Definition: Collapse-Binding

Suppose commitment is *perfectly* binding.

A Better Definition: Collapse-Binding

Suppose commitment is *perfectly* binding.

malicious sender

$$\xrightarrow{c, \sum |m\rangle_M |d\rangle_D}$$

A Better Definition: Collapse-Binding

Suppose commitment is *perfectly* binding.

malicious
sender

$c, \sum |m\rangle_M |d\rangle_D$

- Run the verifier in superposition on M, D and measure its output (accept or reject)

A Better Definition: Collapse-Binding

Suppose commitment is *perfectly* binding.

malicious sender

$c, \sum |m\rangle_M |d\rangle_D$

- Run the verifier in superposition on M, D and measure its output (accept or reject)

Observation: If verification accepts, measuring M cannot disturb the state.

A Better Definition: Collapse-Binding

Suppose commitment is *perfectly* binding.

malicious sender

$$c, \sum |m\rangle_M |d\rangle_D \longrightarrow$$

- Run the verifier in superposition on M, D and measure its output (accept or reject)

Observation: If verification accepts, measuring M cannot disturb the state.

Collapse-binding definition [Unruh16]

Commitment is computationally binding if, given M, D, no efficient adversary can tell whether or not M is measured.

Why this definition?

- Rules out [ARU14]-style attacks where committer can open an arbitrary message
- Compatible with rewinding
- Composable

Collapse-binding definition [Unruh16]

Commitment is computationally binding if, given M, D, no efficient adversary can tell whether or not M is measured.

Why this definition?

- Rules out [ARU14]-style attacks where committer can open an arbitrary message
- Compatible with rewinding
- Composable

Do collapse-binding commitments exist? Yes, assuming LWE.

Collapse-binding definition [Unruh16]

Commitment is computationally binding if, given M, D, no efficient adversary can tell whether or not M is measured.

Why this definition?

- Rules out [ARU14]-style attacks where committer can open an arbitrary message
- Compatible with rewinding
- Composable

Do collapse-binding commitments exist? Yes, assuming LWE.

This will be the notion of binding used throughout today

Collapse-binding definition [Unruh16]

Commitment is computationally binding if, given M, D, no efficient adversary can tell whether or not M is measured.

What does collapse-binding have to do with soundness?

Lazy measurement of prover responses

$|\psi\rangle$ 

$\xrightarrow{c}$

$\xleftarrow{r}$

$\xrightarrow{z}$

z = measurement outcome of $U_r|\psi\rangle|0\rangle_{\mathbf{Out}}$

Lazy measurement of prover responses

$|\psi\rangle$ 

$\xrightarrow{c}$

$\xleftarrow{r}$

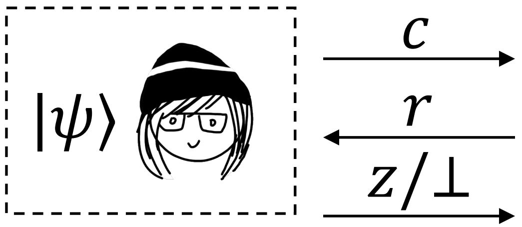
$\xrightarrow{z}$

z = measurement outcome of $U_r|\psi\rangle|0\rangle_{\mathrm{Out}}$

Let $\Pi_r = U_r^{\dagger}\,\Pi_{\mathrm{Valid}} U_r$.

"check if the prover would answer correctly"

Lazy measurement of prover responses



Lazy

z = measurement outcome of $U_r|\psi\rangle|0\rangle_{\mathbf{Out}}$

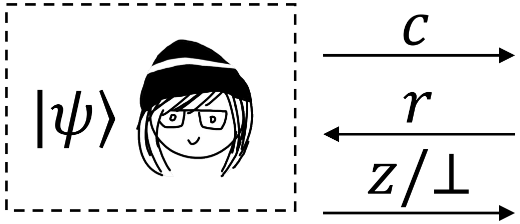
Let $\Pi_r = U_r^\dagger \, \Pi_{\mathbf{Valid}} U_r$.

"check if the prover would answer correctly"

Rule: before measuring z, first measure $(\Pi_r, \mathbf{Id} - \Pi_r)$ and only measure $\boldsymbol{z}$ if outcome is 1 (Π_r)!

Collapsing says: z measurement* is undetectable!

Lazy measurement of prover responses



Lazy

z = measurement outcome of $U_r|\psi\rangle|0\rangle_{\mathrm{Out}}$

Let $\Pi_r = U_r^\dagger\, \Pi_{\mathrm{Valid}} U_r$.

"check if the prover would answer correctly"

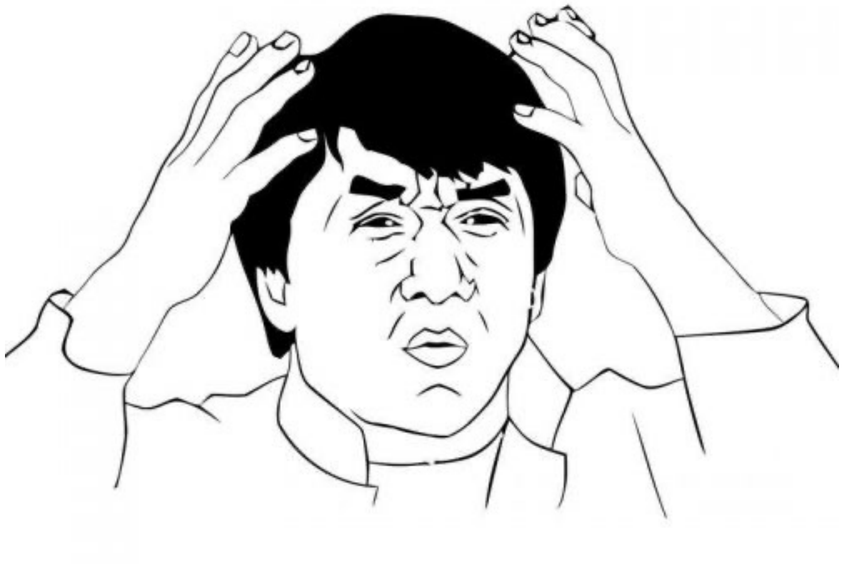
Rule: before measuring z, first measure $(\Pi_r, \mathrm{Id} - \Pi_r)$ and **only measure z** if outcome is 1 (Π_r)!

Collapsing says: z measurement* is undetectable!

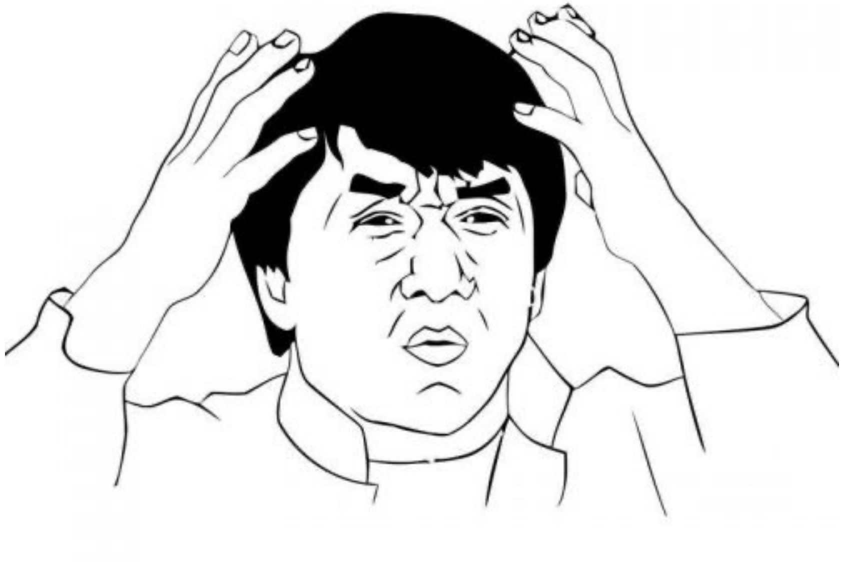
Thus, we can forget about measuring z and pretend we only measure $(\Pi_r, I - \Pi_r)$

Claim [Unruh]: If efficient *quantum* P* convinces V with prob $\frac{1}{\sqrt{2}} + \varepsilon$, then G must have a Ham cycle.

Claim [Unruh]: If efficient *quantum* P* convinces V with prob $\frac{1}{\sqrt{2}} + \varepsilon$, then G must have a Ham cycle.



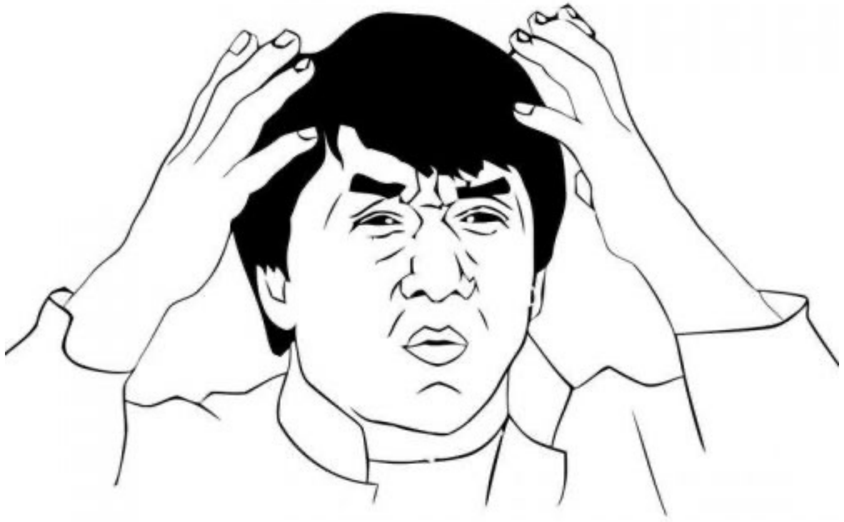
Claim [Unruh]: If efficient *quantum* P* convinces V with prob $\frac{1}{\sqrt{2}} + \varepsilon$, then G must have a Ham cycle.*



*Requires a slight modification to the protocol adding some extra commitments

Claim [Unruh]: If efficient *quantum* P* convinces V with prob $\cancel{\frac{1}{\sqrt{2}} + \varepsilon}$, then G must have a Ham cycle.*

Today: $\frac{9}{10}$



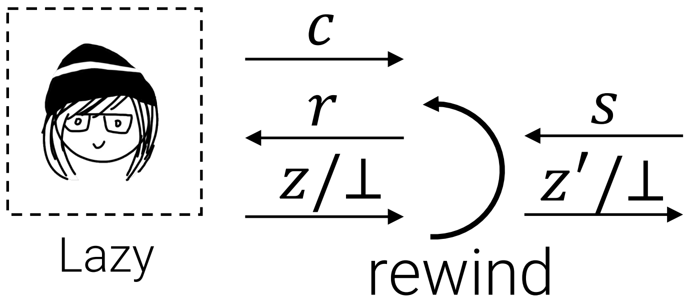
*Requires a slight modification to the protocol adding some extra commitments

Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$

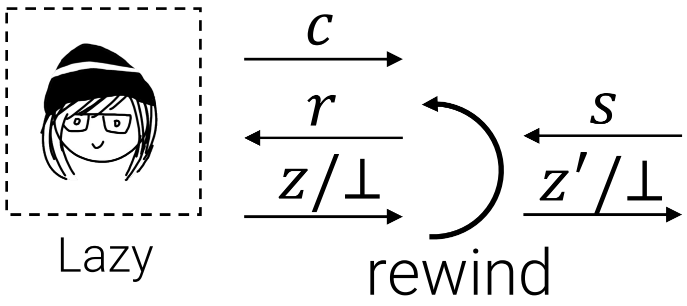
Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$



Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$

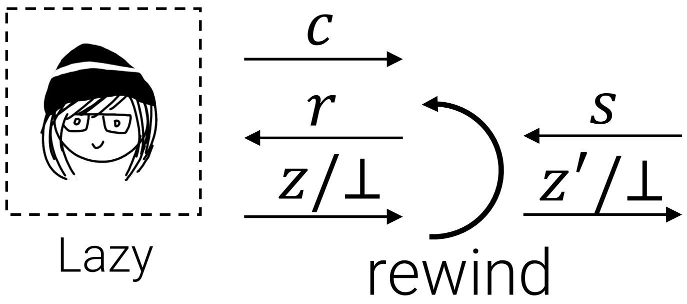


Let $\Pi_r = U_r^\dagger \Pi_{\text{Valid}} U_r$.

"check if the prover would answer correctly"

Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$



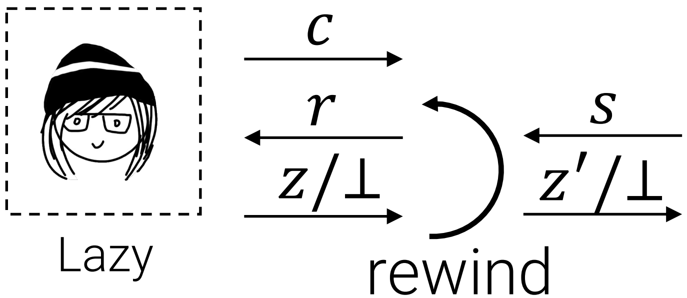
Let $\Pi_r = U_r^\dagger \, \Pi_{\text{Valid}} U_r$.

"check if the prover would answer correctly"

Info-theoretic Claim: $\mathop{\mathbb{E}}_{r,s} \|\Pi_s \Pi_r |\psi\rangle\|^2 \geq 1 - 2\sqrt{\delta} - 2\delta$

Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$



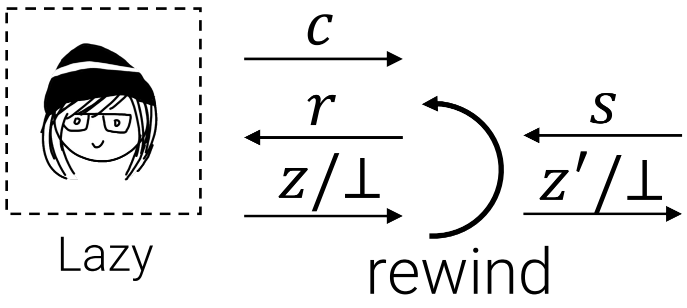
Let $\Pi_r = U_r^\dagger \, \Pi_{\text{Valid}} U_r$.   "check if the prover would answer correctly"

Info-theoretic Claim: $\underset{r,s}{\mathbb{E}} \; \| \Pi_s \Pi_r |\psi\rangle \|^2 \; \geq \; 1 - 2\sqrt{\delta} - 2\delta$

Proof: Gentle Measurement Lemma

Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$

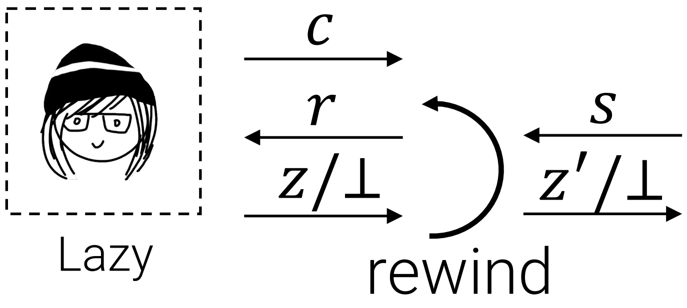


Obtain witness with decent probability by invoking:

1. (**Collapsing**) just need to analyze binary outcome measurements.
2. (**Gentle measurement**) random Π_r, Π_s both accept with good probability.
3. (**Special soundness**) two transcripts reconstruct witness.

Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$



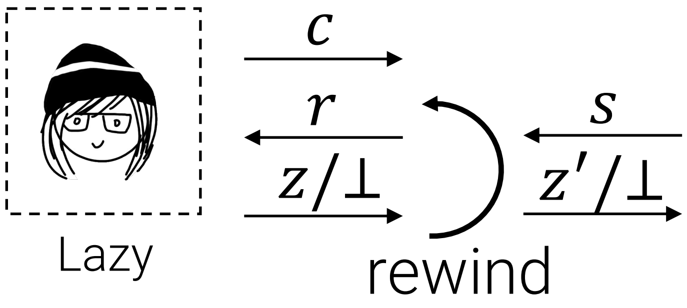
Let $\Pi_r = U_r^\dagger \Pi_{\text{Valid}} U_r$.

