Commitments to Quantum States

Fermi Ma

(Simons Institute and UC Berkeley)

based on joint work with:

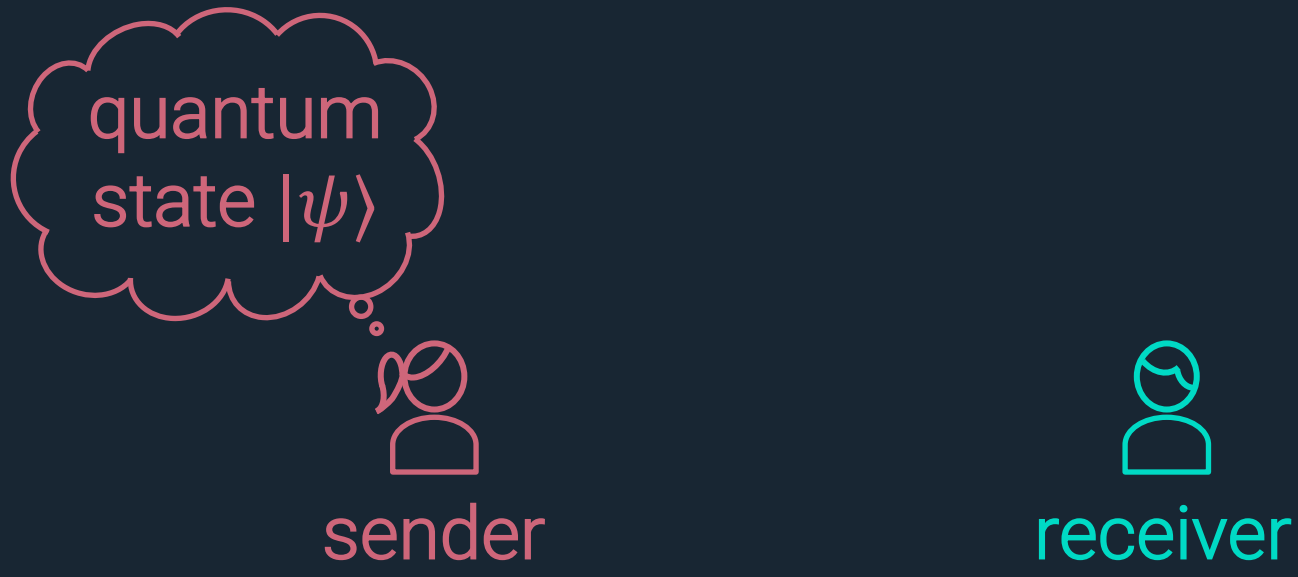
Sam Gunn (UC Berkeley)

Nathan Ju (UC Berkeley)

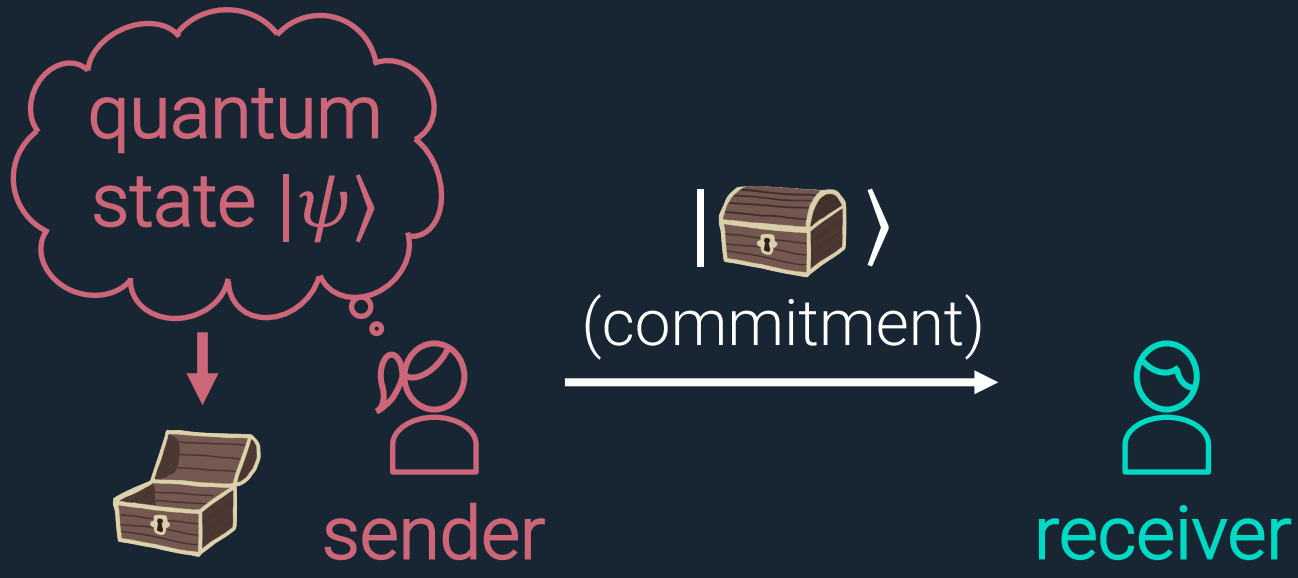
Mark Zhandry (NTT Research)

Is it possible to commit to *quantum information*?

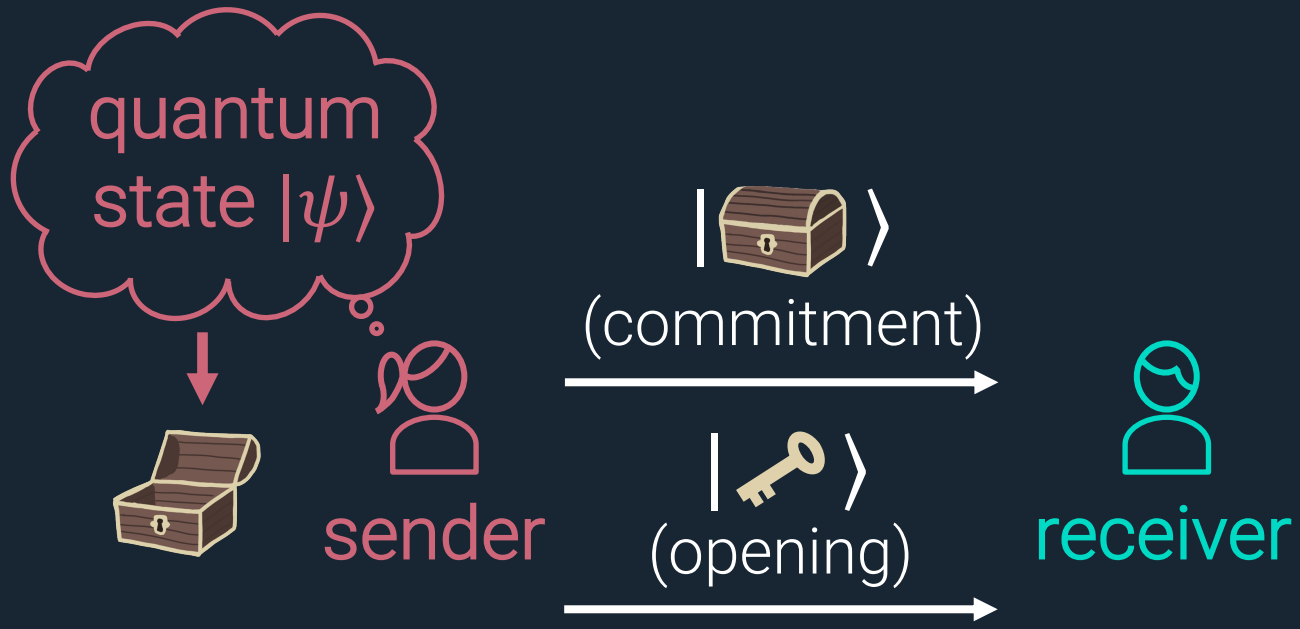
Is it possible to commit to *quantum information*?



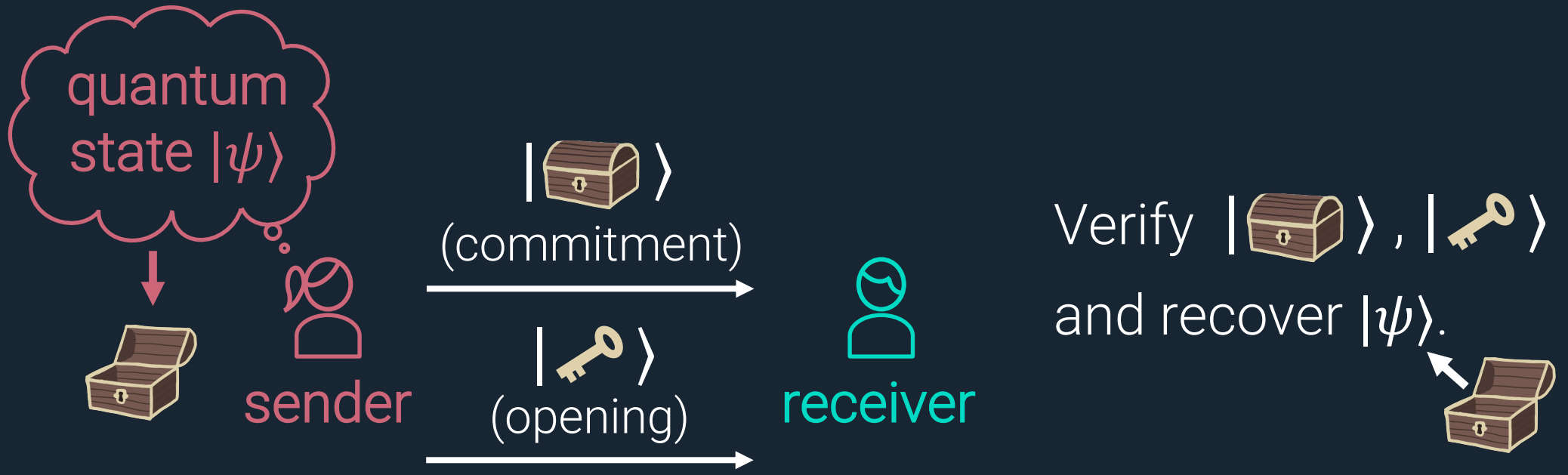
Is it possible to commit to *quantum information*?



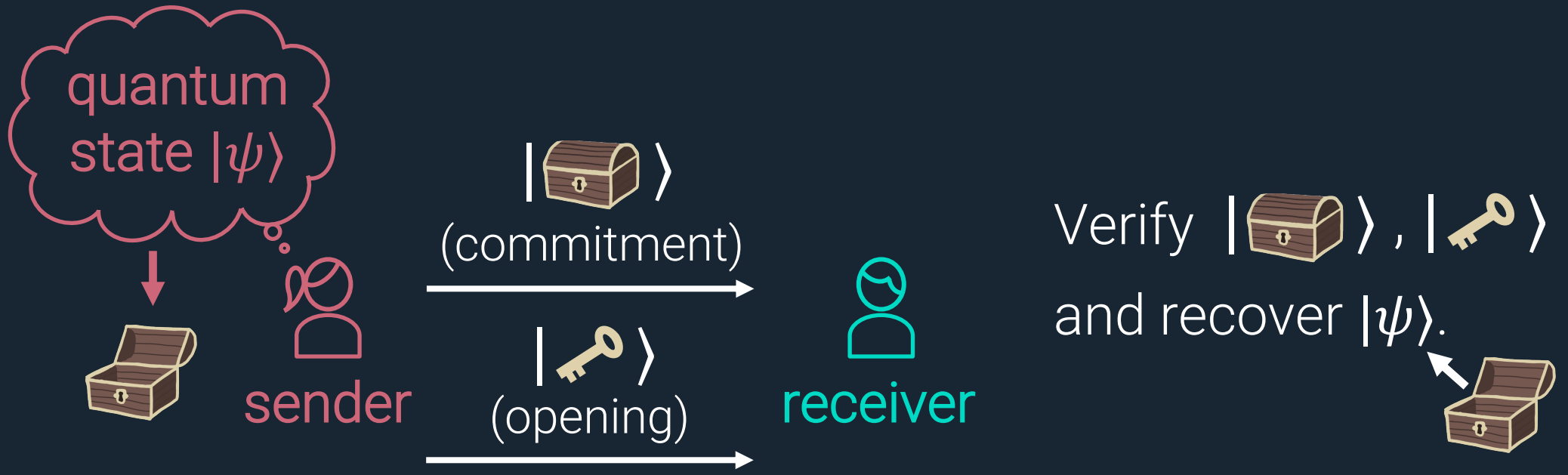
Is it possible to commit to *quantum information*?



Is it possible to commit to *quantum information*?