"check if the prover would answer correctly"

Stronger Info-theoretic Claim [Unruh]: $\mathbb{E}_{r,s} \|\Pi_s \Pi_r |\psi\rangle\|^2 \geq p^3$

Claim [Today]: If efficient *quantum* P* convinces V with prob $\frac{9}{10}$, then G must have a Ham cycle.*

Suppose P* convinces V with prob $p = 1 - \delta$



Let $\Pi_r = U_r^\dagger \, \Pi_{\text{Valid}} U_r$.   "check if the prover would answer correctly"

Stronger Info-theoretic Claim [Unruh]: $\mathop{\mathbb{E}}_{r,s} \; \|\Pi_s \Pi_r |\psi\rangle\|^2 \; \geq p^3$

Open: is there a simple proof that Blum has soundness error ½?

This Talk

1) Blum’s protocol for graph Hamiltonicity ✓

2) Post-Quantum Soundness of Blum ✓

3) Post-Quantum Zero Knowledge of Blum

This Talk

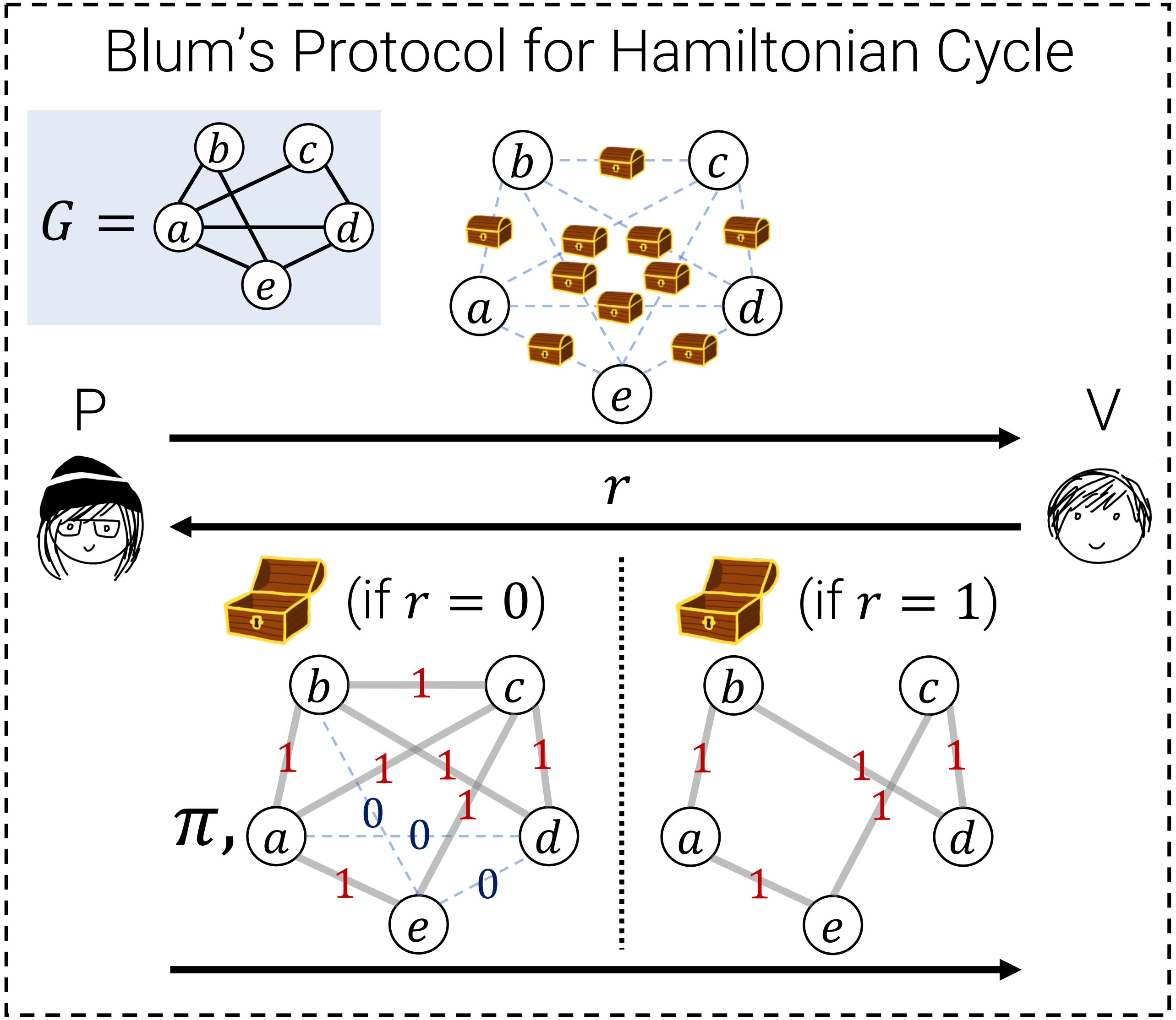
1) Blum's protocol for graph Hamiltonicity ✓

2) Post-Quantum Soundness of Blum ✓

3) Post-Quantum Zero Knowledge of Blum

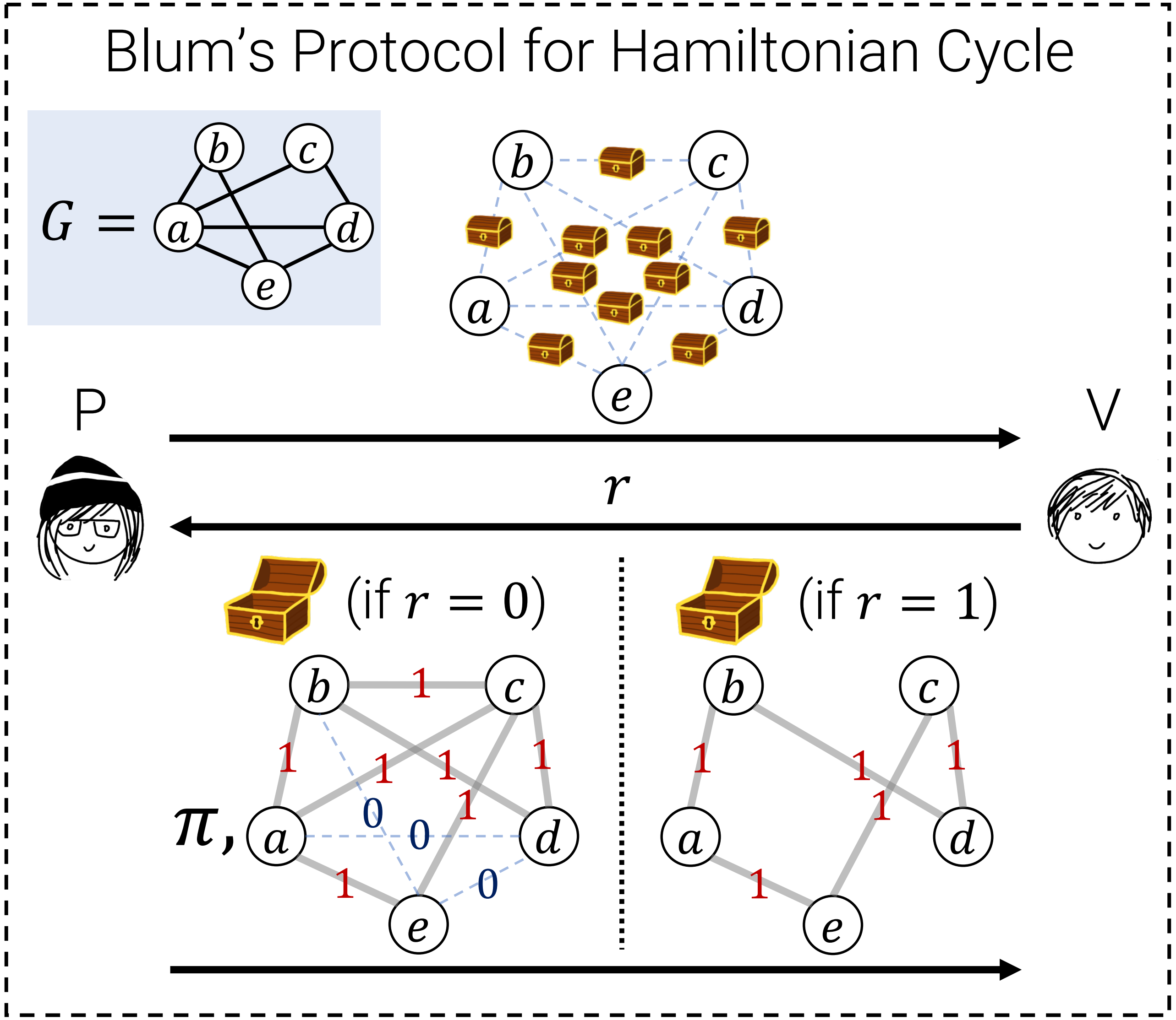
- Classical zero knowledge
- Watrous rewinding with alternating measurements
- Analysis: Jordan's lemma

Classical Zero Knowledge



Key Property: can simulate honest verifier that sends random bit

Classical Zero Knowledge

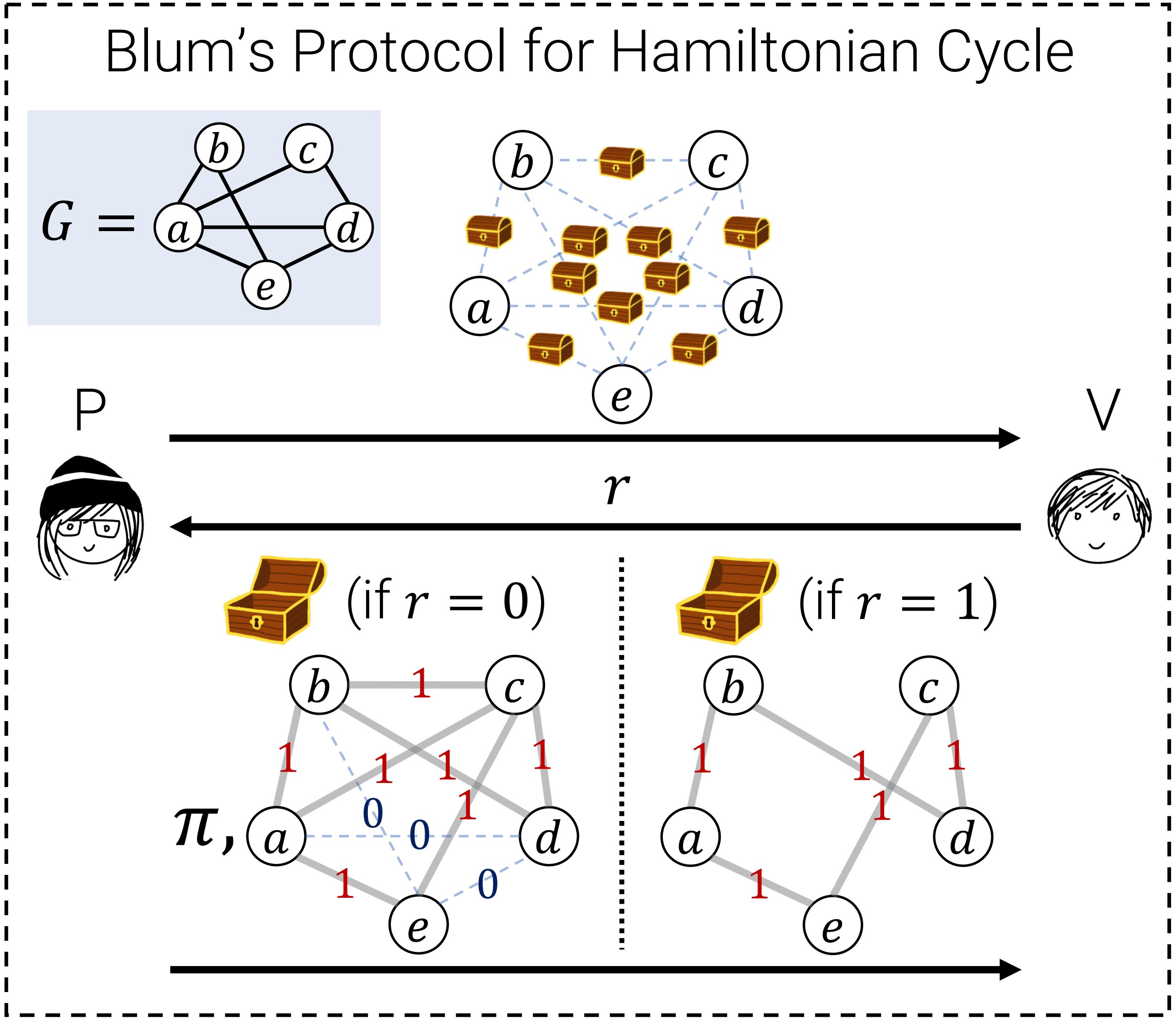


Key Property: can simulate honest verifier that sends random bit

HVSim:

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

Classical Zero Knowledge



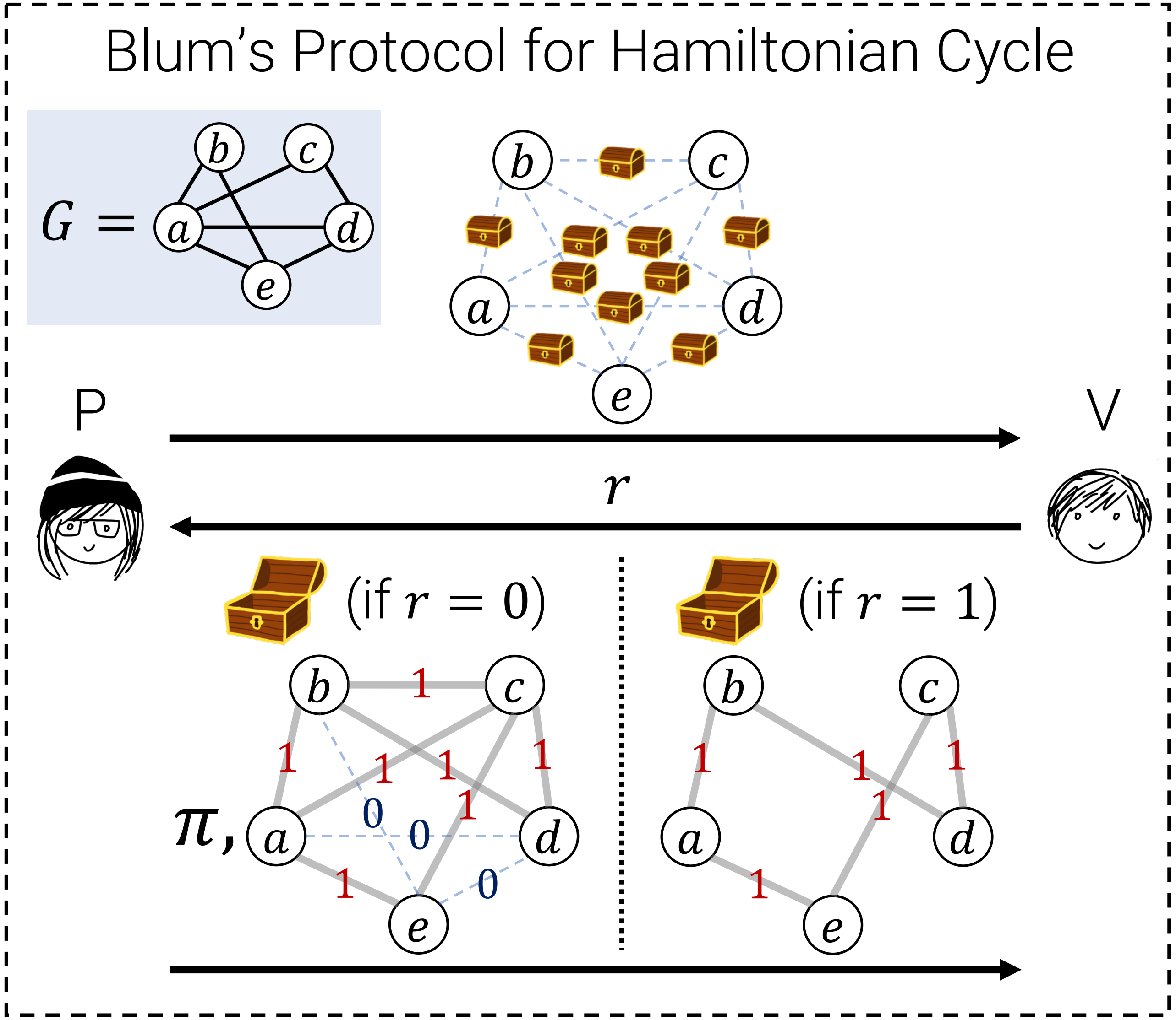
Key Property: can simulate honest verifier that sends random bit

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

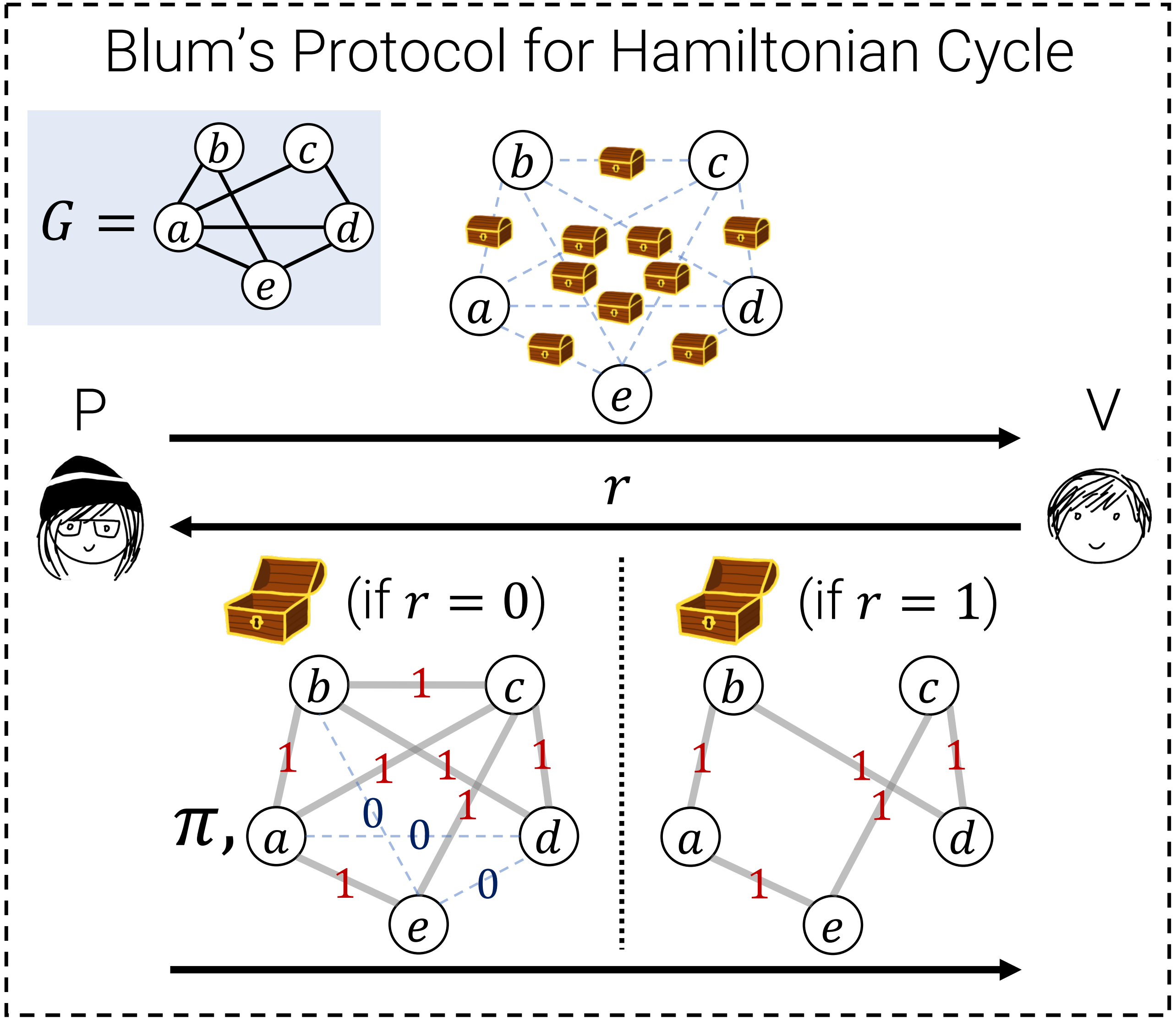
HVSim:

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

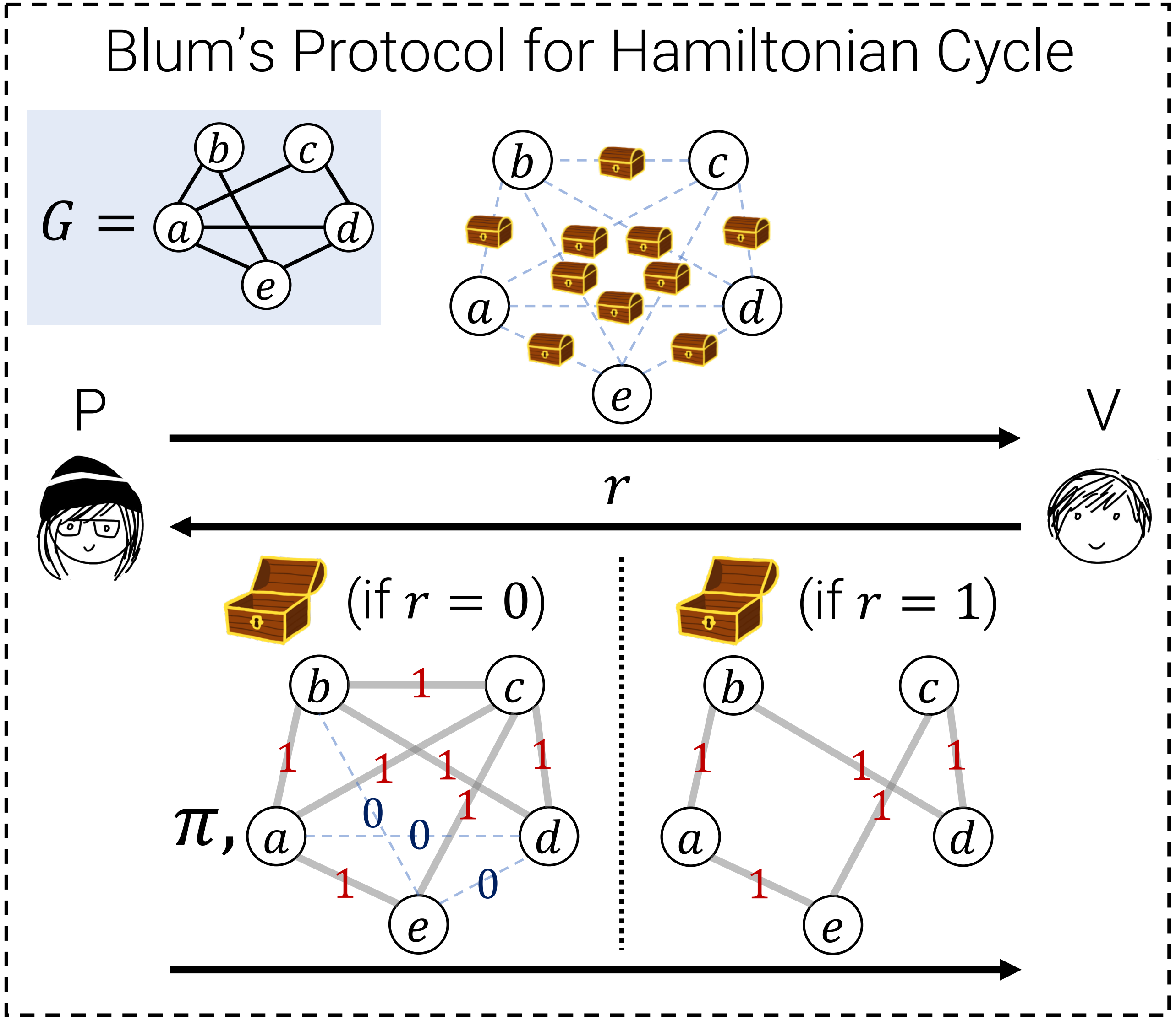
HVSim:

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, $(c, r', z) \leftarrow \mathrm{HVSim}$ 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

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

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.

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

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

V^*

Classical Zero Knowledge

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.

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

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

$\xrightarrow{c}$

$\xleftarrow{r}$

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.

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

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

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

$\xrightarrow{c}$

$\xleftarrow{r}$

$\xrightarrow{z}$

(if $r = r'$)

V^*

Classical Zero Knowledge

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.

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

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

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

$\xrightarrow{c}$

$\xleftarrow{r}$

$\xrightarrow{z}$

(if $r = r'$)

V^*

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

Classical Zero Knowledge

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.

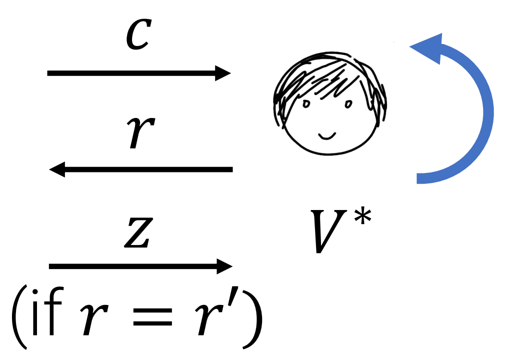
This leads to the complete ZK simulator:

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

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

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

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



If $r \neq r'$ rewind and try again

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 $\mathrm{Guess}(V^*, |\psi\rangle)$ may irreversibly disturb it.

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

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

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

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

c →

r ←

z → (if $r = r'$)

V^*

If $r \neq r'$ rewind and try again

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 $\mathsf{Guess}(V^*, |\psi\rangle)$ may irreversibly disturb it.

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

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

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

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

$\xrightarrow{c}$

$\xleftarrow{r}$

$\xrightarrow{z}$ (if $r = r'$)

V^*

~~If $r \neq r'$ rewind and try again~~

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 $\perp$.

$\xrightarrow{c}$

$\xleftarrow{r}$

$\xrightarrow{z}$ (if $r = r'$)

V^*

~~If $r \neq r'$ rewind and try again~~

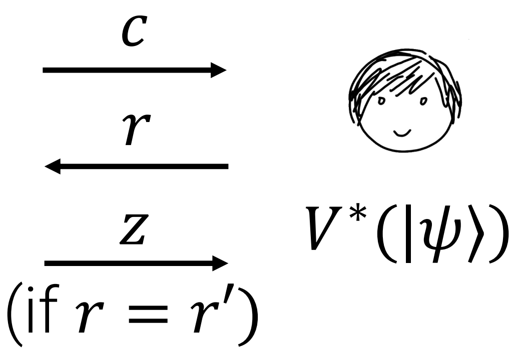
Since c is hiding, $\Pr[r = r'] \approx 1/2$

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

Post-Quantum ZK of Blum [Watrous05]

$\mathsf{Guess}(V^*, |\psi\rangle)$:

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

$\mathsf{Guess}(V^*, |\psi\rangle)$:

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

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

$\xrightarrow{c}$

$\xleftarrow{r}$

$\xrightarrow{z}$

(if $r = r'$)

$V^*(|\psi\rangle)$

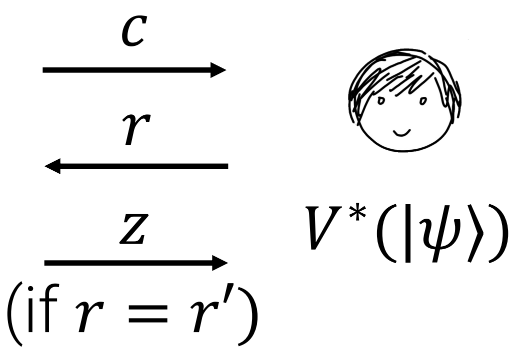
If commitments are hiding, can still simulate with probability $1/2$.

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

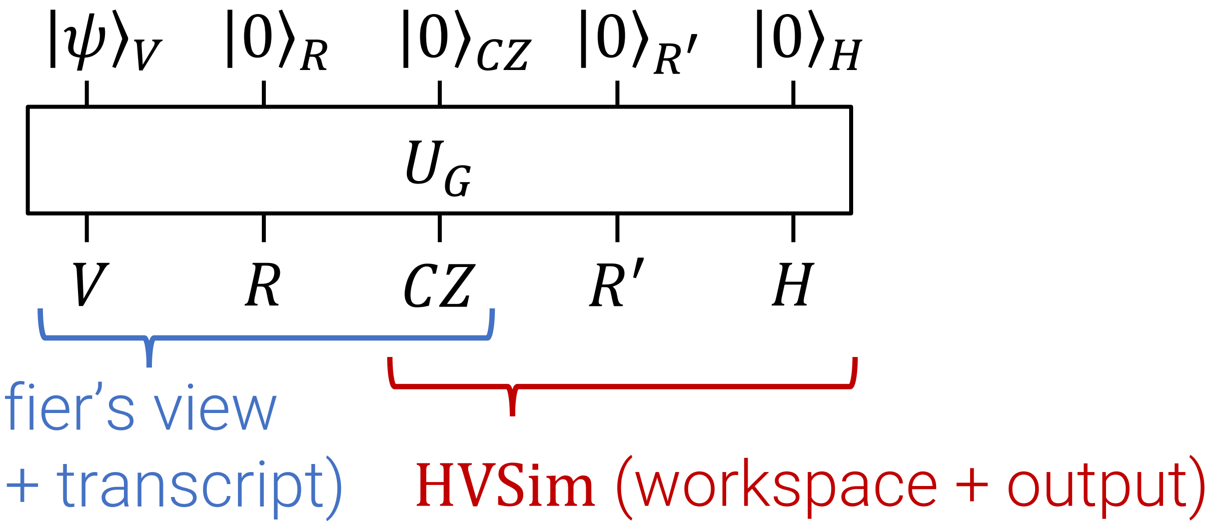
Post-Quantum ZK of Blum [Watrous05]

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

1) Sample $(c, r', z) \leftarrow \mathbf{HVSim}$
2) If $r = r'$, output (c, r, z). Otherwise $\perp$.