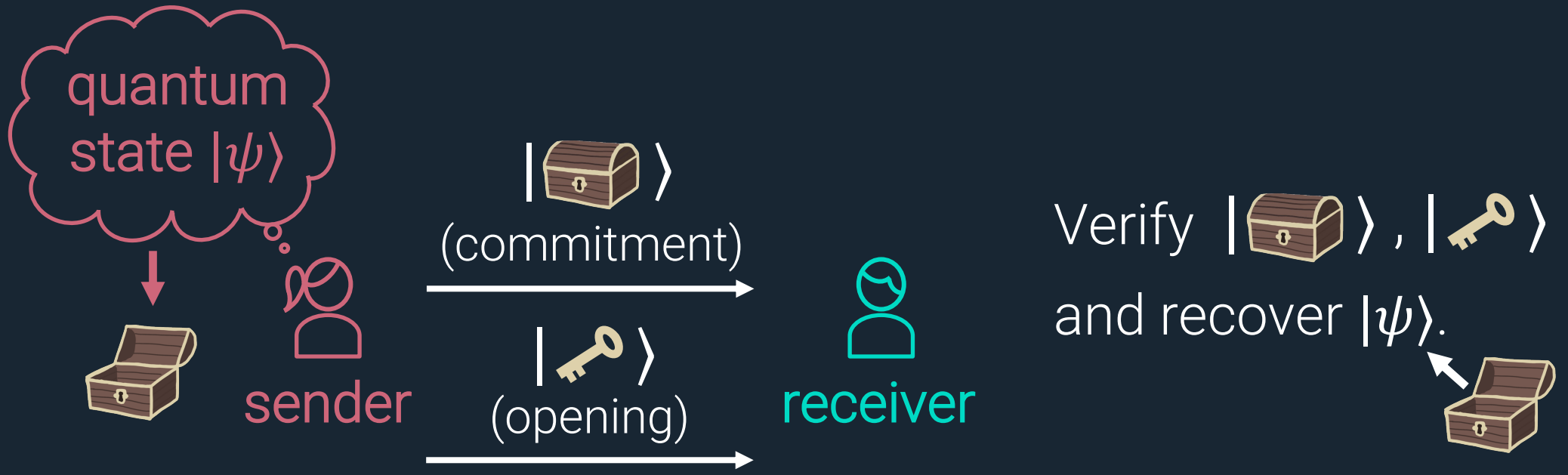


Is it possible to commit to *quantum information*?



Hiding: commitment hides message from receiver

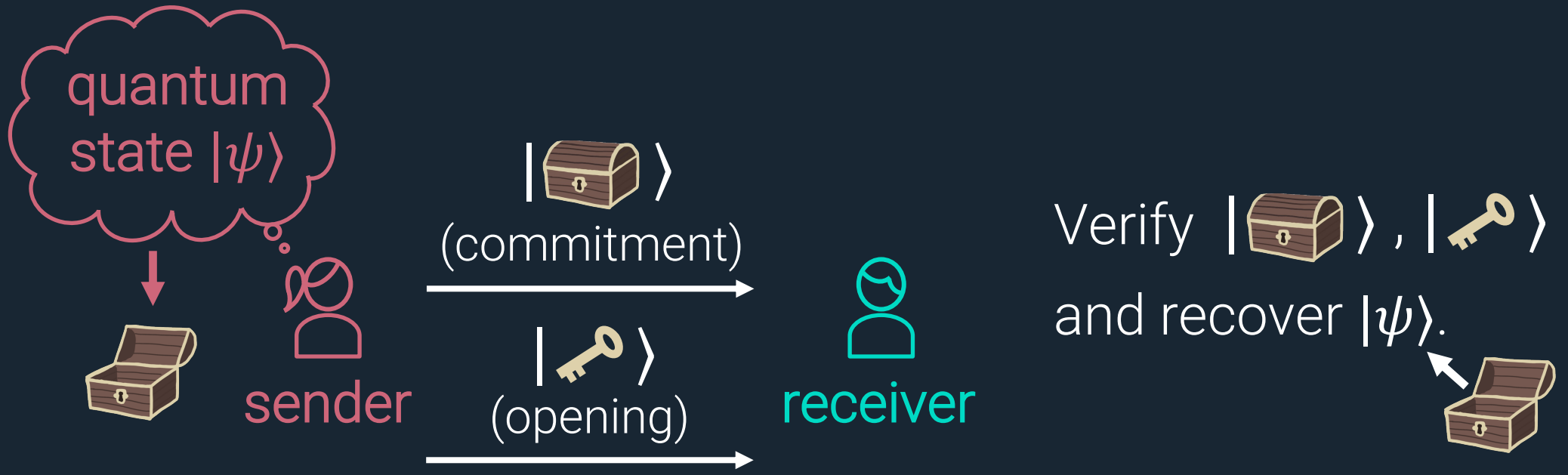
Is it possible to commit to *quantum information*?



Hiding: commitment hides message from receiver

Binding: sender can only open to unique message

Is it possible to commit to *quantum information*?



Folklore:
quantum one-time pad + classical-msg commitments

Folklore:
quantum one-time pad + classical-msg commitments

quantum state $|\psi\rangle$

sender

1) $a, b \leftarrow \{0,1\}$
2) $\mathrm{C} = \mathrm{Com}((a,b); r)$

$= (X^a Z^b |\psi\rangle, \mathrm{C})$

receiver

Folklore:
quantum one-time pad + classical-msg commitments

quantum state $|\psi\rangle$

sender

1) $a, b \leftarrow \{0,1\}$
2) $\mathrm{C} = \mathrm{Com}((a,b); r)$

- X is a bit flip: $X|b\rangle = |1-b\rangle$

$= (X^a Z^b |\psi\rangle, \mathrm{C})$

receiver

Folklore:
quantum one-time pad + classical-msg commitments

quantum state $|\psi\rangle$

sender

- X is a bit flip: $X|b\rangle = |1-b\rangle$
- Z is a phase flip: $Z|b\rangle = (-1)^b|b\rangle$

$= (X^a Z^b|\psi\rangle, \mathrm{C})$

receiver

1) $a, b \leftarrow \{0,1\}$
2) $\mathrm{C} = \mathrm{Com}((a,b); r)$

Folklore:
quantum one-time pad + classical-msg commitments

quantum state $|\psi\rangle$

sender

1) $a, b \leftarrow \{0,1\}$
2) $\mathrm{C} = \mathrm{Com}((a,b); r)$

- X is a bit flip: $X|b\rangle = |1-b\rangle$
- Z is a phase flip: $Z|b\rangle = (-1)^b|b\rangle$
- Fact: $X^a Z^b|\psi\rangle$ is "maximally mixed"

$= (X^a Z^b|\psi\rangle, \mathrm{C})$

receiver

Folklore:
quantum one-time pad + classical-msg commitments

- X is a bit flip: $X|b\rangle = |1-b\rangle$
- Z is a phase flip: $Z|b\rangle = (-1)^b|b\rangle$
- Fact: $X^a Z^b|\psi\rangle$ is "maximally mixed"

quantum state $|\psi\rangle$

sender

receiver

1) $a, b \leftarrow \{0,1\}$
2) $\mathrm{C} = \mathrm{Com}((a,b);r)$

$= (X^a Z^b|\psi\rangle, \mathrm{C})$

$= (a, b, r)$

Folklore:
quantum one-time pad + classical-msg commitments

- X is a bit flip: $X|b\rangle = |1-b\rangle$
- Z is a phase flip: $Z|b\rangle = (-1)^b|b\rangle$
- Fact: $X^a Z^b|\psi\rangle$ is "maximally mixed"

quantum state $|\psi\rangle$

sender

1) $a, b \leftarrow \{0,1\}$
2) $\mathrm{C} = \mathrm{Com}((a,b);r)$

$= (X^a Z^b|\psi\rangle, \mathrm{C})$

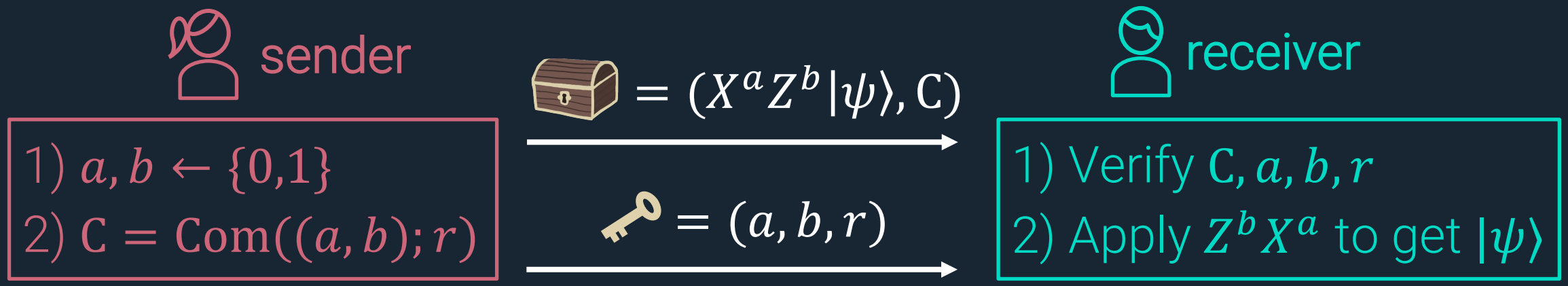
$= (a,b,r)$

receiver

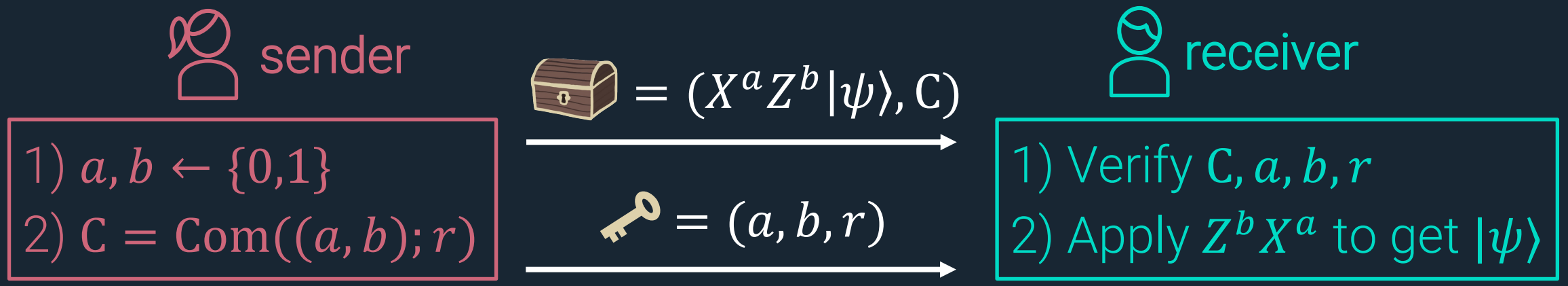
1) Verify C, a, b, r
2) Apply $Z^b X^a$ to get $|\psi\rangle$

Folklore:
quantum one-time pad + classical-msg commitments

Security seems “obvious”…



Security seems “obvious”…



Security seems “obvious”…

Hiding (commitment hides $|\psi\rangle$ from receiver)

sender

1) $a, b \leftarrow \{0,1\}$
2) $\mathrm{C} = \mathrm{Com}((a,b);r)$

$= (X^a Z^b |\psi\rangle, \mathrm{C})$

$= (a, b, r)$

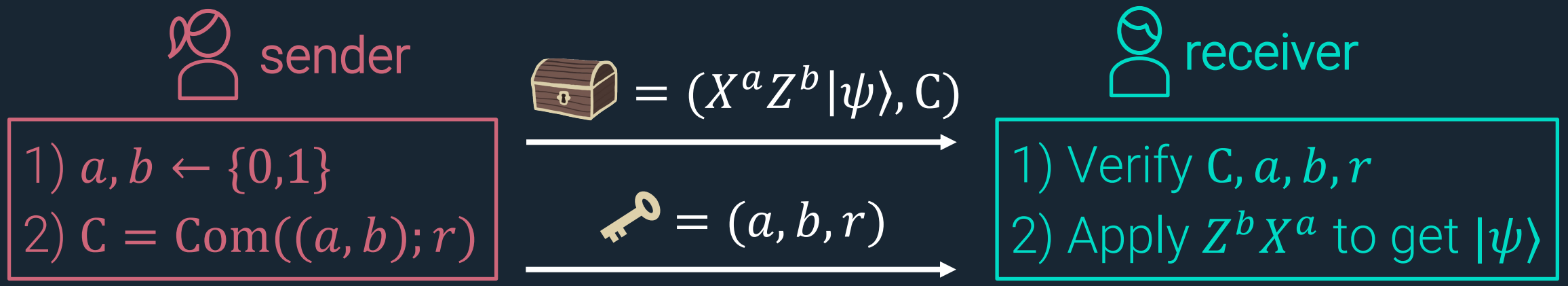
receiver

1) Verify C, a, b, r
2) Apply $Z^b X^a$ to get $|\psi\rangle$

Security seems “obvious”…

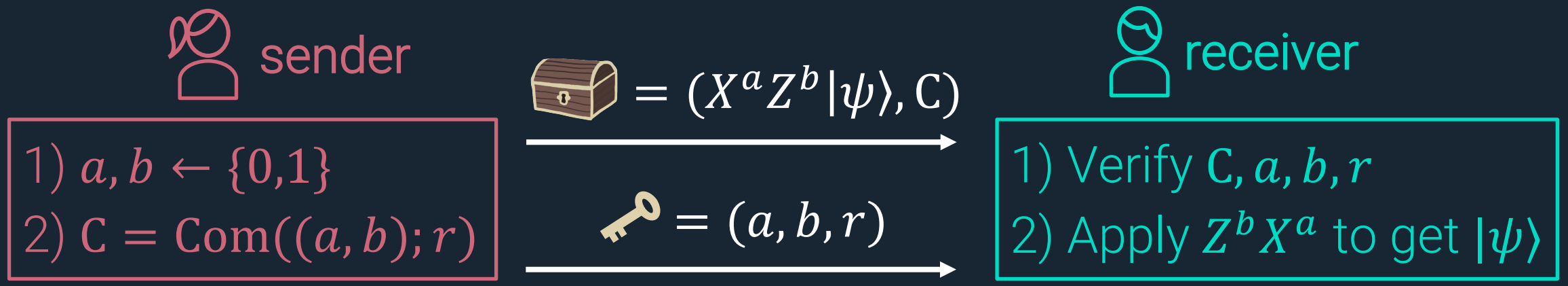
Hiding (commitment hides $|\psi\rangle$ from receiver)

- Intuition: $X^a Z^b |\psi\rangle$ is maximally mixed and C hides a, b.



Security seems “obvious”…

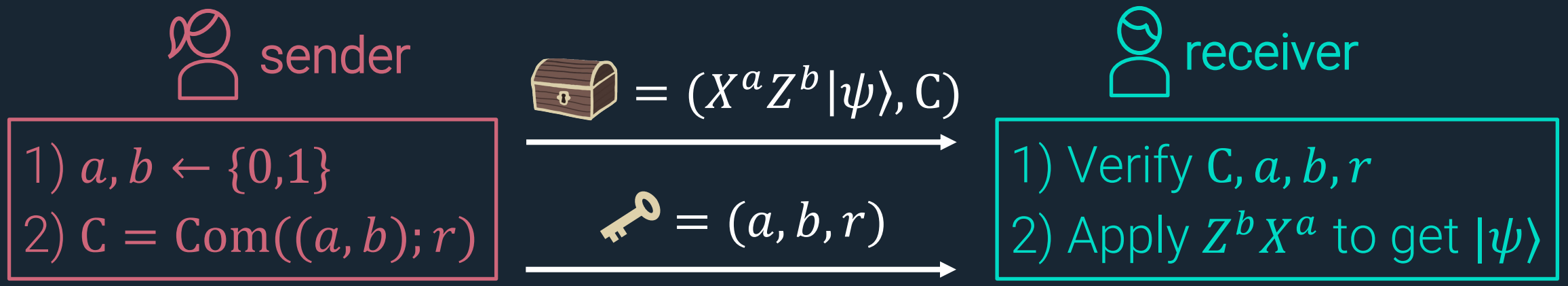
Binding (sender can only open to unique $|\psi\rangle$)



Security seems “obvious”…

Binding (sender can only open to unique $|\psi\rangle$)

- Intuition: C is binding to a, b and receiver holds $X^a Z^b |\psi\rangle$.



Big problem: totally unclear what this means!

Binding (sender can only open to unique $|\psi\rangle$)

- Intuition: C is binding to a, b and receiver holds $X^a Z^b |\psi\rangle$.

Our current understanding of commitments to quantum states:

Our current understanding of commitments to quantum states:

- one folklore construction

Our current understanding of commitments to quantum states:

- one folklore construction
- no security definitions

Our current understanding of commitments to quantum states:

- one folklore construction
- no security definitions
- …that’s it

This work: a theory of quantum state commitments (QSCs)

This work: a theory of quantum state commitments (QSCs)

definitions

constructions

applications

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

constructions

applications

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

applications

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)

applications

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)
(2) first ***succinct*** QSC (|commitment| < |message|)

applications

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)
(2) first ***succinct*** QSC (|commitment| < |message|)

- (1), (2) are non-interactive + use weaker-than-OWF assumptions

applications

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)
(2) first ***succinct*** QSC (|commitment| < |message|)

- (1), (2) are non-interactive + use weaker-than-OWF assumptions

applications

succinct QSC + quantum PCP → succinct arguments

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)
(2) first ***succinct*** QSC (|commitment| < |message|)

- (1), (2) are non-interactive + use weaker-than-OWF assumptions

applications

succinct QSC + quantum PCP → succinct arguments

- 3-msg succinct arg for NP from weaker-than-OWF assumptions

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)
(2) first ***succinct*** QSC (|commitment| < |message|)

- (1), (2) are non-interactive + use weaker-than-OWF assumptions

applications

succinct QSC + quantum PCP → succinct arguments

- 3-msg succinct arg for NP from weaker-than-OWF assumptions

classical comparison: [Kilian92] is 4 messages + assumes CRHFs

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)
(2) first ***succinct*** QSC (|commitment| < |message|)

- (1), (2) are non-interactive + use weaker-than-OWF assumptions

applications

succinct QSC + quantum PCP → succinct arguments

- 3-msg succinct arg for NP from weaker-than-OWF assumptions
- extends to QMA assuming quantum PCP conjecture!

This work: a theory of quantum state commitments (QSCs)

definitions

binding: committing to $|\psi\rangle$ ***erases*** it from sender's view.

- handles entanglement
- falsifiable, composable
- extends classical-msg binding
- hiding-binding duality!

constructions

(1) hiding-binding QSC (formalizing folklore)
(2) first ***succinct*** QSC (|commitment| < |message|)

- (1), (2) are non-interactive + use weaker-than-OWF assumptions

applications

succinct QSC + quantum PCP → succinct arguments

- 3-msg succinct arg for NP from weaker-than-OWF assumptions
- extends to QMA assuming quantum PCP conjecture!
- new tools to rewind quantum protocols/extract quantum states

Plan for today

1) What does it mean to commit to a quantum state?

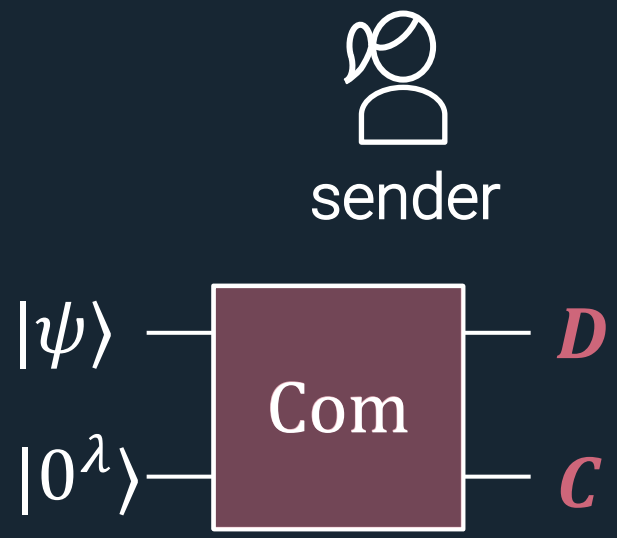
2) Can we ***succinctly*** commit to a quantum state?

3) Application: quantum succinct arguments

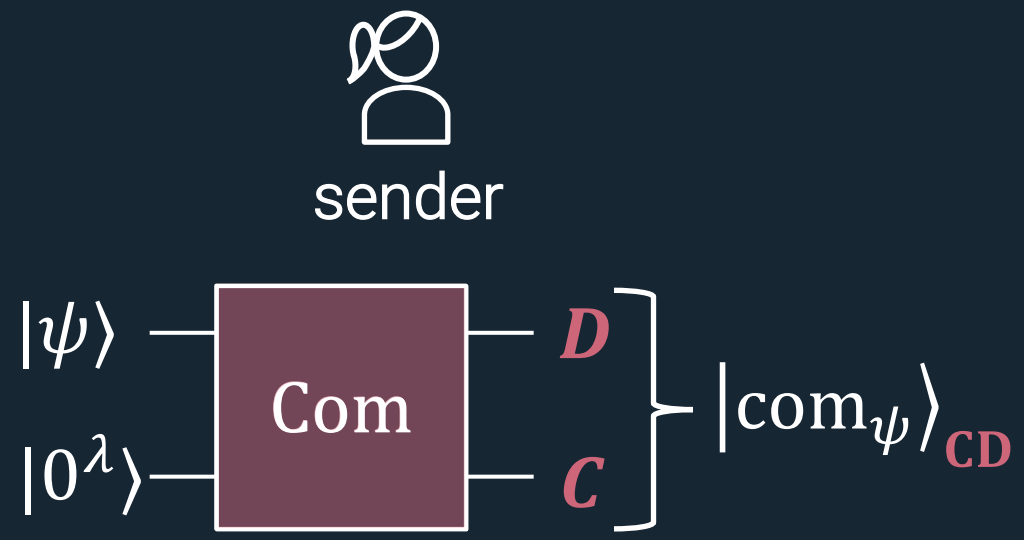
Plan for today

1) What does it mean to commit to a quantum state?
2) Can we ***succinctly*** commit to a quantum state?
3) Application: quantum succinct arguments

Step 0: basic syntax for QSCs

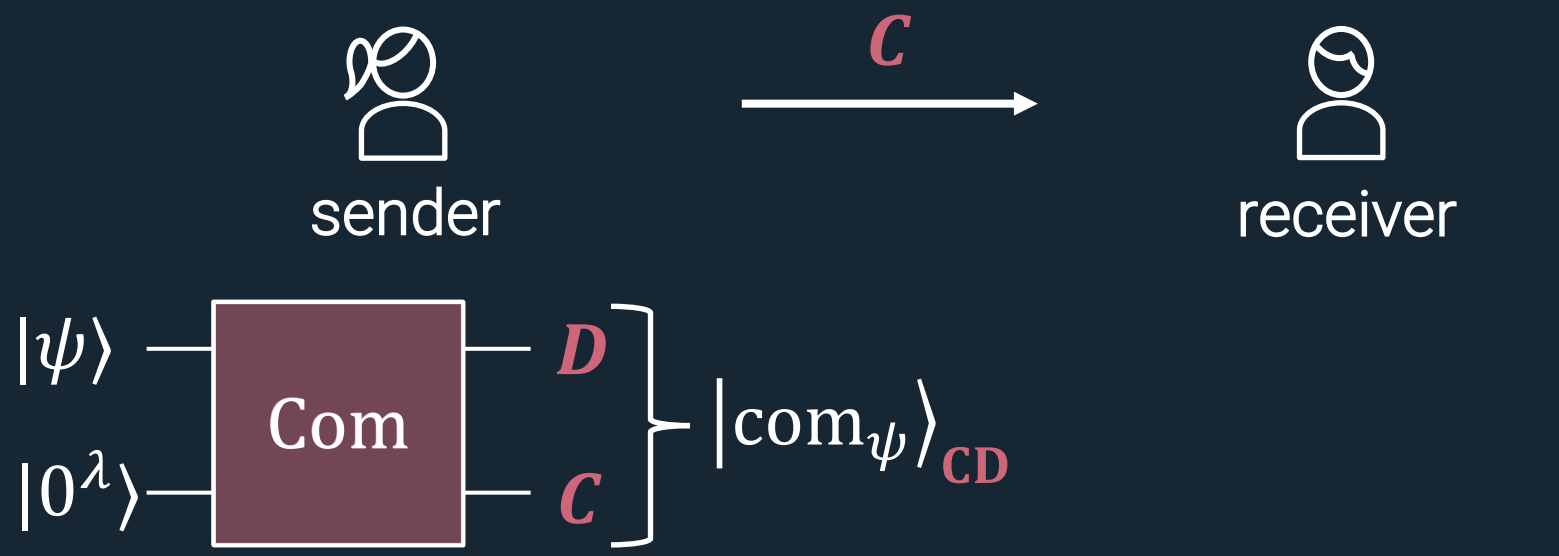


Step 0: basic syntax for QSCs



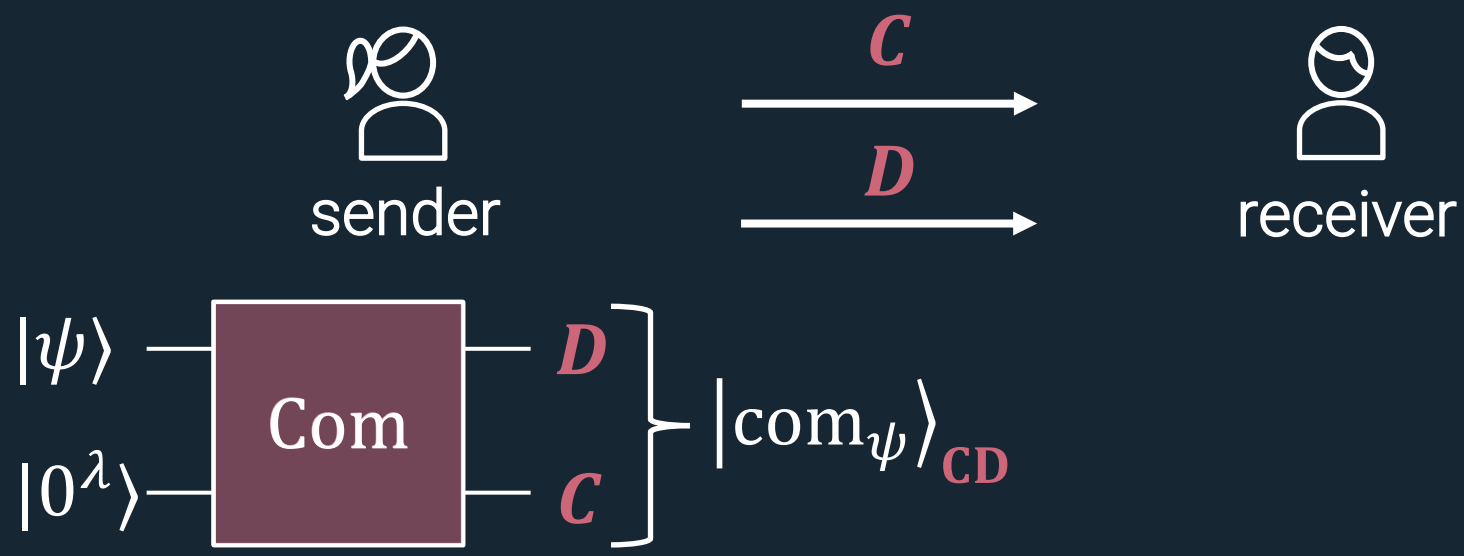
- **To commit to $|\psi\rangle$**: prepare $|\mathrm{com}_\psi\rangle_{\mathrm{CD}} = \mathrm{Com}|\psi\rangle|0^\lambda\rangle$, send C to commit, send D to decommit.