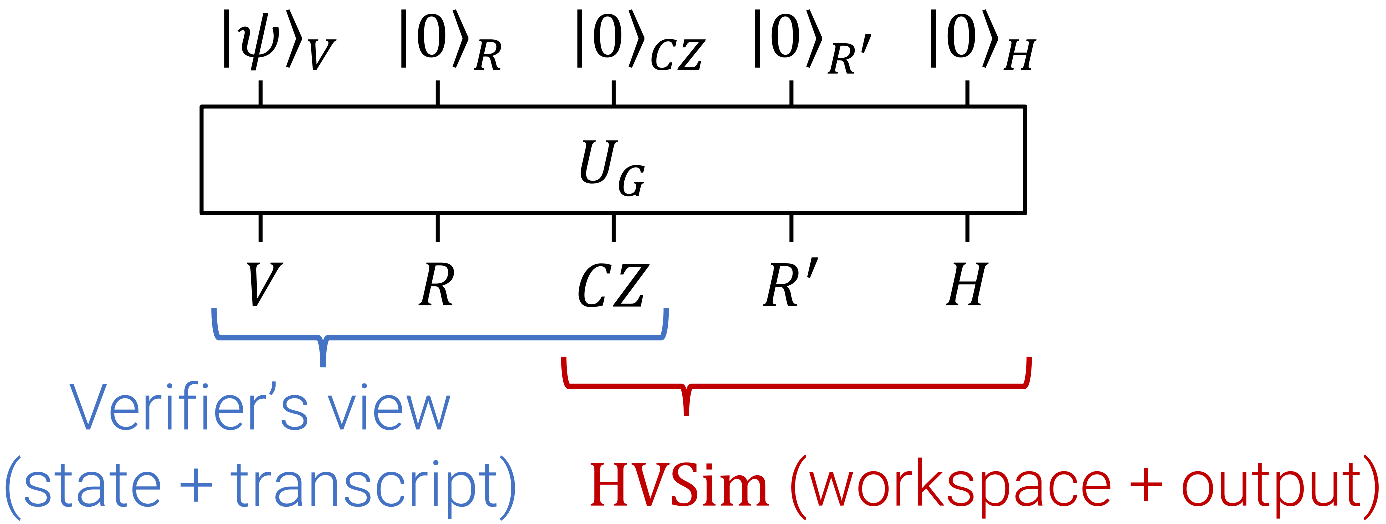
C, R, Z, R' correspond to c, r, z, r'



- 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'

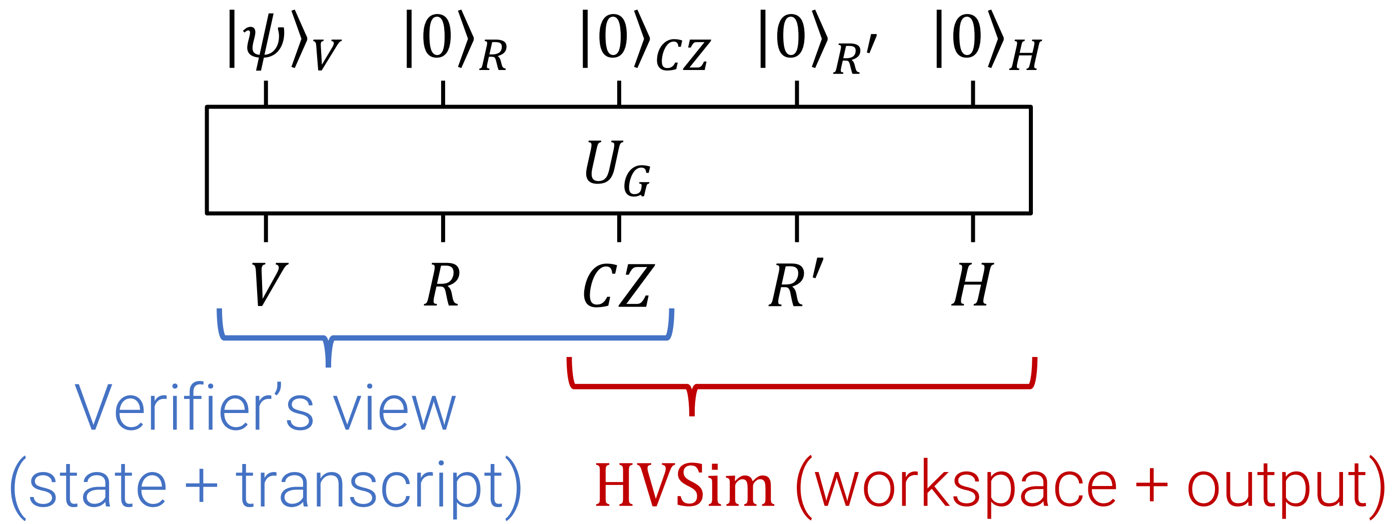


- Computing $U_G|\psi\rangle|0\rangle$ and checking if $R = R'$ is the same as running $\mathbf{Guess}(V^*, |\psi\rangle)$.

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'



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

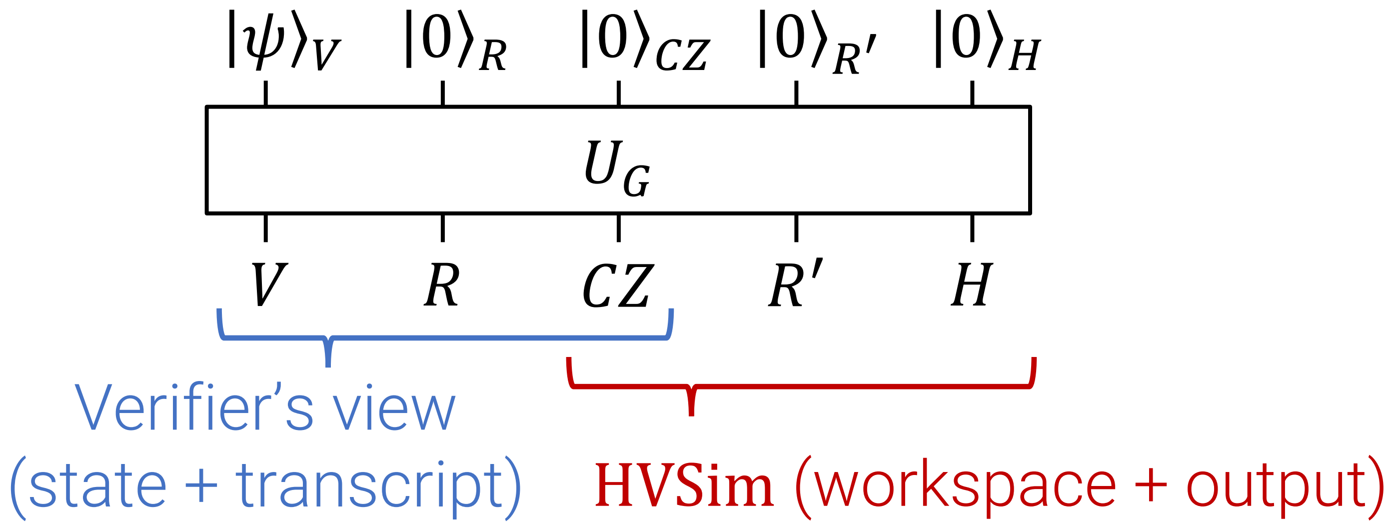
Post-Quantum ZK of Blum [Watrous05]

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.
- 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]

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

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

The Post-Quantum ZK Simulator [MW05, W05]

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

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]

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

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 $M_G \to 1$.

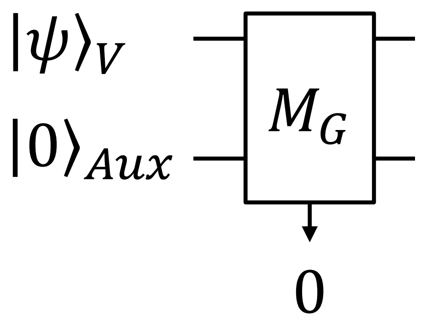
$|\psi\rangle_V$ –

$|0\rangle_{Aux}$ –

The Post-Quantum ZK Simulator [MW05, W05]

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

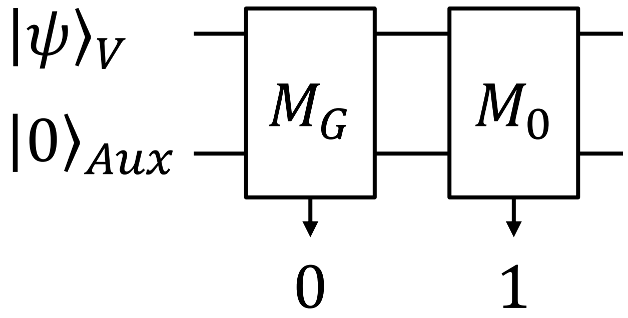
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



The Post-Quantum ZK Simulator [MW05, W05]

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

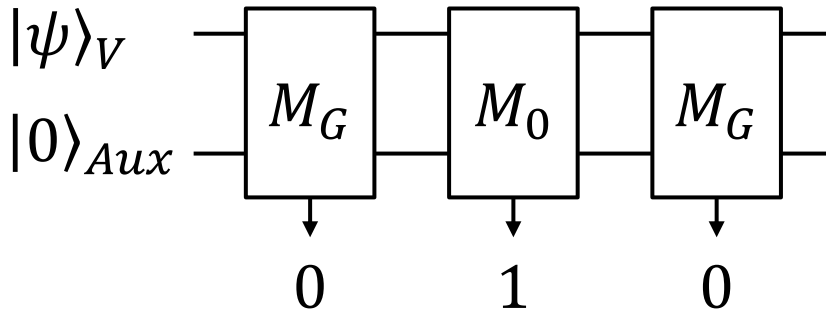
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



The Post-Quantum ZK Simulator [MW05, W05]

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

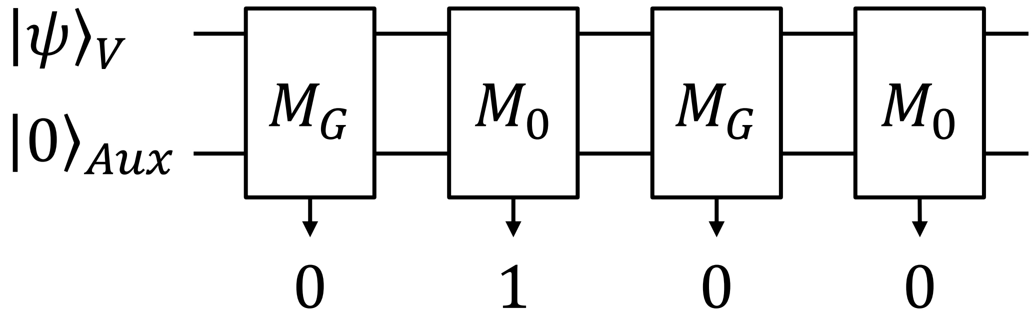
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



The Post-Quantum ZK Simulator [MW05, W05]

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

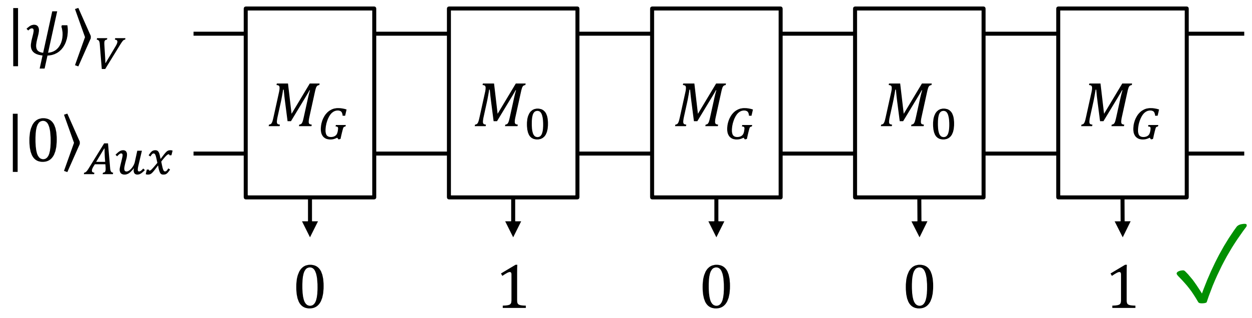
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



The Post-Quantum ZK Simulator [MW05, W05]

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

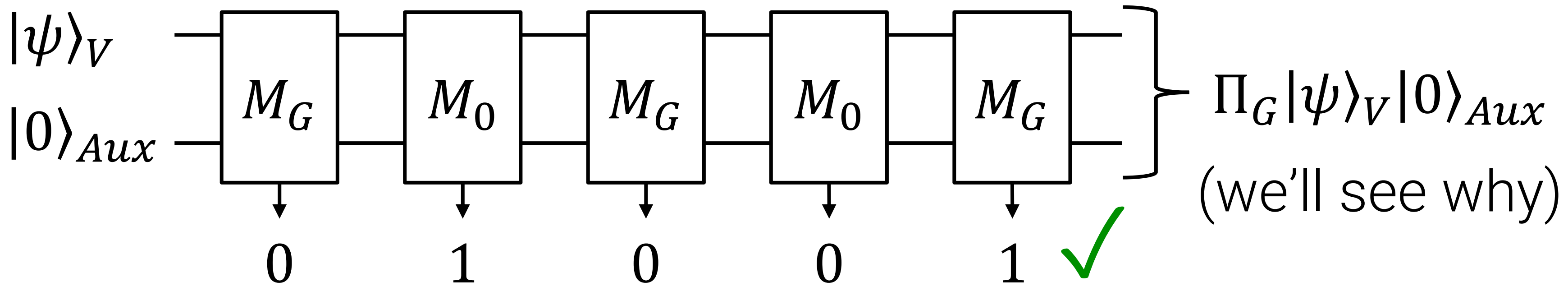
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



The Post-Quantum ZK Simulator [MW05, W05]

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

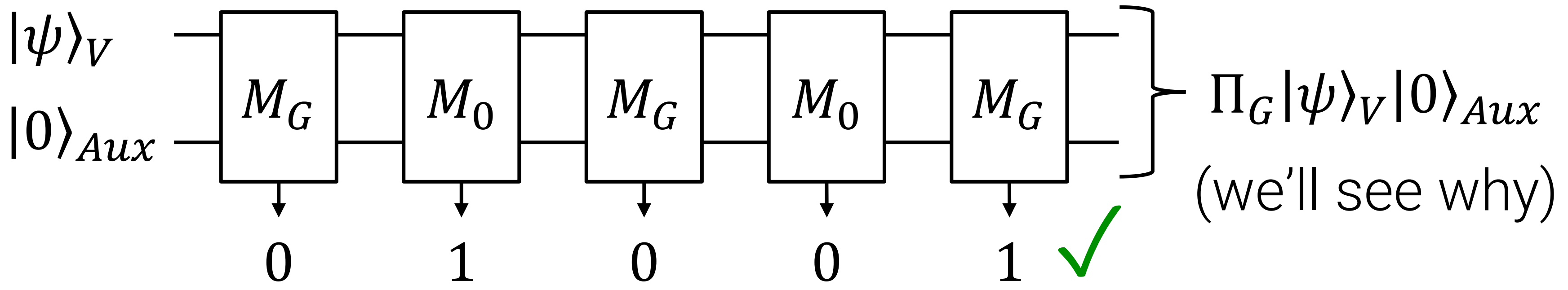
1) Initialize $|\psi\rangle_V|0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.



The Post-Quantum ZK Simulator [MW05, W05]

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

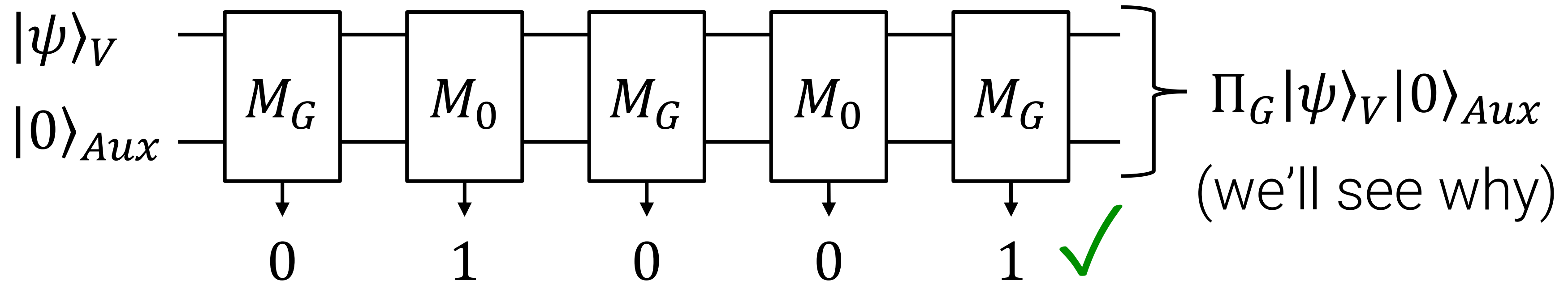
1) Initialize $|\psi\rangle_V |0\rangle_{Aux}$. Let $\Pi_0 = |0\rangle\langle 0|_{Aux}$.
2) Alternate $M_G = (\Pi_G, \mathbb{I} - \Pi_G)$ and $M_0 = (\Pi_0, \mathbb{I} - \Pi_0)$ until $M_G \to 1$.
3) Generate verifier's view (apply U_G).



The Post-Quantum ZK Simulator [MW05, W05]

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

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).

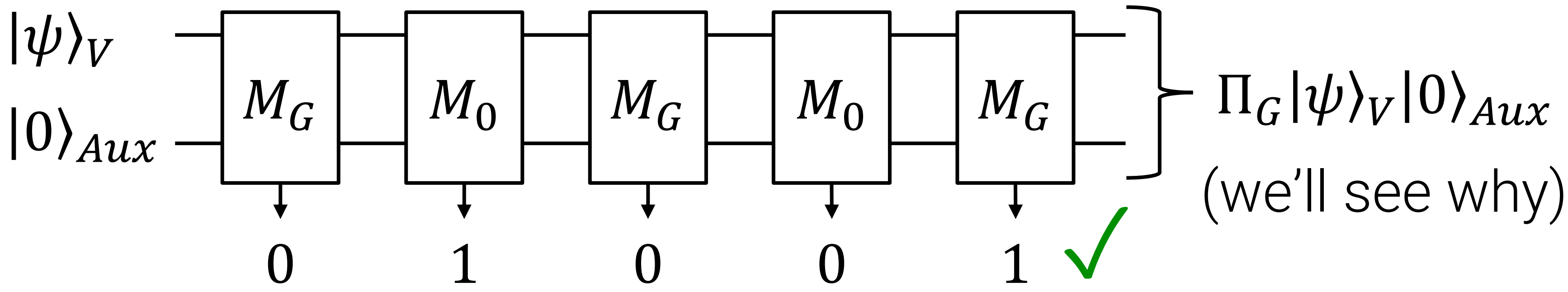


But why does this simulator work? Need to resolve:

The Post-Quantum ZK Simulator [MW05, W05]

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

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).



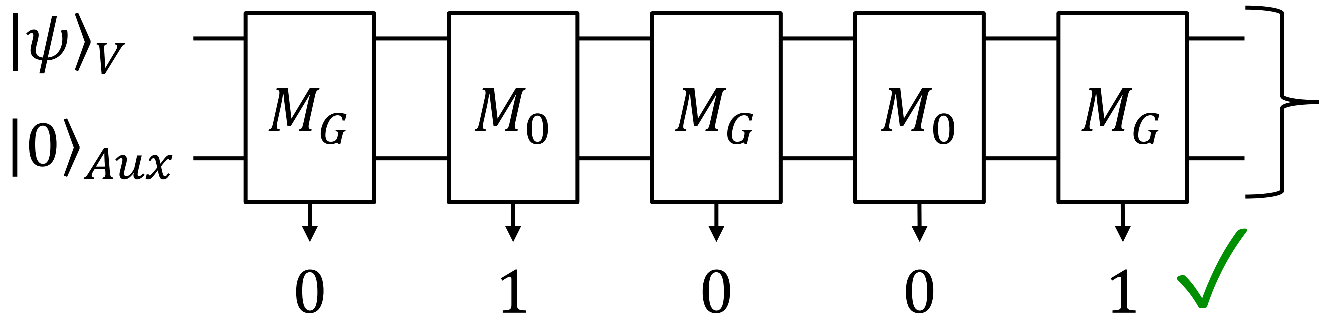
But why does this simulator work? Need to resolve:

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

The Post-Quantum ZK Simulator [MW05, W05]

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

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).



$\Pi_G |\psi\rangle_V |0\rangle_{Aux}$

(we'll see why)

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 $\Pi_G |\psi\rangle_V |0\rangle_{Aux}$?

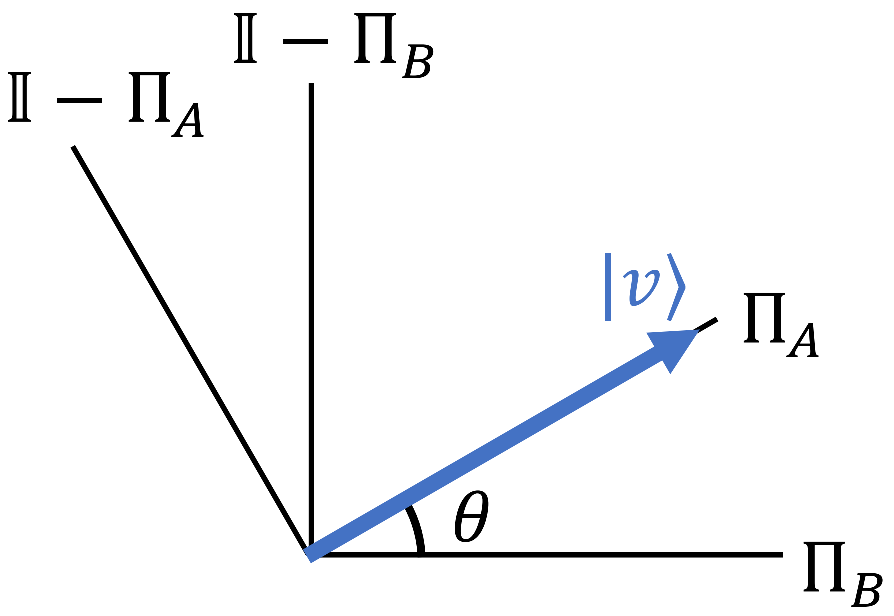
Understanding Alternating Measurements [MW05]

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 $(\Pi_B, \mathbb{I} - \Pi_B)$?

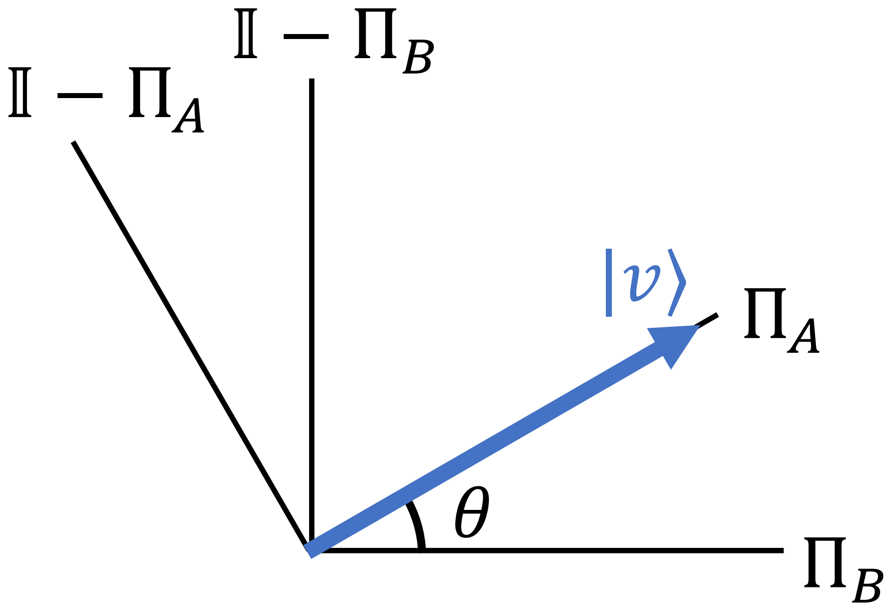
Easy case: Π_A, Π_B live in 2D



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: Π_A, Π_B live in 2D

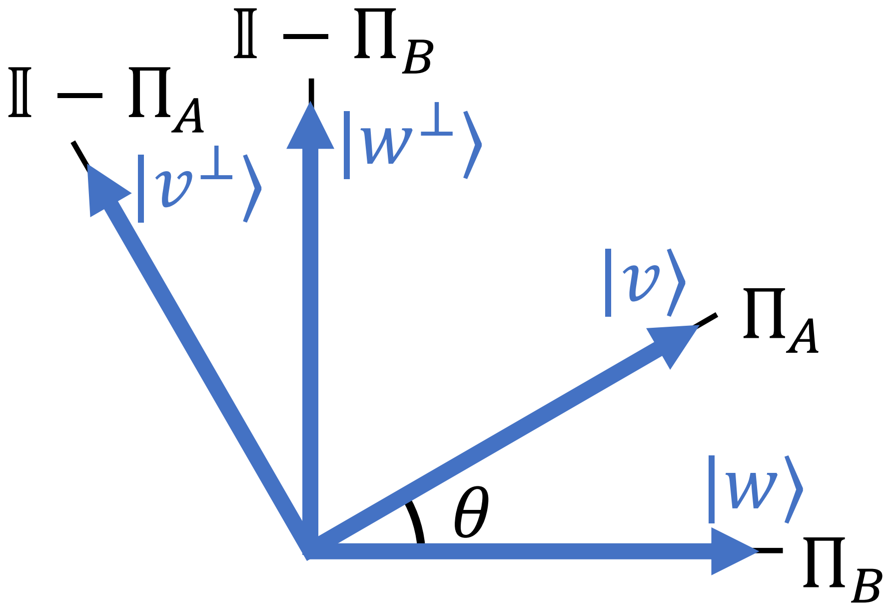


When we alternate measurements, we jump between four states

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: Π_A, Π_B live in 2D

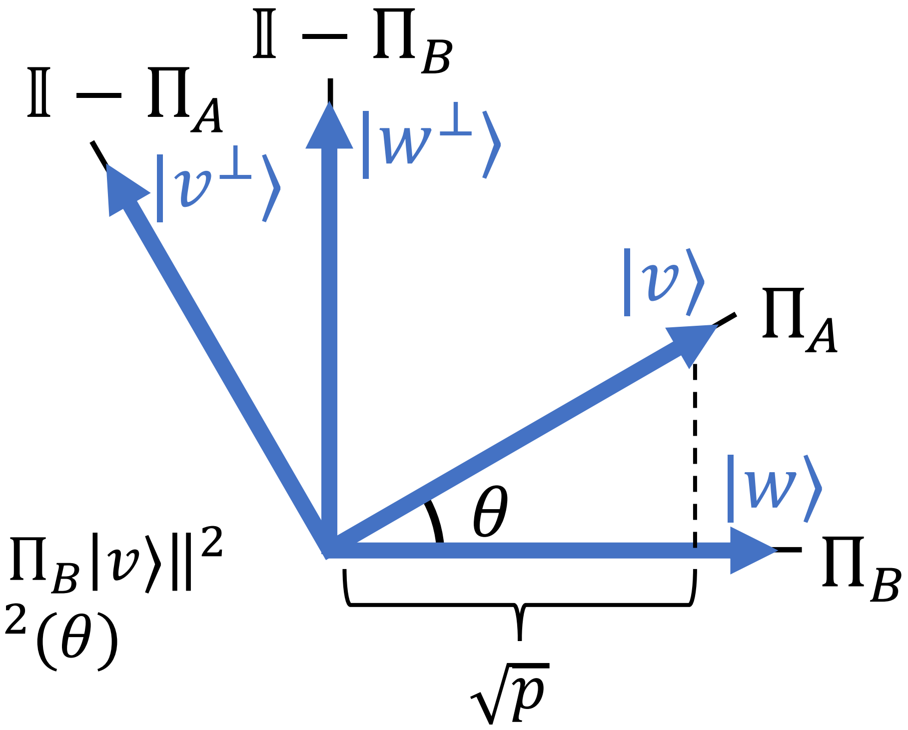


When we alternate measurements, we jump between four states

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: Π_A, Π_B live in 2D



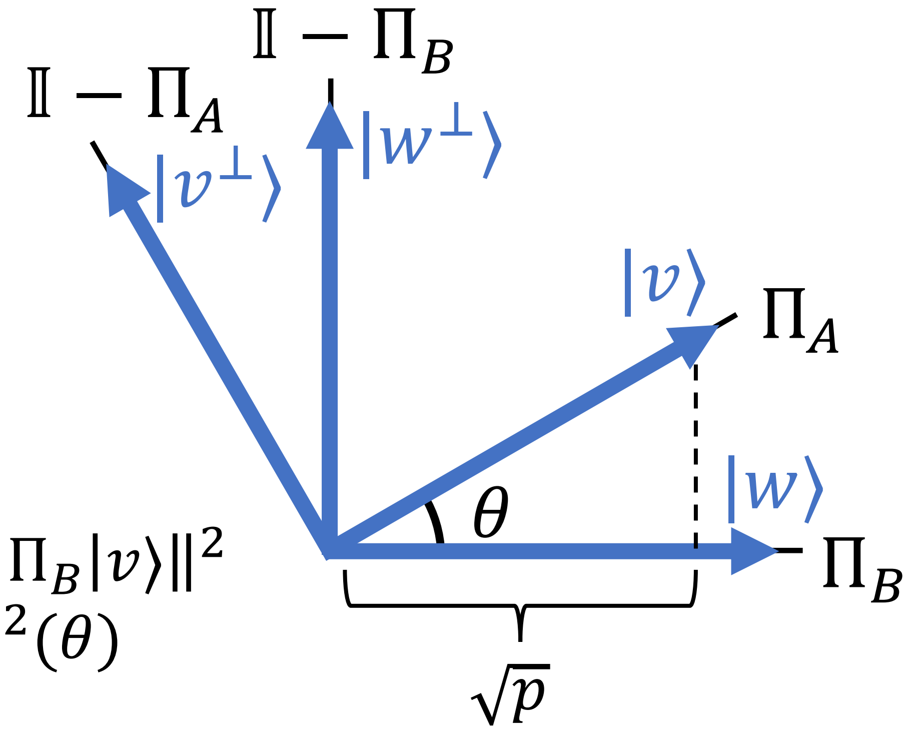
$p \coloneqq \|\Pi_B|v\rangle\|^2$
$= cos^2(\theta)$

When we alternate measurements, we jump between four states

Understanding Alternating Measurements [MW05]

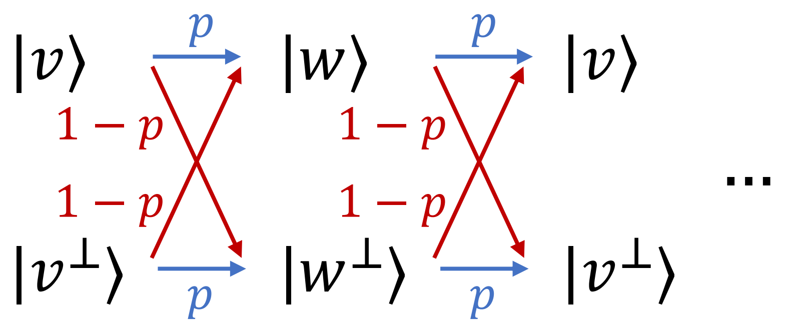
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

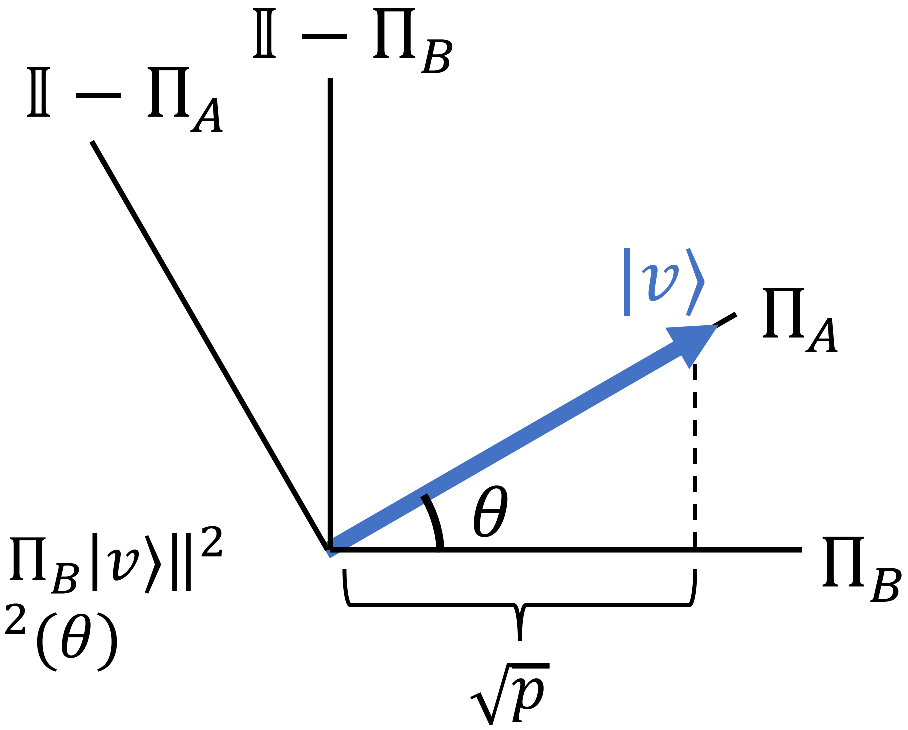
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