Step 0: basic syntax for QSCs



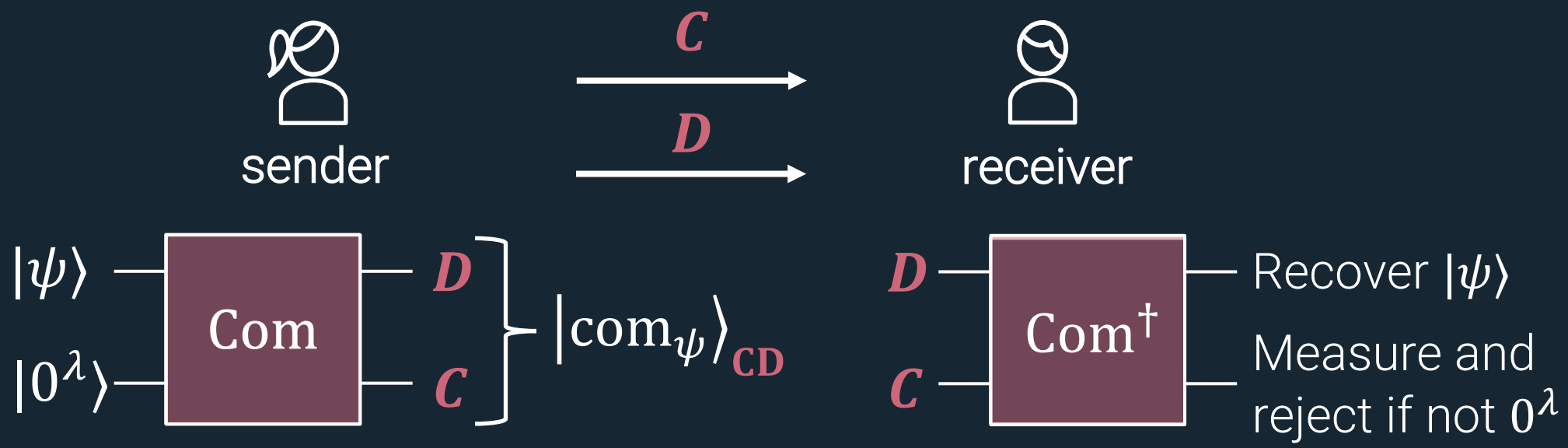
- **To commit to $|\psi\rangle$**: prepare $|\mathrm{com}_\psi\rangle_{\mathrm{CD}} = \mathrm{Com}|\psi\rangle|0^\lambda\rangle$, send $\boldsymbol{C}$ to commit, send $\boldsymbol{D}$ to decommit.

Step 0: basic syntax for QSCs



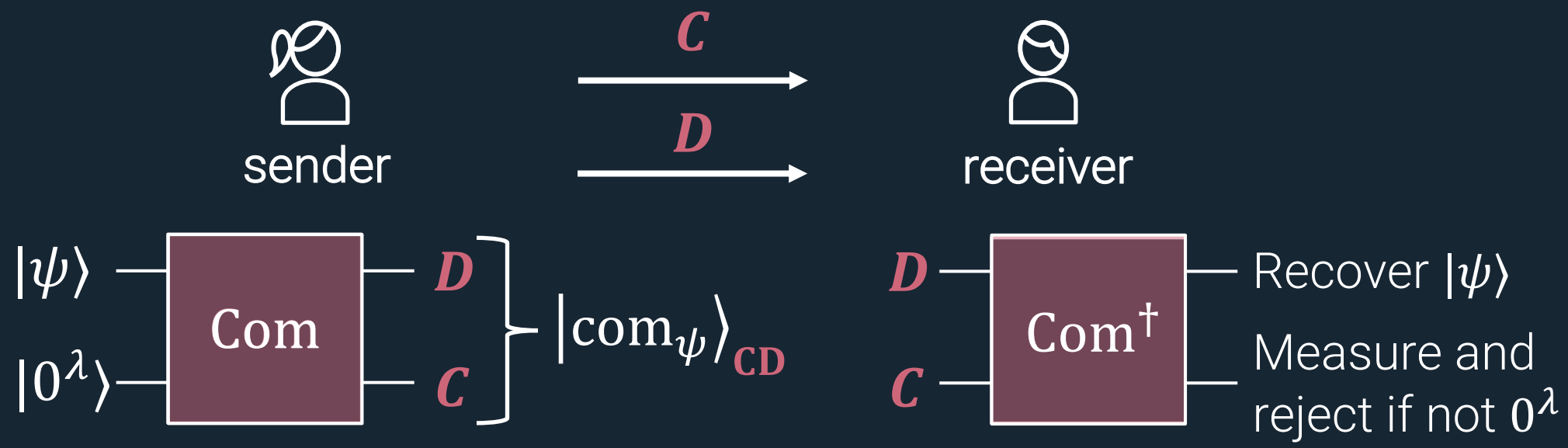
- **To commit to $|\psi\rangle$**: prepare $|\mathrm{com}_\psi\rangle_{\mathrm{CD}} = \mathrm{Com}|\psi\rangle|0^\lambda\rangle$, send $\boldsymbol{C}$ to commit, send $\boldsymbol{D}$ to decommit.

Step 0: basic syntax for QSCs



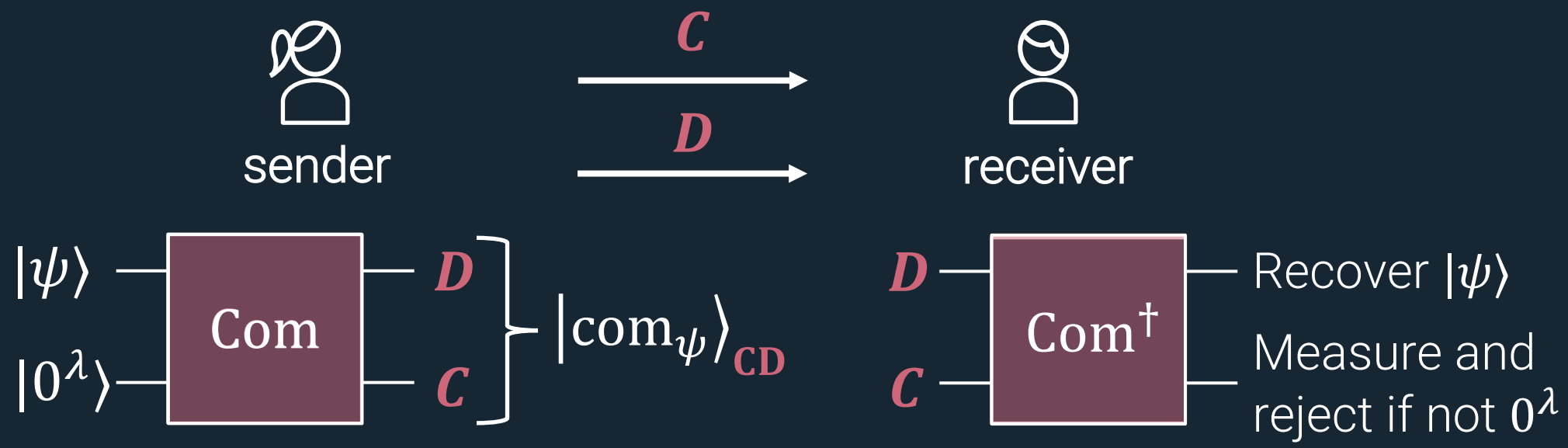
- **To commit to $|\psi\rangle$**: prepare $|\mathrm{com}_\psi\rangle_{\mathrm{CD}} = \mathrm{Com}|\psi\rangle|0^\lambda\rangle$, send C to commit, send D to decommit.

Step 0: basic syntax for QSCs



- **To commit to $|\psi\rangle$**: prepare $|\mathrm{com}_\psi\rangle_{\mathrm{CD}} = \mathrm{Com}|\psi\rangle|0^\lambda\rangle$, send C to commit, send D to decommit.
- **To verify:** apply $\mathrm{Com}^\dagger$ and check if the last λ qubits are 0

Step 0: basic syntax for QSCs



- **To commit to $|\psi\rangle$**: prepare $|\mathrm{com}_\psi\rangle_{\mathrm{CD}} = \mathrm{Com}|\psi\rangle|0^\lambda\rangle$, send C to commit, send D to decommit.
- **To verify:** apply $\mathrm{Com}^\dagger$ and check if the last λ qubits are 0

(any QSC can be rewritten in this form)

What does it mean to commit to a quantum state?

Classical binding definition: Adv can't output commitment c and two valid openings $(m_0, r_0), (m_1, r_1)$ to distinct messages $m_0 \neq m_1$.

Classical binding definition: Adv can't output commitment c and two valid openings $(m_0, r_0), (m_1, r_1)$ to distinct messages $m_0 \neq m_1$.

This definition completely fails for quantum state commitments.

Classical binding definition: Adv can't output commitment c and two valid openings $(m_0, r_0), (m_1, r_1)$ to distinct messages $m_0 \neq m_1$.

This definition completely fails for quantum state commitments.

Many problems:

1) Verifying the first opening might disturb the commitment.

Classical binding definition: Adv can't output commitment c and two valid openings $(m_0, r_0), (m_1, r_1)$ to distinct messages $m_0 \neq m_1$.

This definition completely fails for quantum state commitments.

Many problems:

1) Verifying the first opening might disturb the commitment.
2) Challenger can't check $\psi_0 \neq \psi_1$!

Classical binding definition: Adv can't output commitment c and two valid openings $(m_0, r_0), (m_1, r_1)$ to distinct messages $m_0 \neq m_1$.

This definition completely fails for quantum state commitments.

Many problems:

1) Verifying the first opening might disturb the commitment.
2) Challenger can't check $\psi_0 \neq \psi_1$!
3) Quantum attacker might not produce two openings *simultaneously*.

Classical binding definition: Adv can't output commitment c and two valid openings $(m_0, r_0), (m_1, r_1)$ to distinct messages $m_0 \neq m_1$.

This definition completely fails for quantum state commitments.

Many problems:

1) Verifying the first opening might disturb the commitment.
2) Challenger can't check $\psi_0 \neq \psi_1$!
3) Quantum attacker might not produce two openings *simultaneously*.

A priori, not obvious that a cryptographic definition is possible!

Classical binding definition: Adv can't output commitment c and two valid openings $(m_0, r_0), (m_1, r_1)$ to distinct messages $m_0 \neq m_1$.

This definition completely fails for quantum state commitments.

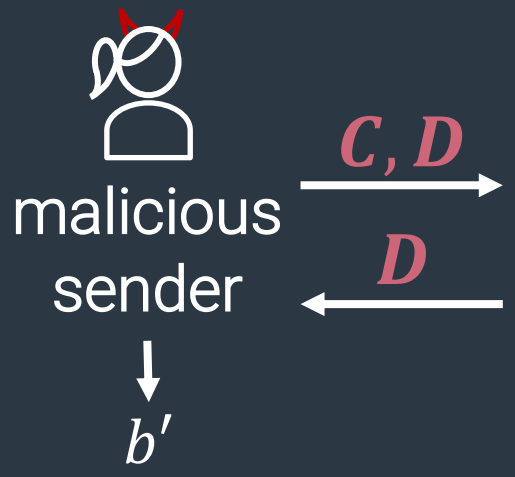
Many problems:

1) Verifying the first opening might disturb the commitment.
2) Challenger can't check $\psi_0 \neq \psi_1$!
3) Quantum attacker might not produce two openings *simultaneously*.

As a result, our new definition looks quite different…

Our Definition: Swap Binding

Our Definition: Swap Binding



$\boldsymbol{C}, \boldsymbol{D}$

$\boldsymbol{D}$

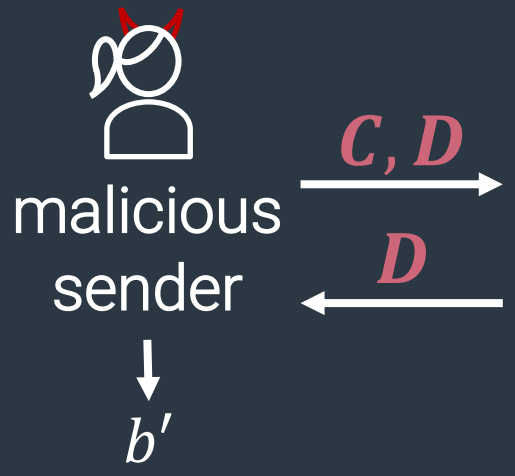
Challenger

1) Verify $\boldsymbol{C}, \boldsymbol{D}$.

2) $b \leftarrow \{0,1\}$. If $b = 0$, swap $|\psi\rangle$ with junk.