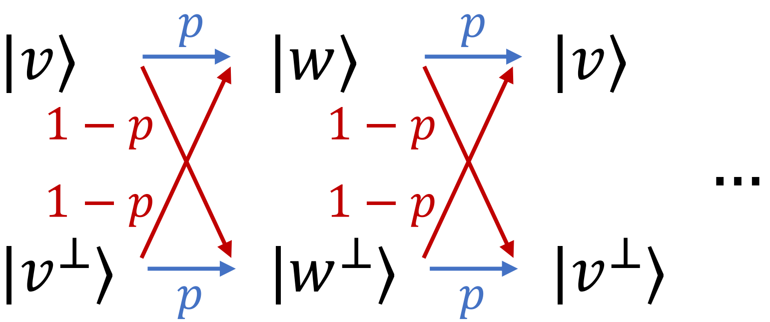
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

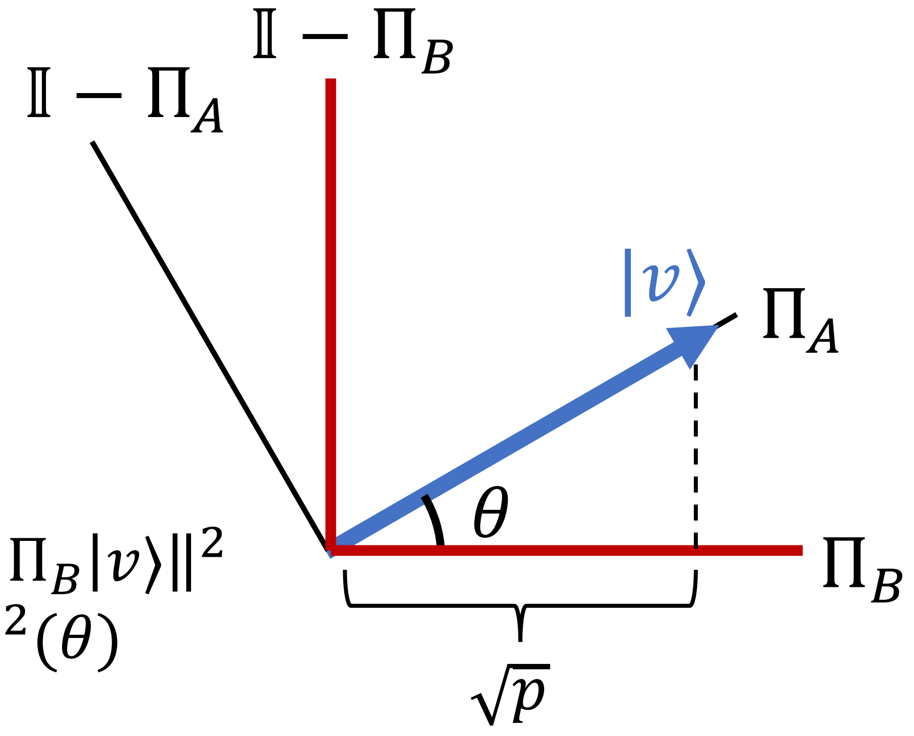
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

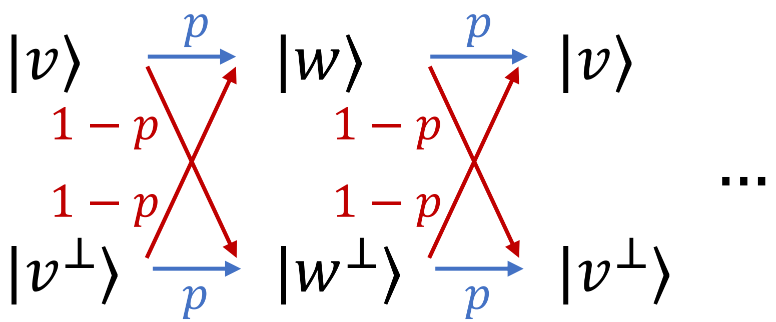
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

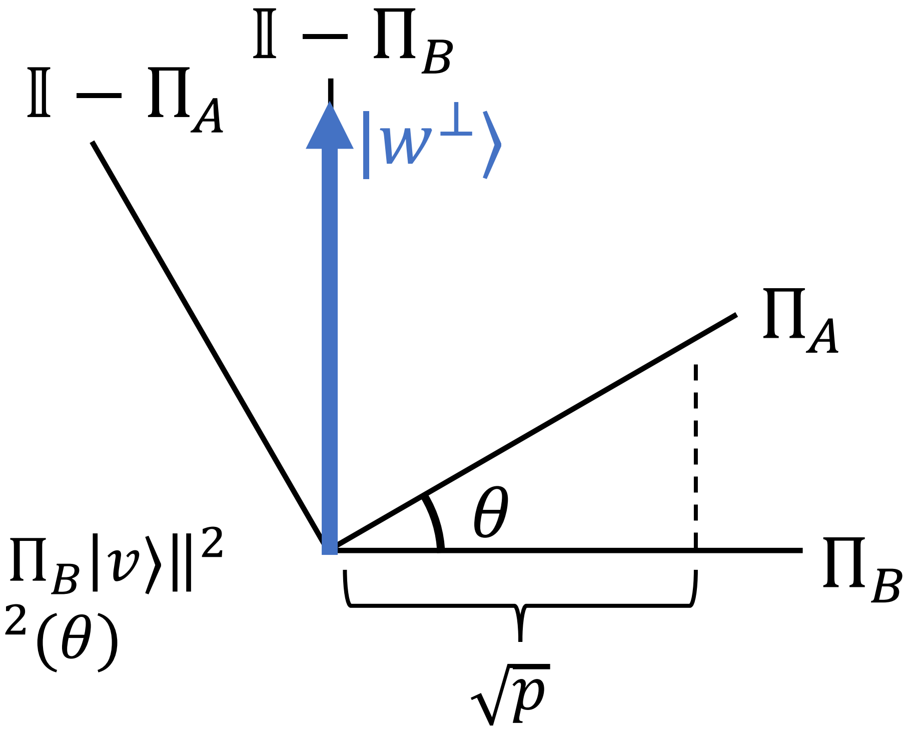
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

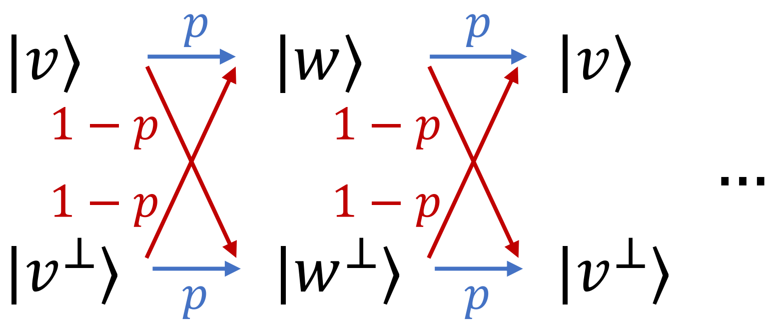
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

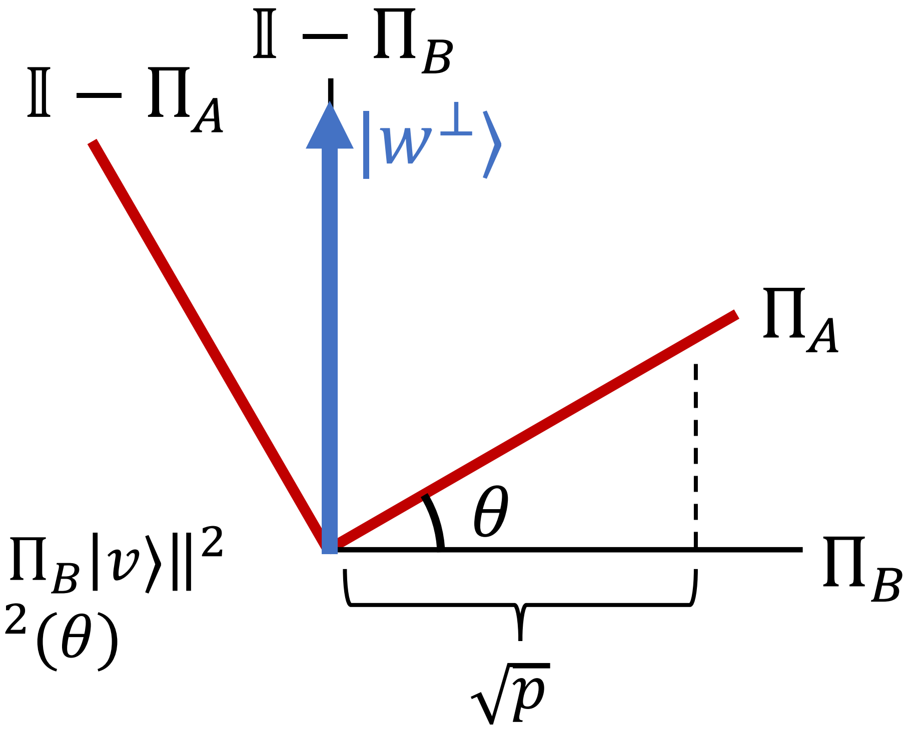
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

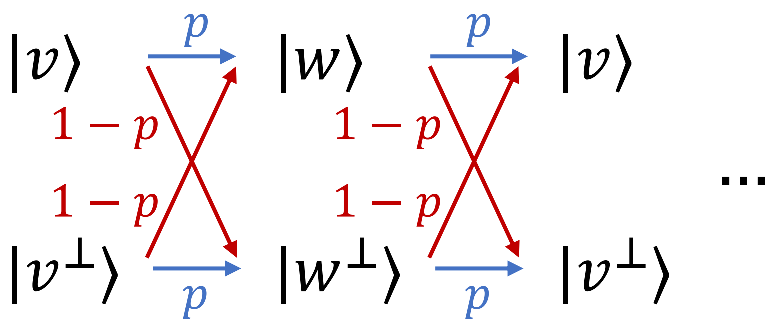
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

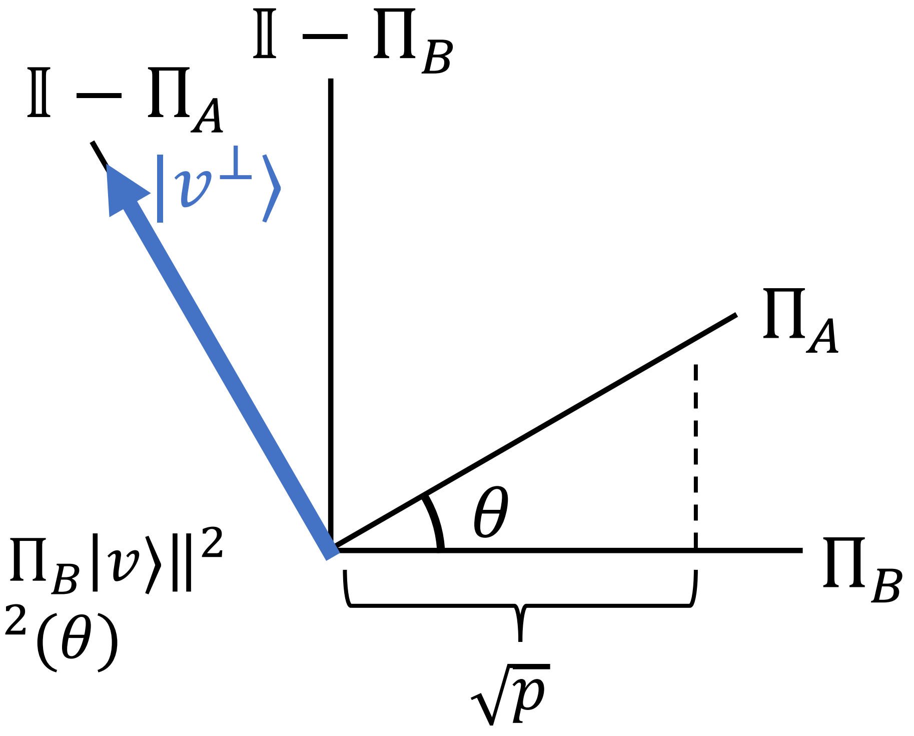
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

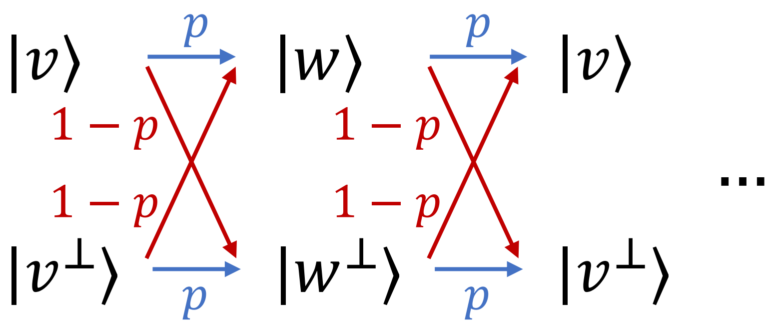
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

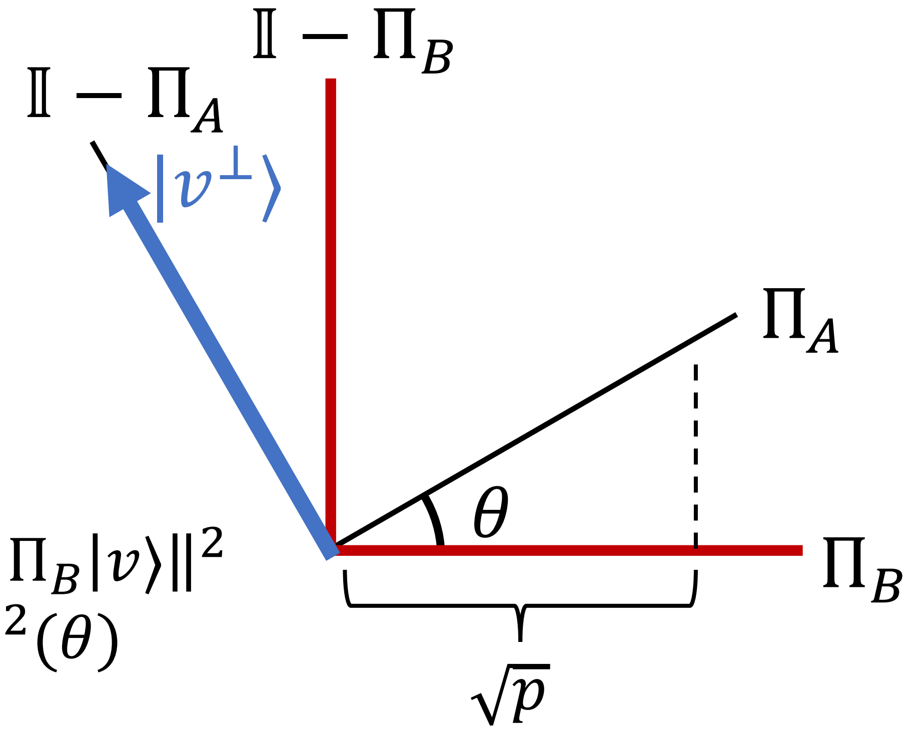
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

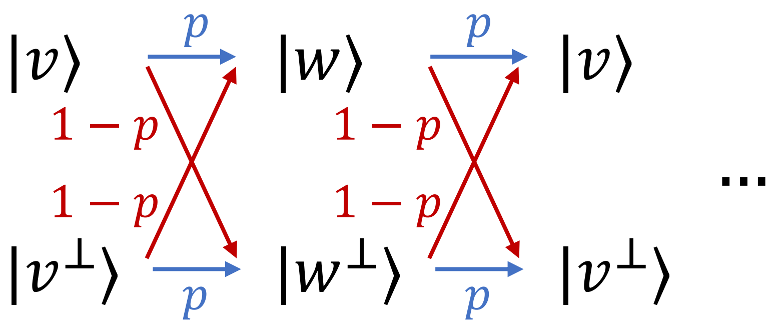
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

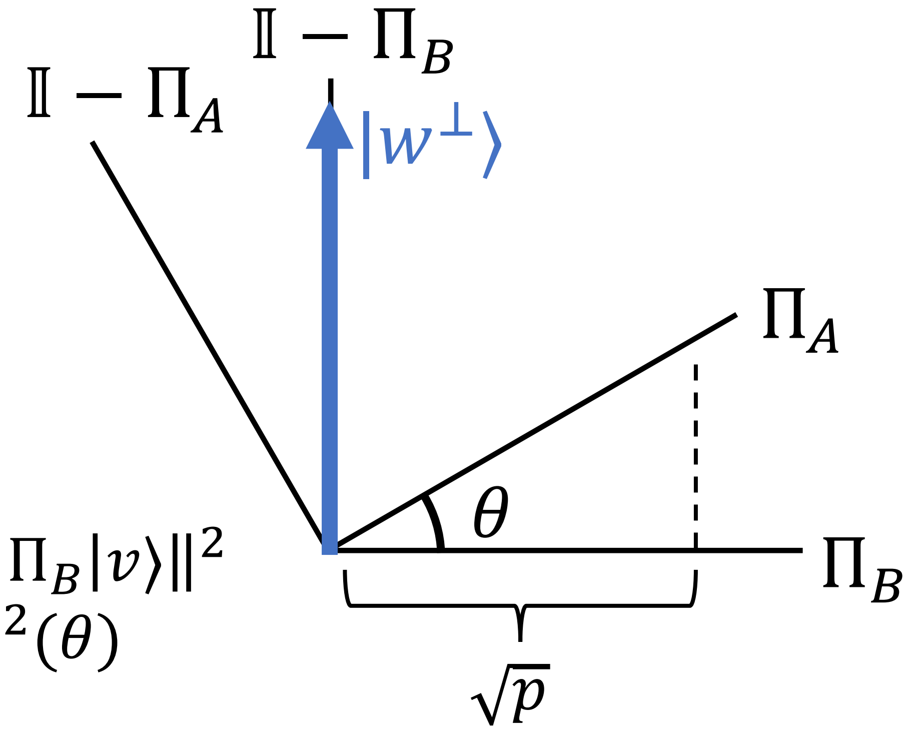
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

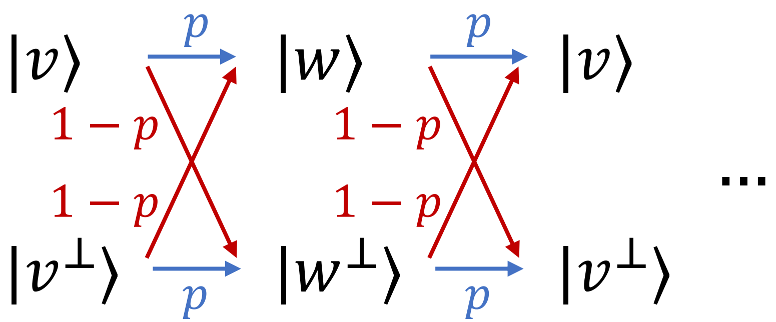
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

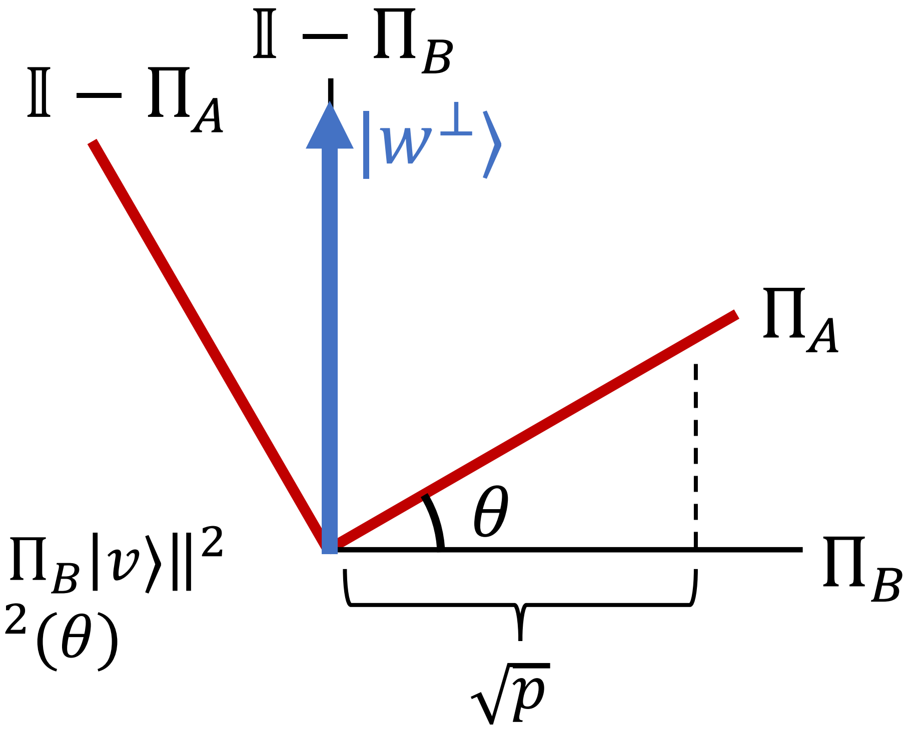
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

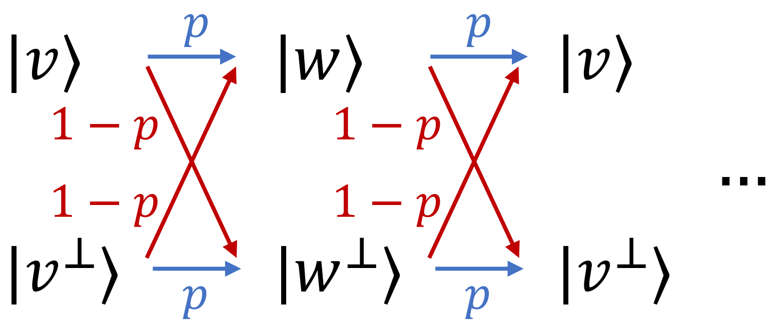
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

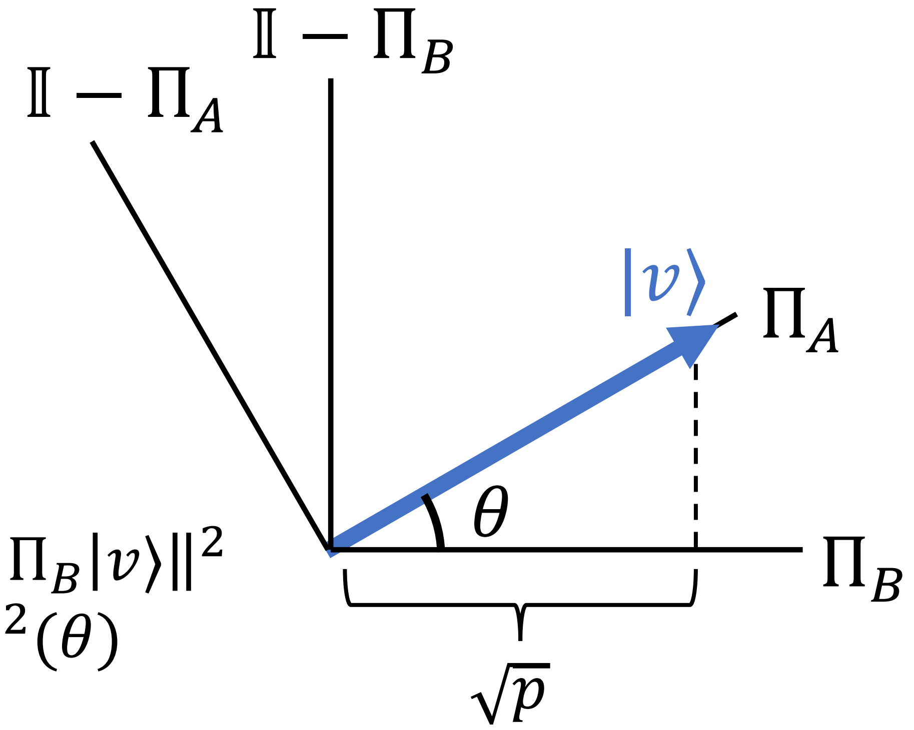
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

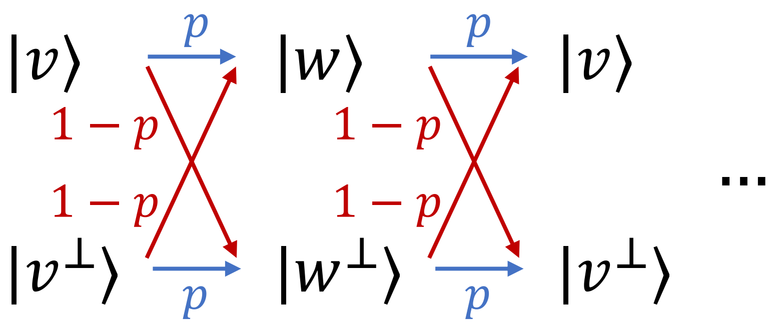
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

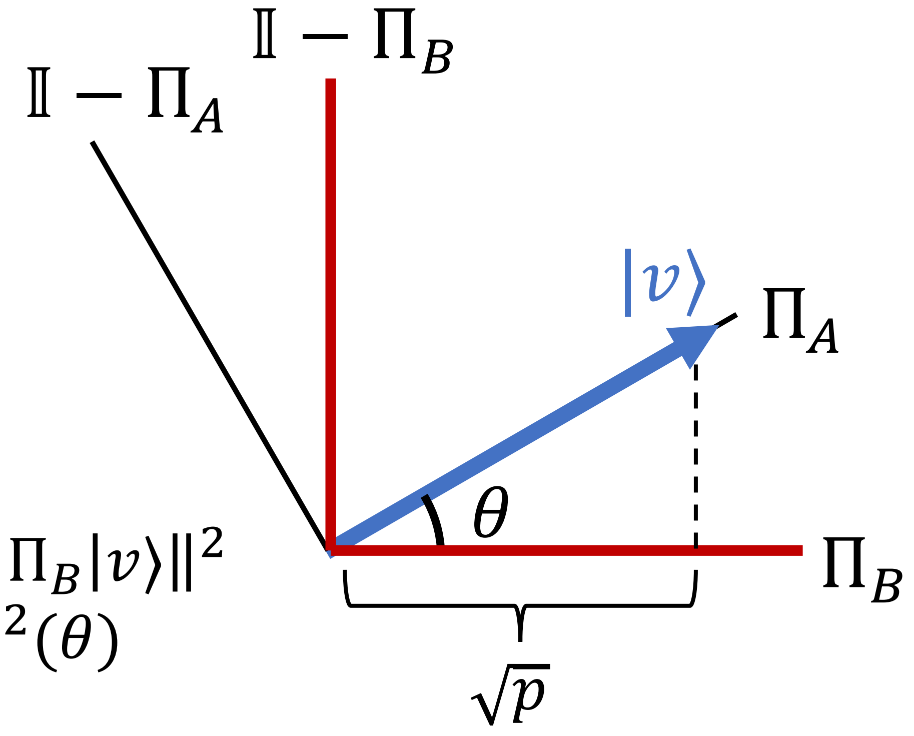
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

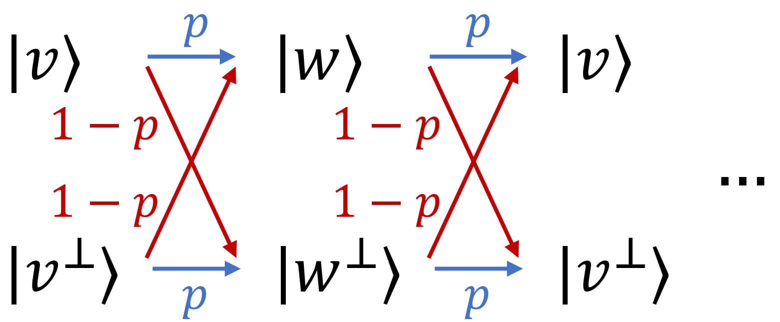
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

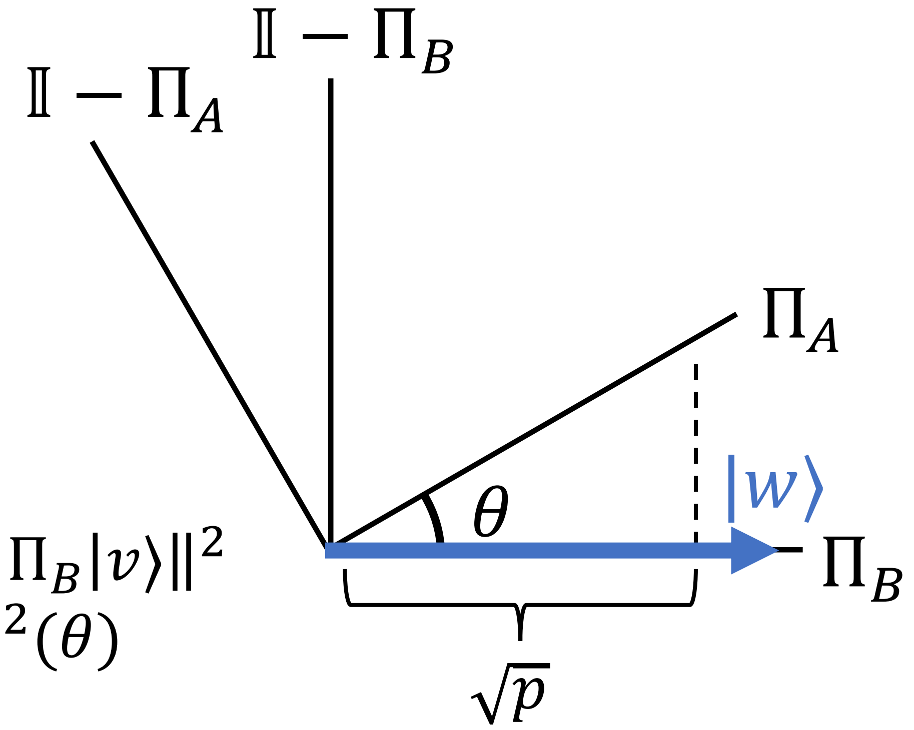
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

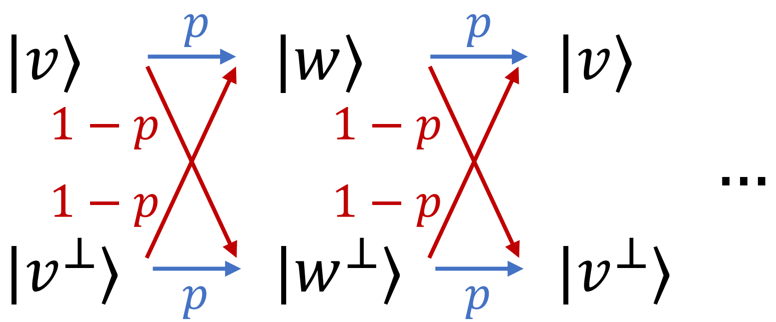
What happens if we start at $|v\rangle \in \mathbf{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

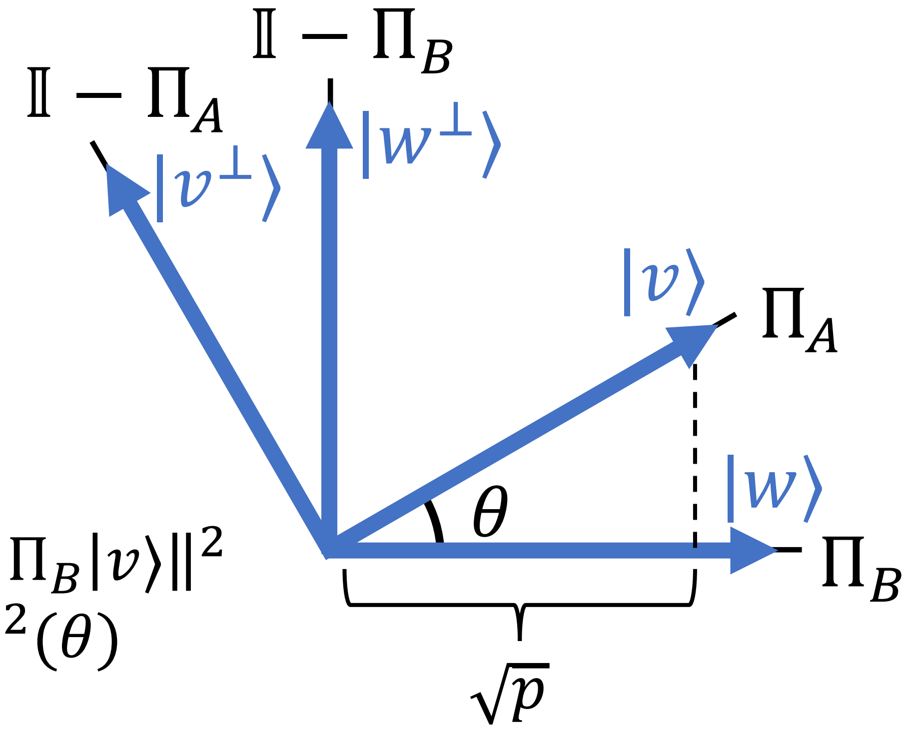
When we alternate measurements, we jump between four states