Binding: $\Pr[b' = b] \leq 1/2 + \mathrm{negl}(\lambda)$

Our Definition: Swap Binding



$\boldsymbol{C}, \boldsymbol{D}$

$\boldsymbol{D}$

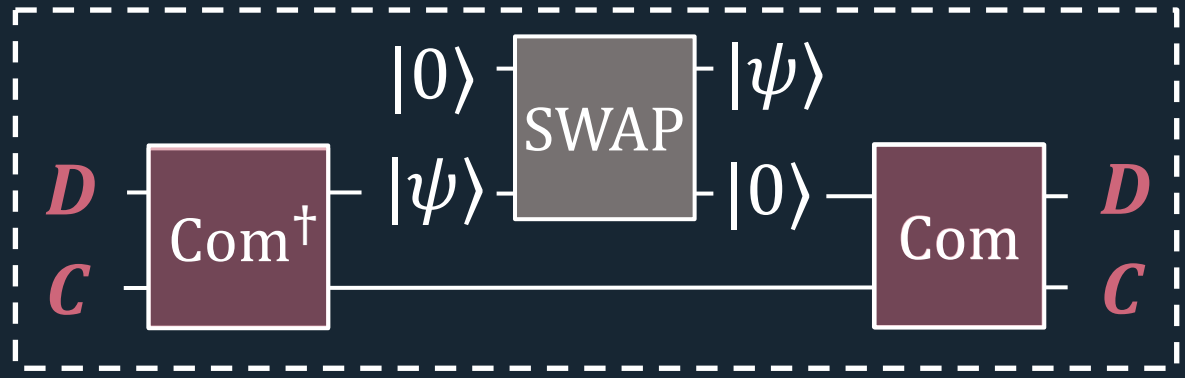
Challenger

1) Verify $\boldsymbol{C}, \boldsymbol{D}$.

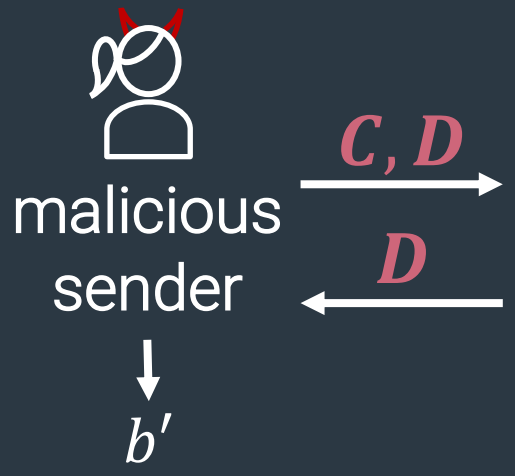
2) $b \leftarrow \{0,1\}$. If $b = 0$, swap $|\psi\rangle$ with junk.

Binding: $\Pr[b' = b] \leq 1/2 + \mathrm{negl}(\lambda)$

"swap $|\psi\rangle$ with junk" =



Our Definition: Swap Binding



$\boldsymbol{C}, \boldsymbol{D}$

$\boldsymbol{D}$

Challenger

1) Verify $\boldsymbol{C}, \boldsymbol{D}$.

2) $b \leftarrow \{0,1\}$. If $b = 0$, swap $|\psi\rangle$ with junk.

Binding: $\Pr[b' = b] \leq 1/2 + \mathrm{negl}(\lambda)$

Informally: $|\mathrm{com}_{\psi}\rangle_{\boldsymbol{CD}} \approx |\mathrm{com}_{0}\rangle_{\boldsymbol{CD}}$

(given only the $\boldsymbol{D}$ part)

Why this definition?

Swapping-Distinguishing Equivalence [AAS20]

These are **equivalent** for orthogonal $|x\rangle, |y\rangle$:

(1) Swapping $|x\rangle \leftrightarrow |y\rangle$

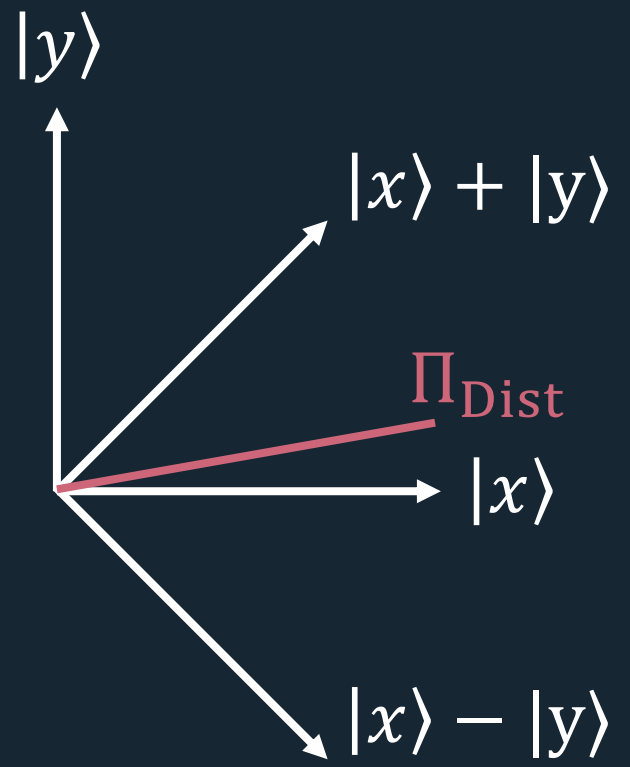
(2) Distinguishing $|x\rangle + |y\rangle$ vs $|x\rangle - |y\rangle$

Swapping-Distinguishing Equivalence [AAS20]

These are **equivalent** for orthogonal $|x\rangle, |y\rangle$:

(1) Swapping $|x\rangle \leftrightarrow |y\rangle$

(2) Distinguishing $|x\rangle + |y\rangle$ vs $|x\rangle - |y\rangle$

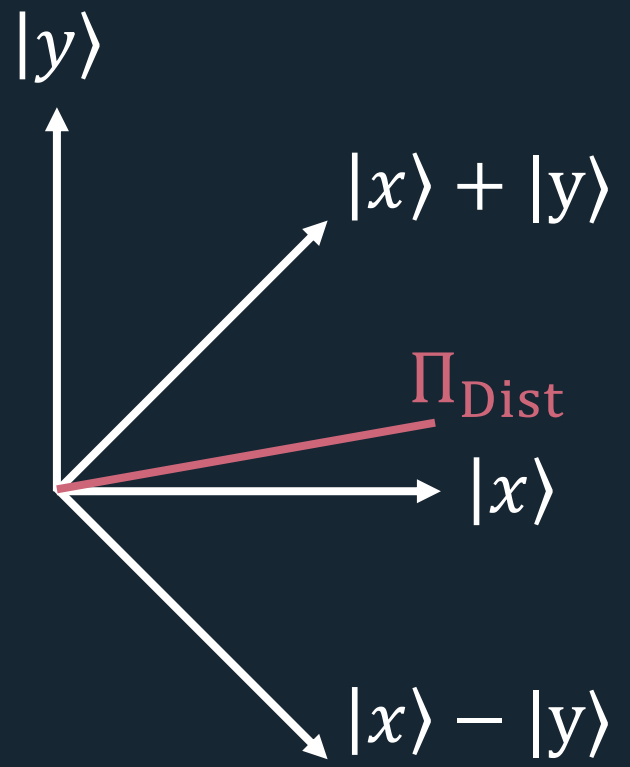


Swapping-Distinguishing Equivalence [AAS20]

These are **equivalent** for orthogonal $|x\rangle, |y\rangle$:

(1) Swapping $|x\rangle \leftrightarrow |y\rangle$

(2) Distinguishing $|x\rangle + |y\rangle$ vs $|x\rangle - |y\rangle$



Proof Sketch:

Π_{Dist} distinguishes $|x\rangle + |y\rangle$ vs $|x\rangle - |y\rangle$ iff $2\Pi_{\mathrm{Dist}} - \mathrm{Id}$ (reflection about Π_{Dist}) swaps $|x\rangle \leftrightarrow |y\rangle$.

Defining Binding for QSCs: Intuition

Suppose the sender honestly commits to a classical bit.

Defining Binding for QSCs: Intuition

Suppose the sender honestly commits to a classical bit.

Necessary: Sender can't swap $|\mathbf{com}_0\rangle_{\mathbf{CD}} \leftrightarrow |\mathbf{com}_1\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$).

Defining Binding for QSCs: Intuition

Suppose the sender honestly commits to a classical bit.

Necessary: Sender can't swap $|\mathrm{com}_0\rangle_{\mathbf{CD}} \leftrightarrow |\mathrm{com}_1\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$).

Equivalently, $|\mathrm{com}_+\rangle_{\mathbf{CD}} \approx |\mathrm{com}_-\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$).

$= \mathrm{Com}|+\rangle|0^\lambda\rangle$
$= |\mathrm{com}_0\rangle + |\mathrm{com}_1\rangle$

$= \mathrm{Com}|-\rangle|0^\lambda\rangle$
$= |\mathrm{com}_0\rangle - |\mathrm{com}_1\rangle$

Defining Binding for QSCs: Intuition

Suppose the sender honestly commits to a classical bit.

Necessary: Sender can't swap $|\mathrm{com}_0\rangle_{\mathbf{CD}} \leftrightarrow |\mathrm{com}_1\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$).

Equivalently, $|\mathrm{com}_+\rangle_{\mathbf{CD}} \approx |\mathrm{com}_-\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$).

$= \mathrm{Com}|+\rangle|0^\lambda\rangle$
$= |\mathrm{com}_0\rangle + |\mathrm{com}_1\rangle$

$= \mathrm{Com}|-\rangle|0^\lambda\rangle$
$= |\mathrm{com}_0\rangle - |\mathrm{com}_1\rangle$

This is (essentially) [Unruh16]'s collapse-binding definition, extended to quantum bit commitments.

Defining Binding for QSCs: Intuition

What if the sender honestly commits to an arbitrary state $|\psi\rangle$?

Defining Binding for QSCs: Intuition

What if the sender honestly commits to an arbitrary state $|\psi\rangle$?

Necessary: Sender can't swap $|\mathbf{com}_{\psi}\rangle_{\mathbf{CD}} \leftrightarrow |\mathbf{com}_{\psi^{\perp}}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

Defining Binding for QSCs: Intuition

What if the sender honestly commits to an arbitrary state $|\psi\rangle$?

Necessary: Sender can't swap $|\mathrm{com}_{\psi}\rangle_{\mathbf{CD}} \leftrightarrow |\mathrm{com}_{\psi^{\perp}}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

Equivalently, $|\mathrm{com}_{\psi+\psi^{\perp}}\rangle_{\mathbf{CD}} \approx |\mathrm{com}_{\psi-\psi^{\perp}}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

Defining Binding for QSCs: Intuition

What if the sender honestly commits to an arbitrary state $|\psi\rangle$?

Necessary: Sender can't swap $|\mathrm{com}_\psi\rangle_{\mathbf{CD}} \leftrightarrow |\mathrm{com}_{\psi^\perp}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

Equivalently, $|\mathrm{com}_{\psi+\psi^\perp}\rangle_{\mathbf{CD}} \approx |\mathrm{com}_{\psi-\psi^\perp}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

This is guaranteed by swap-binding, which says:

$|\mathrm{com}_\psi\rangle_{\mathbf{CD}} \approx |\mathrm{com}_0\rangle_{\mathbf{CD}}$ (given only $\boldsymbol{D}$)

Defining Binding for QSCs: Intuition

What if the sender honestly commits to an arbitrary state $|\psi\rangle$?

Necessary: Sender can't swap $|\mathrm{com}_\psi\rangle_{\mathbf{CD}} \leftrightarrow |\mathrm{com}_{\psi^\perp}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

Equivalently, $|\mathrm{com}_{\psi+\psi^\perp}\rangle_{\mathbf{CD}} \approx |\mathrm{com}_{\psi-\psi^\perp}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

This is guaranteed by swap-binding, which says:

$|\mathrm{com}_\psi\rangle_{\mathbf{CD}} \approx |\mathrm{com}_0\rangle_{\mathbf{CD}}$ (given only $\boldsymbol{D}$)

Swapping-distinguishing makes it possible to ***test*** if sender changes ψ.

Defining Binding for QSCs: Intuition

What if the sender honestly commits to an arbitrary state $|\psi\rangle$?

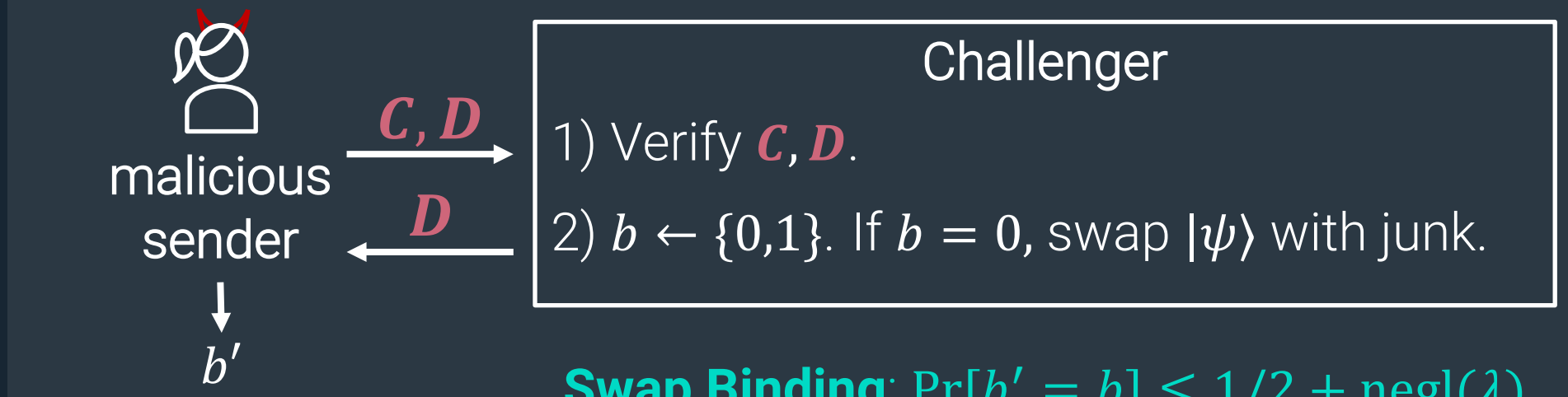
Necessary: Sender can't swap $|\mathrm{com}_\psi\rangle_{\mathbf{CD}} \leftrightarrow |\mathrm{com}_{\psi^\perp}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

Equivalently, $|\mathrm{com}_{\psi+\psi^\perp}\rangle_{\mathbf{CD}} \approx |\mathrm{com}_{\psi-\psi^\perp}\rangle_{\mathbf{CD}}$ (given only $\mathbf{D}$)

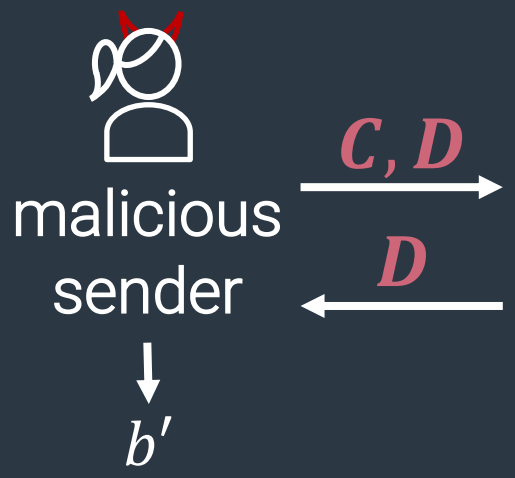
This is guaranteed by swap-binding, which says:

$$|\mathrm{com}_\psi\rangle_{\mathbf{CD}} \approx |\mathrm{com}_0\rangle_{\mathbf{CD}} \text{ (given only } \boldsymbol{D})$$

This paper: swap-binding captures security against *arbitrary malicious senders*.



Additional Properties



Challenger

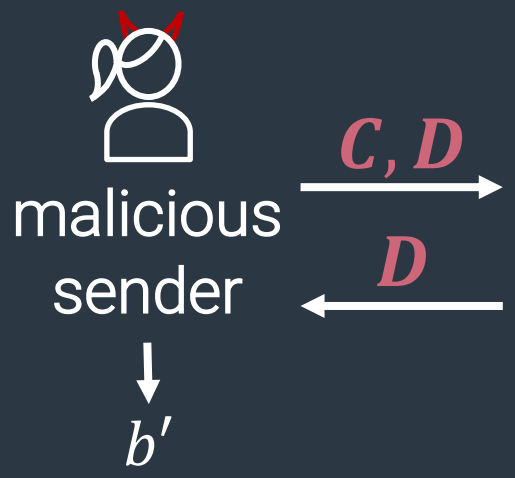
1) Verify C, D.

2) $b \leftarrow \{0,1\}$. If $b = 0$, swap $|\psi\rangle$ with junk.

Swap Binding: $\Pr[b' = b] \leq 1/2 + \mathrm{negl}(\lambda)$

Additional Properties

- handles entangled messages
- composable
- statistical or computational
- formalizes folklore (QSCs exist iff quantum bit commitments exist)



Challenger

1) Verify C, D.

2) $b \leftarrow \{0,1\}$. If $b = 0$, swap $|\psi\rangle$ with junk.

Swap Binding: $\Pr[b' = b] \leq 1/2 + \mathrm{negl}(\lambda)$

Additional Properties

Bonus: swap-binding is dual to hiding!

- swap-binding means D hides ψ
- hiding means C hides ψ (same game but adversary gets C)

Hiding-Binding Duality

- Primal scheme: $\boldsymbol{C}$ is the commitment and $\boldsymbol{D}$ is the opening.
- Dual scheme: $\boldsymbol{D}$ is the commitment and $\boldsymbol{C}$ is the opening.

Hiding-Binding Duality

- Primal scheme: C is the commitment and D is the opening.
- Dual scheme: D is the commitment and C is the opening.

Immediate consequence of hiding/binding definitions:

For $\mathrm{X} \in \{\mathbf{statistically}, \mathbf{computationally}\}$:

primal is X-binding $\Leftrightarrow$ dual is X-hiding

primal is X-hiding $\Leftrightarrow$ dual is X-binding

Plan for today

1) What does it mean to commit to a quantum state?

2) Can we ***succinctly*** commit to a quantum state?

3) Application: quantum succinct arguments

Succinct commitment to an n-qubit state

Succinct QSC:

- |commitment| < n qubits
- binding

Succinct commitment to an n-qubit state

Succinct QSC:
- |commitment| < n qubits
- binding

$\Longleftrightarrow$

Dual scheme:
- |opening| < n qubits
- hiding

Succinct commitment to an n-qubit state

Succinct QSC:
- |commitment| < n qubits
- binding

$\Longleftrightarrow$

Dual scheme: Encryption!
- |opening| < n qubits
- hiding

Dual is easy to construct: just need to *encrypt* a quantum state with a short classical key (opening).

Succinct commitment to an n-qubit state

Succinct QSC:
- |commitment| < n qubits
- binding

$\Longleftrightarrow$

Dual scheme: Encryption!
- |opening| < n qubits
- hiding

Dual is easy to construct: just need to *encrypt* a quantum state with a short classical key (opening).

Example: quantum one-time-pad $|\psi\rangle$ with pseudorandom string.

Succinct commitment to an n-qubit state

Succinct QSC:
- |commitment| < n qubits
- binding

$\Longleftrightarrow$

Dual scheme: Encryption!
- |opening| < n qubits
- hiding

Dual is easy to construct: just need to *encrypt* a quantum state with a short classical key (opening).

Example: quantum one-time-pad $|\psi\rangle$ with pseudorandom string.

assume PRG $\mathbf{G}$: $\{0,1\}^{n/2} \to \{0,1\}^{2n}$

$$\sum_k |k\rangle_C \otimes X^{\mathrm{G}_0(k)} Z^{\mathrm{G}_1(k)} |\psi\rangle_D$$

Succinct QSC: $\boldsymbol{C}$ (n/2 qubits) $\boldsymbol{D}$ (n qubits)

Succinct commitment to an n-qubit state

Succinct QSC:
- |commitment| < n qubits
- binding

$\Leftrightarrow$

Dual scheme: Encryption!
- |opening| < n qubits
- hiding

Dual is easy to construct: just need to *encrypt* a quantum state with a short classical key (opening).

Example: quantum one-time-pad $|\psi\rangle$ with pseudorandom string.

assume PRG G: $\{0,1\}^{n/2} \to \{0,1\}^{2n}$

$$\sum_k |k\rangle_C \otimes X^{\mathrm{G}_0(k)} Z^{\mathrm{G}_1(k)} |\psi\rangle_D$$

Note: classical succinct commitments from PRGs is *not* known!

Succinct commitment to an n-qubit state

Succinct QSC:
- |commitment| < n qubits
- binding

$\Longleftrightarrow$

Dual scheme: Encryption!
- |opening| < n qubits
- hiding

Dual is easy to construct: just need to *encrypt* a quantum state with a short classical key (opening).

In fact, one-way functions might not be necessary!

Succinct commitment to an n-qubit state

Succinct QSC:
- |commitment| < n qubits
- binding

$\Leftrightarrow$

Dual scheme: Encryption!
- |opening| < n qubits
- hiding

Dual is easy to construct: just need to *encrypt* a quantum state with a short classical key (opening).

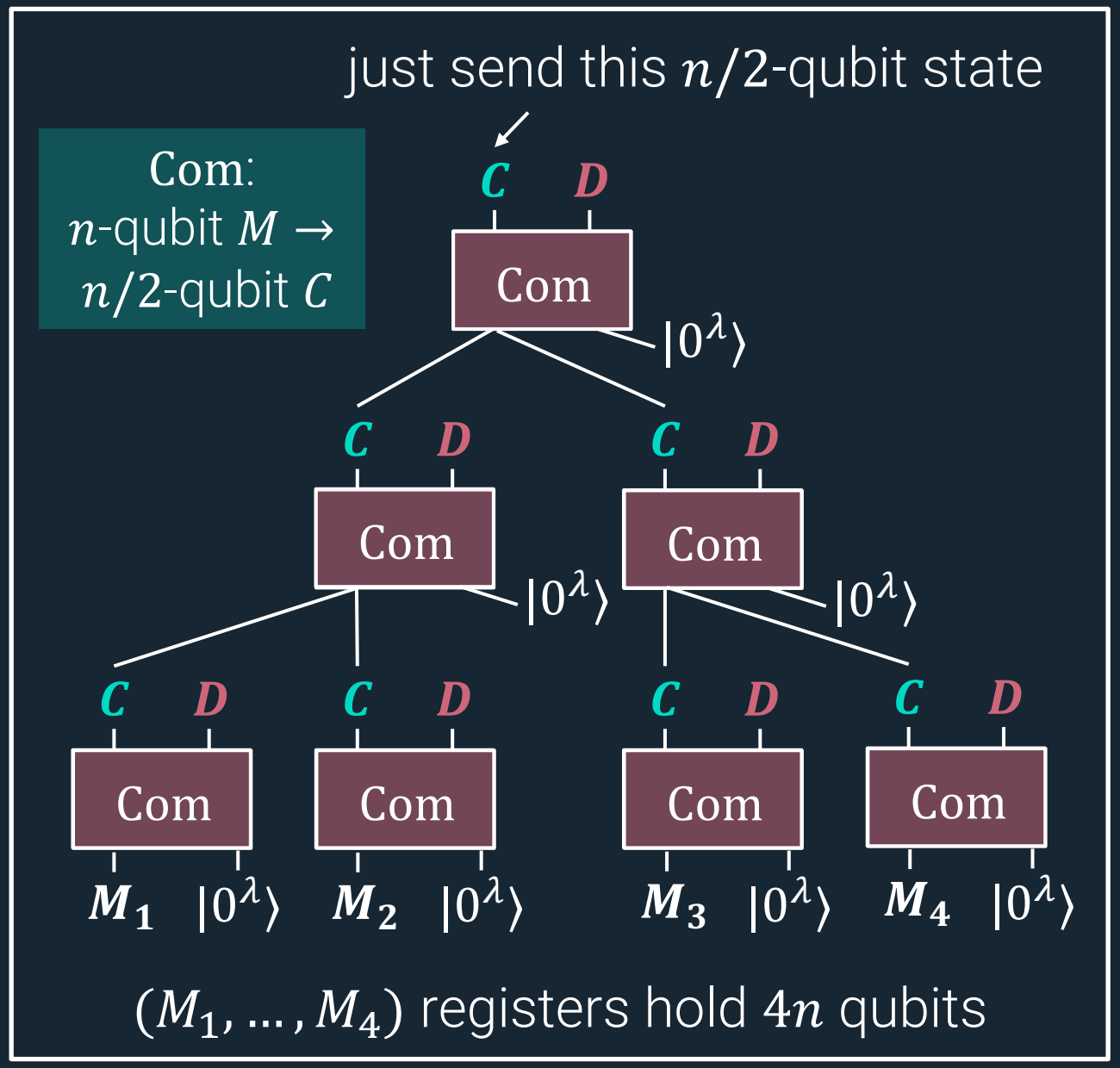
In fact, one-way functions might not be necessary! In the paper:

- This kind of encryption can be built from any pseudorandom unitary and (by [K21]) is potentially *weaker* than OWFs.