Understanding Alternating Measurements [MW05]

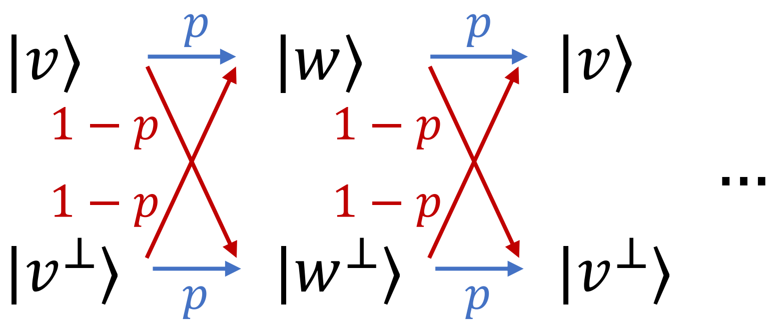
What happens if we start at $|v\rangle \in \mathrm{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

When we alternate measurements, we jump between four states

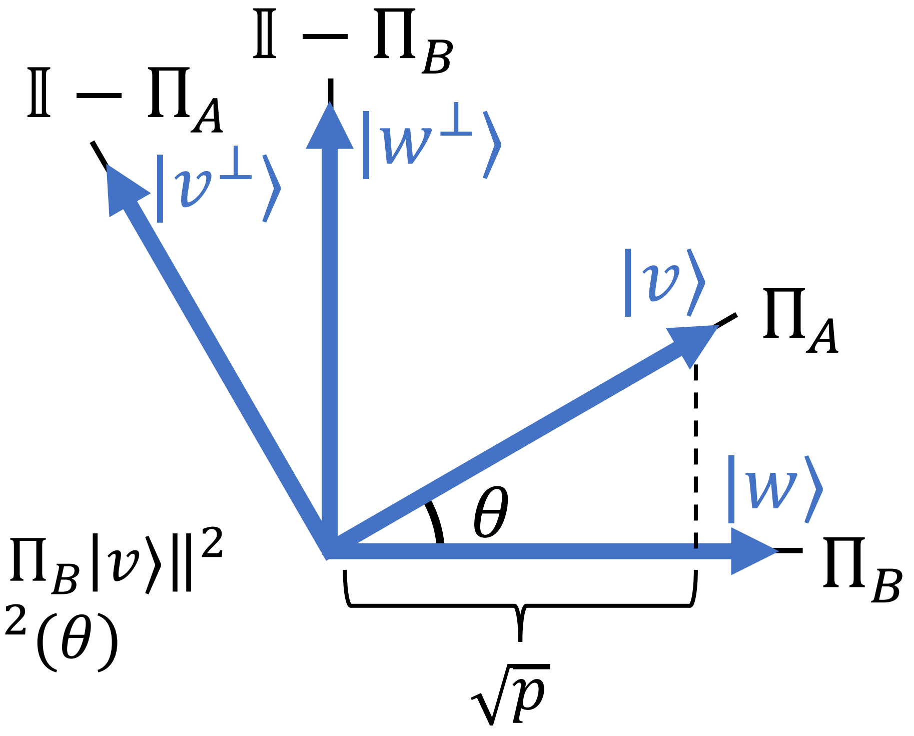


Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/p steps with prob $1 - 2^{-O(\lambda)}$.

Understanding Alternating Measurements [MW05]

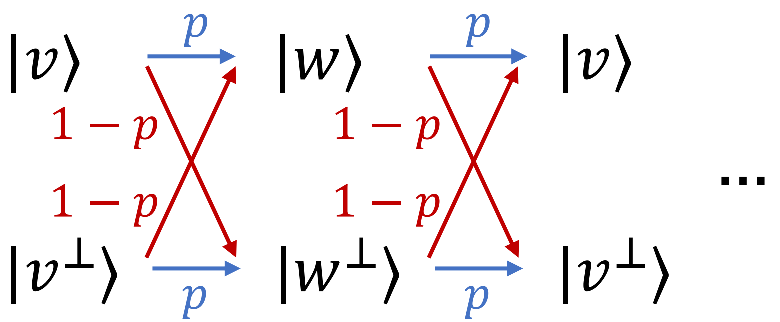
What happens if we start at $|v\rangle \in \mathrm{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

When we alternate measurements, we jump between four states



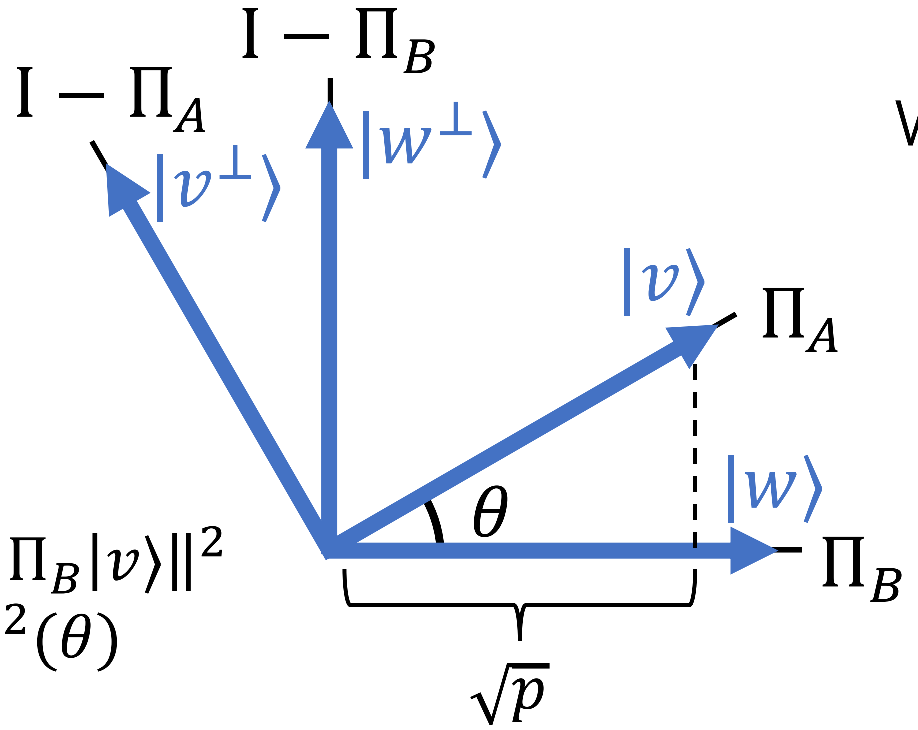
Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/p steps with prob $1 - 2^{-O(\lambda)}$.

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 $|v\rangle \in \mathrm{image}(\Pi_A)$ and alternate the measurements $(\Pi_A, \mathbb{I} - \Pi_A)$ and $(\Pi_B, \mathbb{I} - \Pi_B)$?

Easy case: Π_A, Π_B live in 2D



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

These are the guarantees we want, but Π_0, Π_G don't live in 2D!

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/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 Π_A, Π_B live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/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 Π_A, Π_B live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/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 Π_A, Π_B live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/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 Π_A, Π_B: no!

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

If Π_A, Π_B live in two dimensions:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/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 Π_A, Π_B: no!
- For Π_0, Π_G: yes!

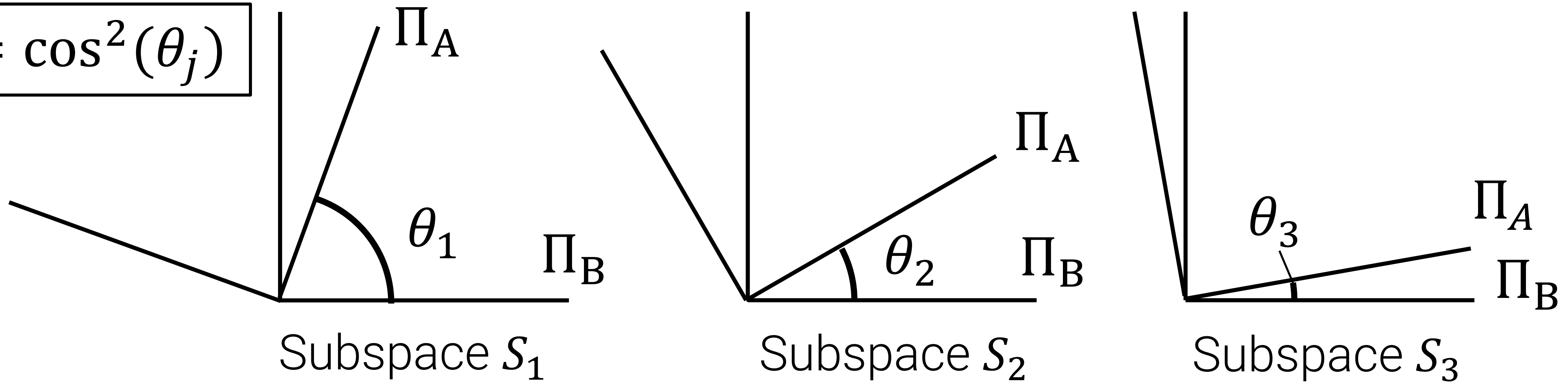
Extremely Useful Tool

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

Extremely Useful Tool

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

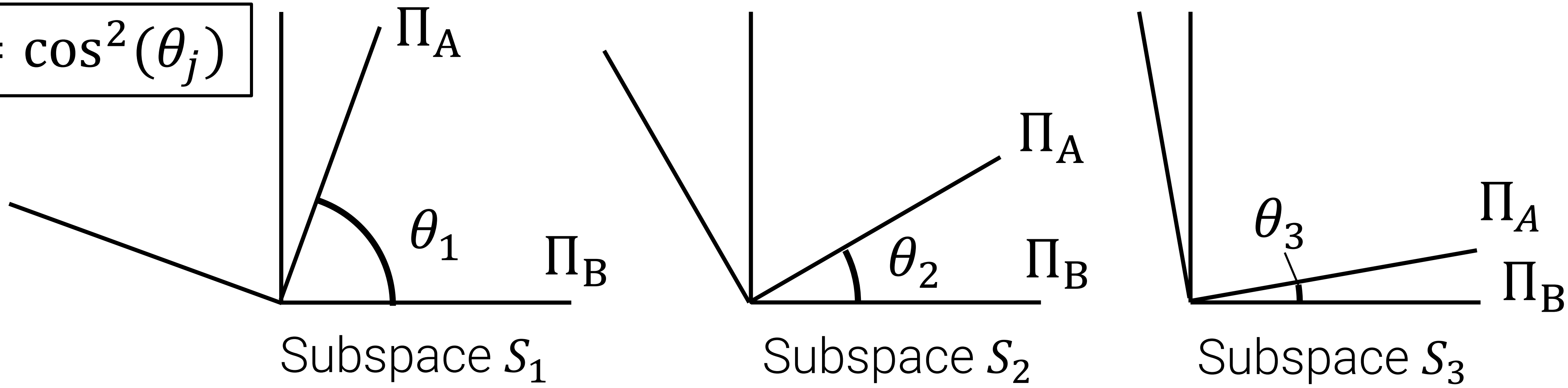
$$p_j = \cos^2(\theta_j)$$



Extremely Useful Tool

Jordan's Lemma: For any Π_A, Π_B, we can decompose space into 2-dim invariant subspaces $\{S_j\}$ where Π_A, Π_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 Π_0, Π_G.

Key Fact: for any $|\phi\rangle \in \mathrm{image}(\Pi_0)$, 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 $|\phi\rangle \in \text{image}(\Pi_0)$, 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 $\perp$.

$\xrightarrow{c}$

$\xleftarrow{r}$

$\xrightarrow{z}$
(if $r = r'$)

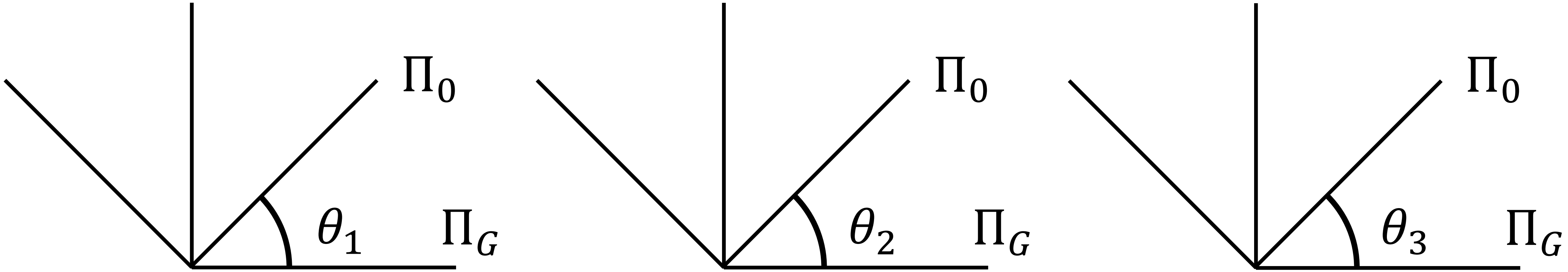
$V^*, |\psi\rangle$

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

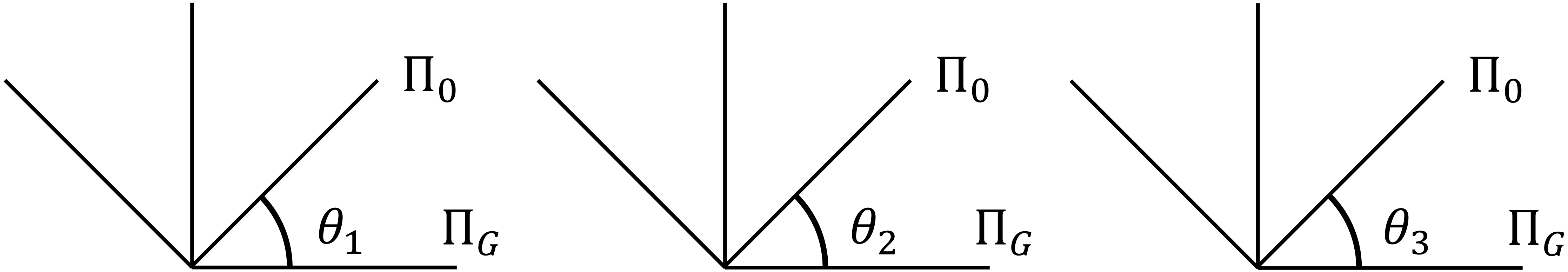
Equivalently, $p_j \approx 1/2$ in every Jordan subspace S_j (so $\theta_j \approx \pi/4$).



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

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

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 Π_A, Π_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 Π_A, Π_B in 2-D:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/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 Π_A, Π_B in 2-D:

Claim 1: $(\Pi_B, \mathbb{I} - \Pi_B)$ accepts in λ/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 (Π_A, Π_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 (Π_A, Π_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 (Π_A, Π_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 (Π_A, Π_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 Π_A, Π_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 (Π_A, Π_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 (Π_A, Π_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 (Π_A, Π_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 (Π_A, Π_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 Π_0 and Π_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 (Π_A, Π_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 Π_0 and Π_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.

Recap

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

Soundness:

- Collapse-binding commitments enable "lazy" measurement
- Unruh's rewinding: if protocol is collapsing, can extract *two* accepting transcripts from a successful adversary

Zero Knowledge:

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

The next two talks

Part 2: Unruh's rewinding applies to protocols where security requires extracting ***two*** transcripts.

What if we need more transcripts?

Part 3: Watrous' rewinding applies to protocols where simulation entails guessing the verifier's challenge.

What if guessing is impossible?

Thank You!

Questions?