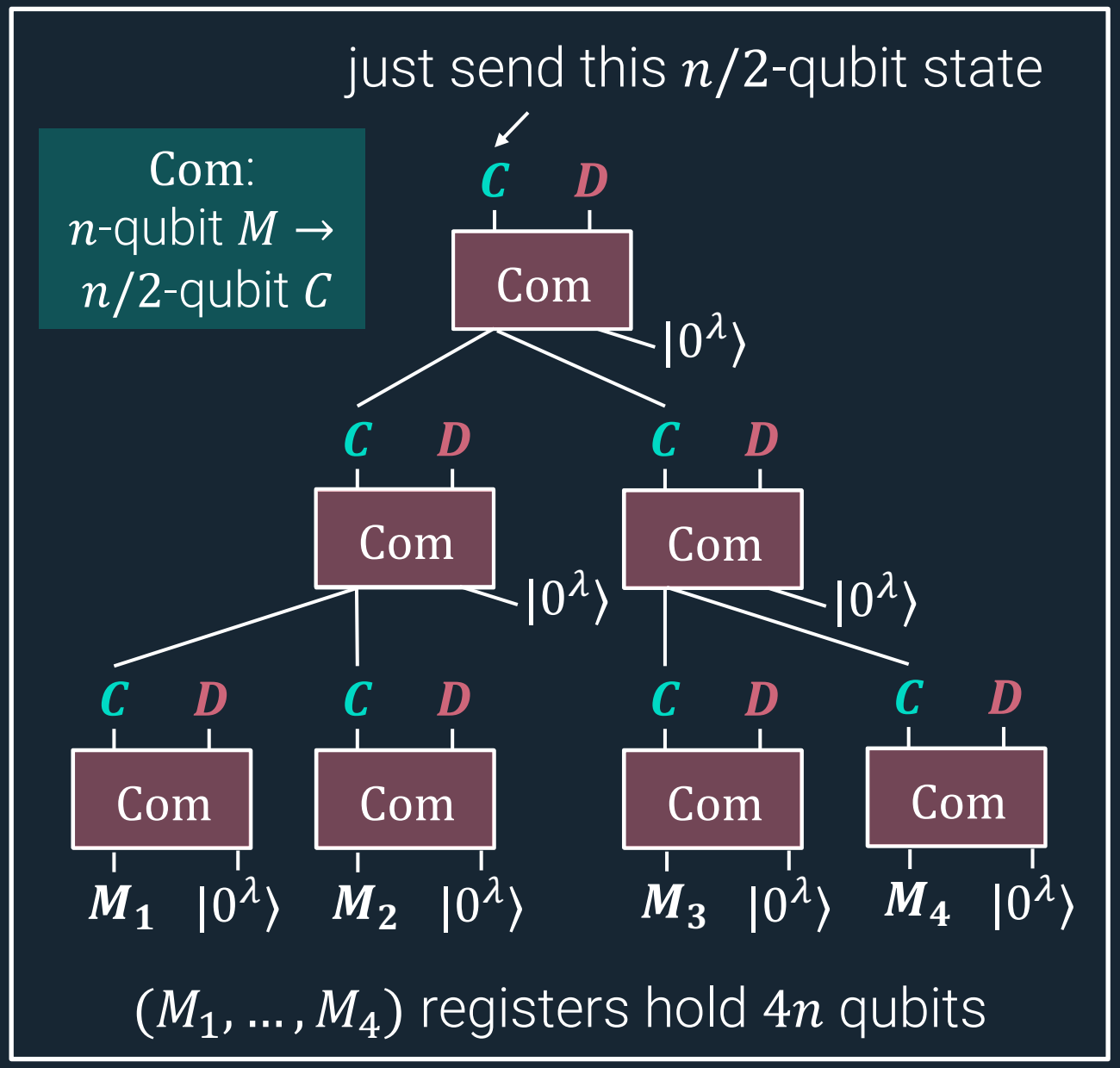
Useful property: succinct QSCs compose easily.

Useful property: succinct QSCs compose easily.

- Domain extension: 1-qubit compression → any compression (see paper)
- Merkle tree: succinct commitments with local openings (we'll see this next)

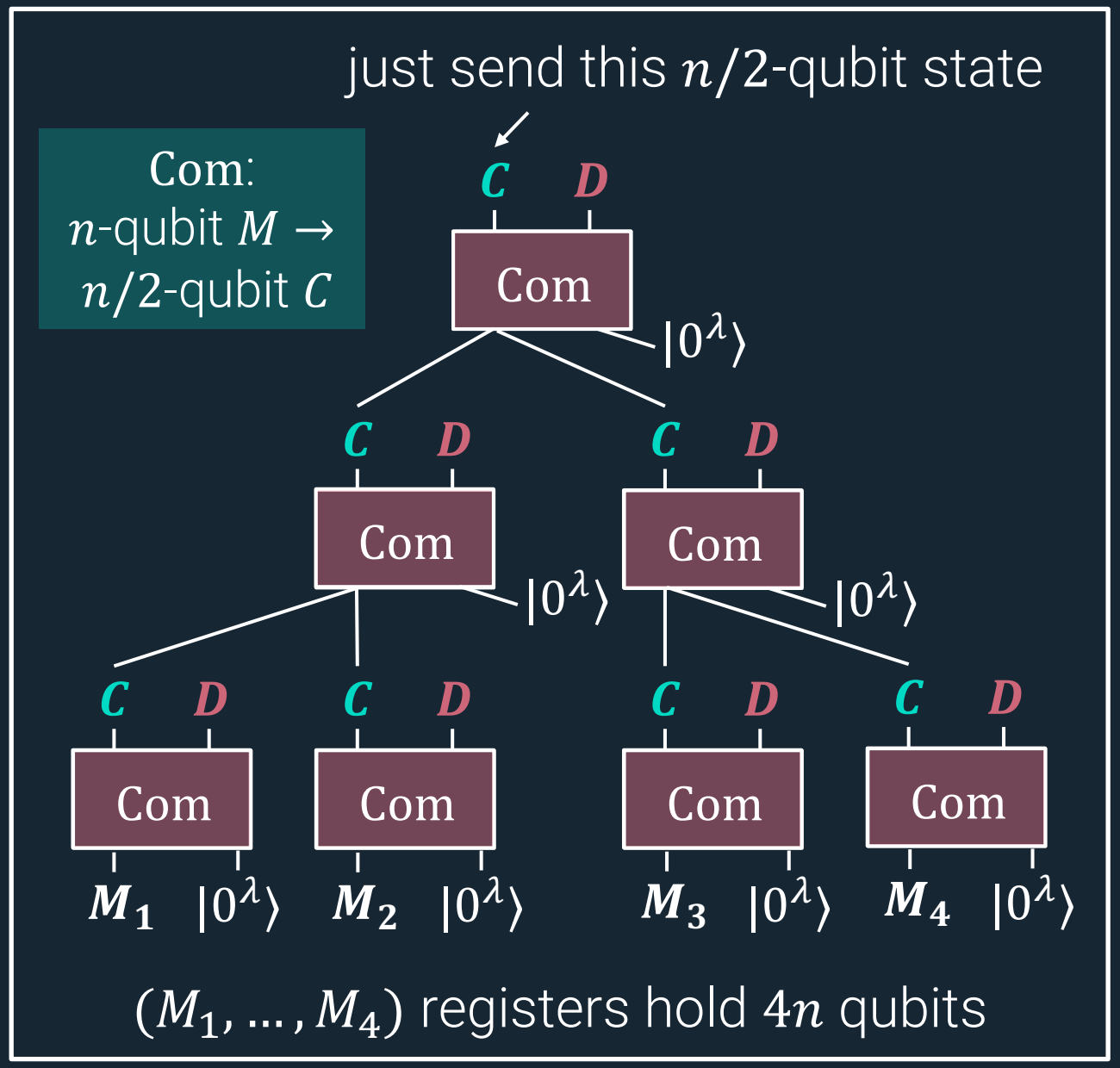


Merkle tree commitments



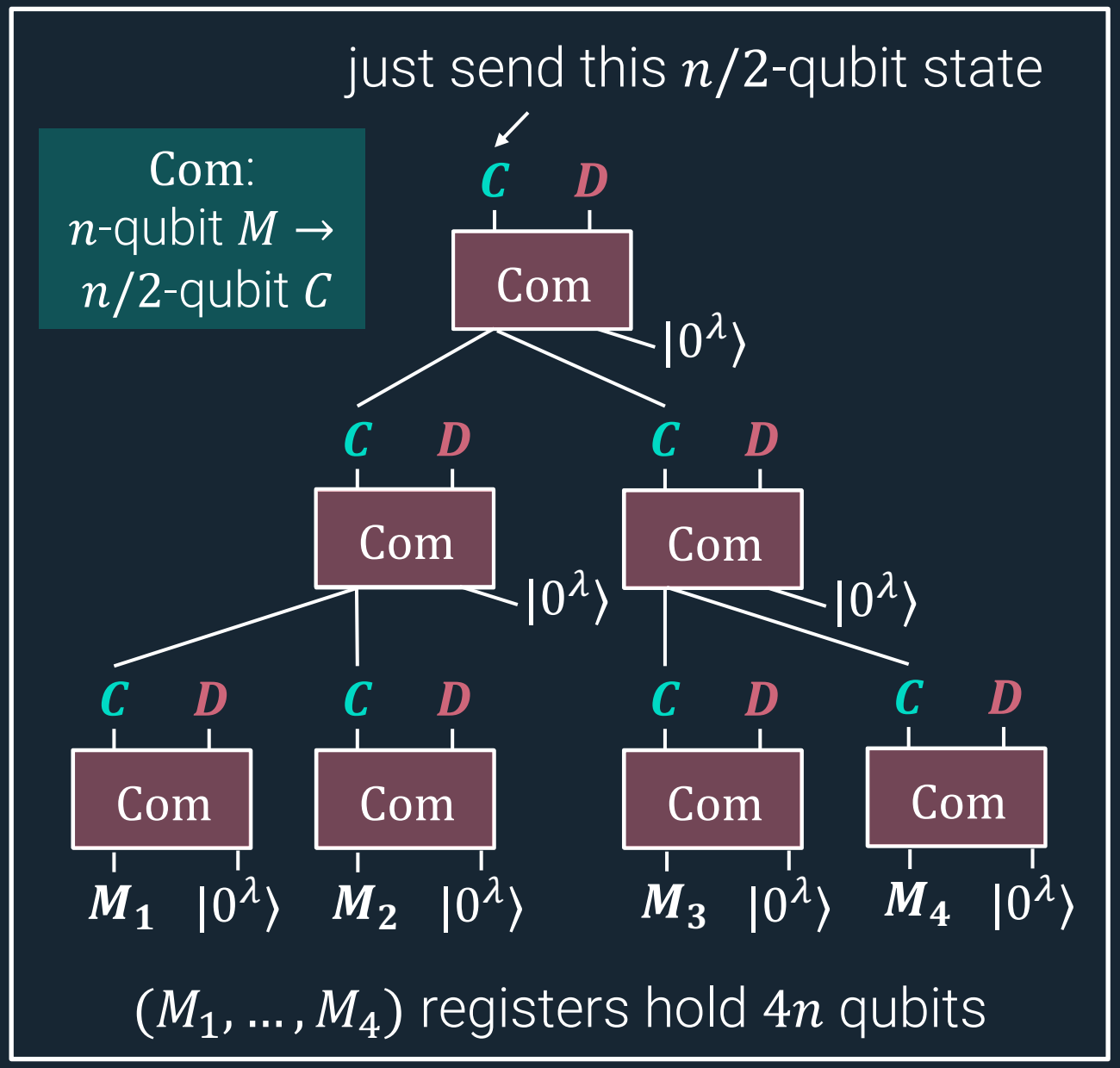
Merkle tree commitments

- since swap binding composes, this is swap-binding on every local opening.



Merkle tree commitments

- since swap binding composes, this is swap-binding on every local opening.
- get succinct commitments with local openings!



Merkle tree commitments

- since swap binding composes, this is swap-binding on every local opening.
- get succinct commitments with local openings!

Note: this is similar to a heuristic proposal of [Chen-Movassagh22]

Plan for today

1) What does it mean to commit to a quantum state?

2) Can we *succinctly* commit to a quantum state?

3) Application: quantum succinct arguments

Classically, tree commitments are **the key cryptographic component** of succinct arguments for NP [Kilian92].

Classically, tree commitments are **the key cryptographic component** of succinct arguments for NP [Kilian92].

Succinct Arguments [Kilian92,Micali94]

Claim: $x \in$ 3SAT

- "Succinct" = very short communication + verification
- "Argument" = efficient prover can't fool verifier

Classically, tree commitments are **the key cryptographic component** of succinct arguments for NP [Kilian92].

Succinct Arguments [Kilian92,Micali94]

Claim: $x \in$ 3SAT

- "Succinct" = very short communication + verification
- "Argument" = efficient prover can't fool verifier

Kilian's protocol: tree commit to a locally checkable proof π (aka PCP).

This work: quantum succinct arguments

This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

quantum tree commitments + quantum PCP → quantum succinct arguments

This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

quantum tree commitments + quantum PCP → quantum succinct arguments

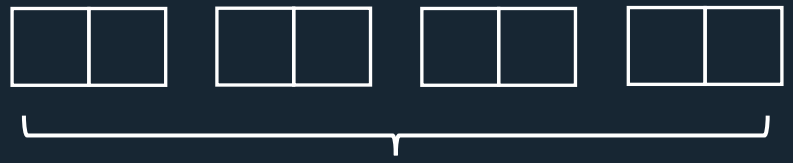
quantum PCP means quantum proof $|\pi\rangle$ that can be verified by checking a few qubits.

(includes classical PCPs!)

This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

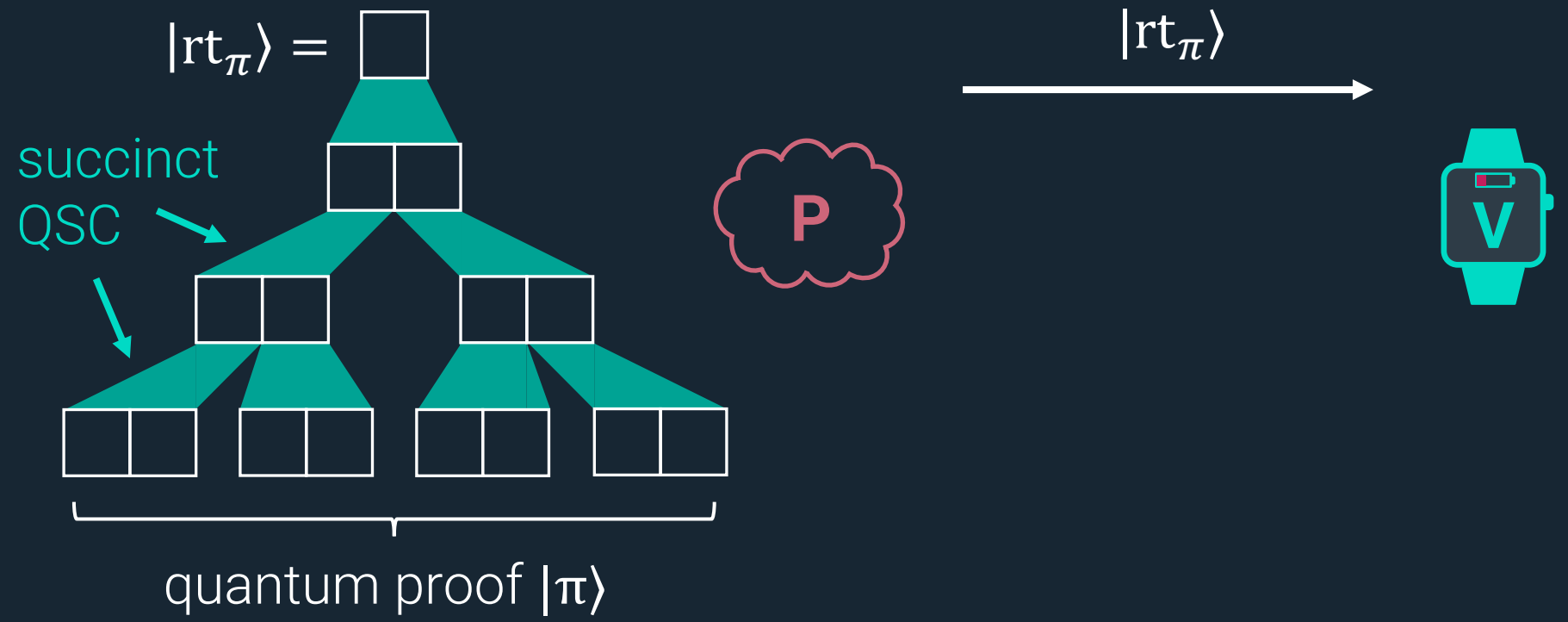
quantum tree commitments + quantum PCP → quantum succinct arguments



This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

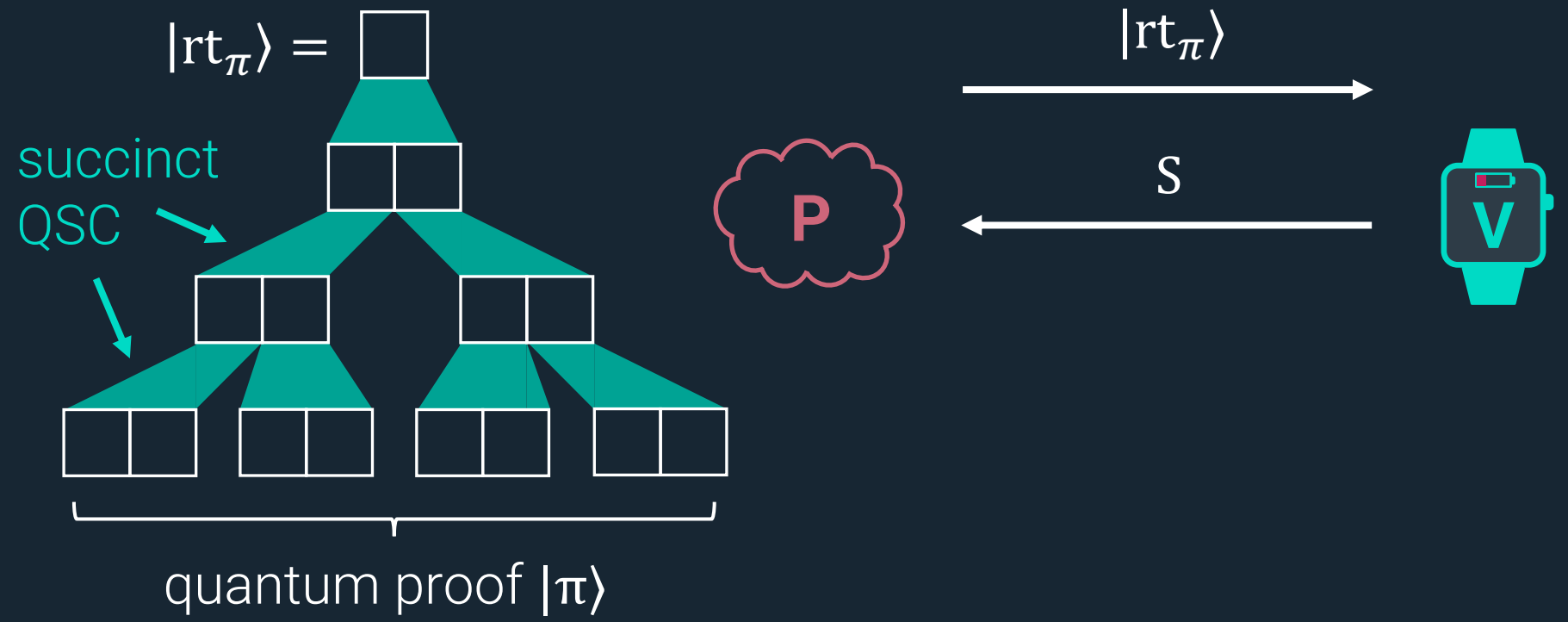
quantum tree commitments + quantum PCP → quantum succinct arguments



This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

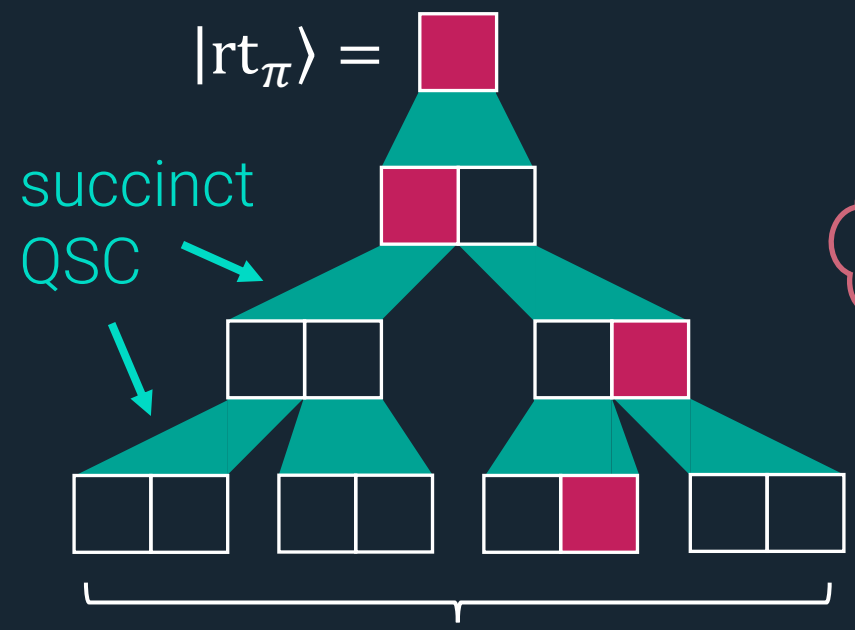
quantum tree commitments + quantum PCP → quantum succinct arguments

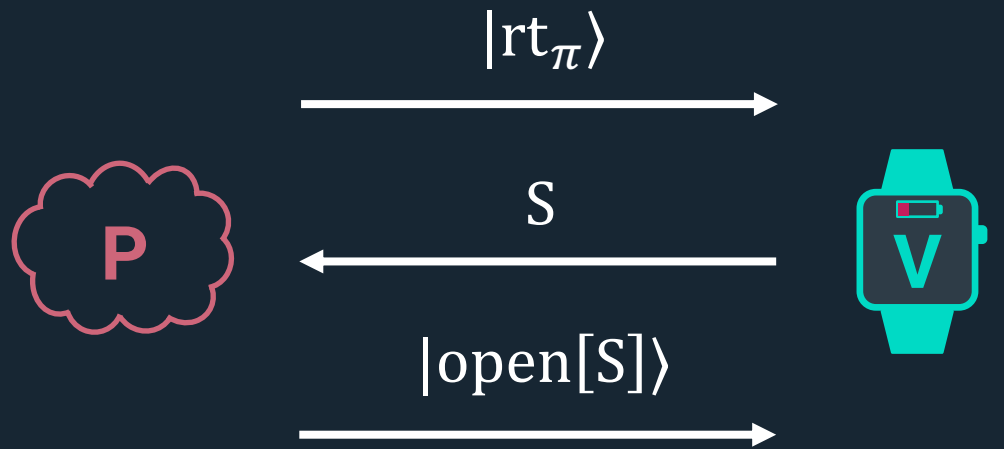


This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

quantum tree commitments + quantum PCP → quantum succinct arguments

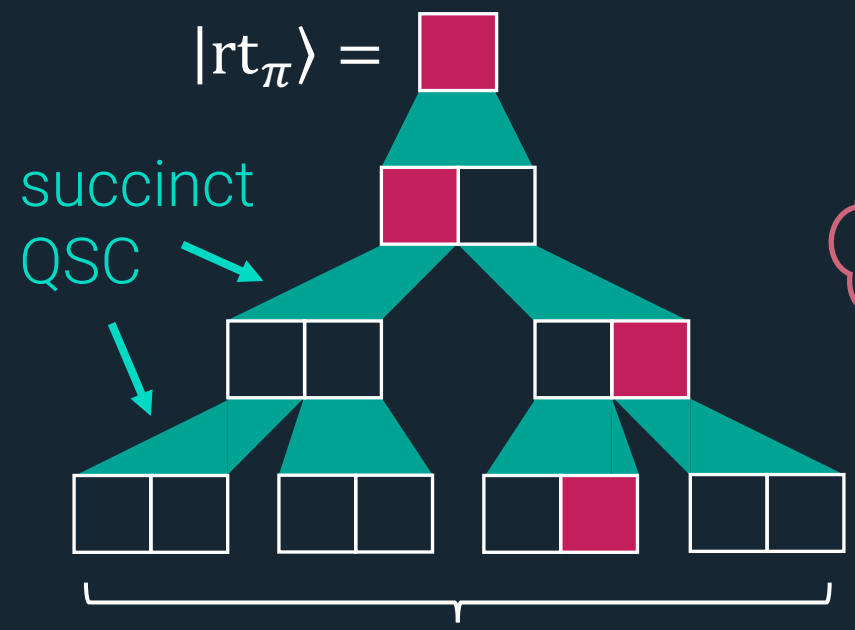


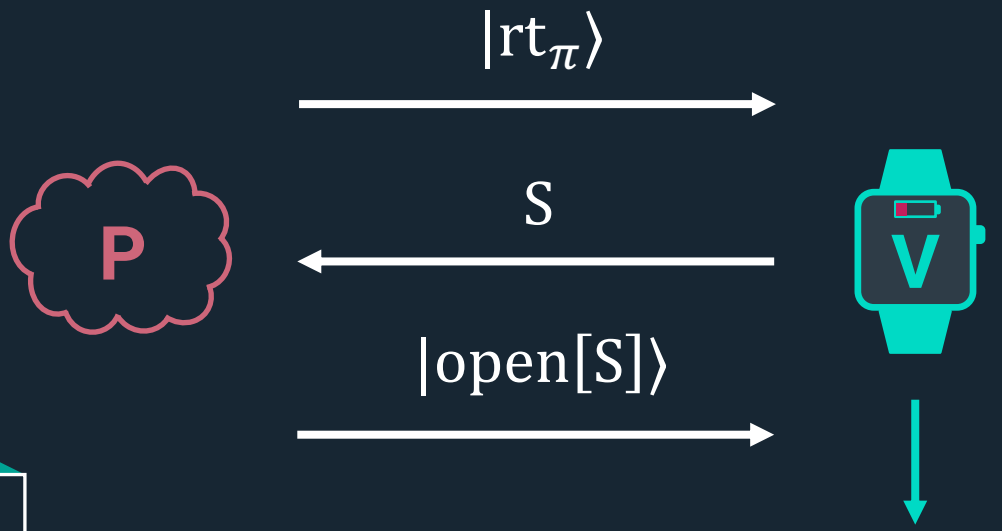


This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

quantum tree commitments + quantum PCP → quantum succinct arguments





1) Check if $|\mathbf{open}[S]\rangle$ is valid.

2) Apply $\mathbf{Com}^\dagger$ to reveal $|\pi[S]\rangle$ and run PCP verifier.

This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

quantum tree commitments + quantum PCP → quantum succinct arguments

Corollary: 3-msg succinct arguments for NP from less-than-OWF assumptions.

This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

quantum tree commitments + quantum PCP → quantum succinct arguments

Corollary: 3-msg succinct arguments for NP from less-than-OWF assumptions.

recall Kilian's classical protocol:

- assumes collision-resistant hash functions (CRHFs)
- needs 4 messages (extra message to send CHRF key)

This work: quantum succinct arguments

We prove a quantum analogue of [Kilian92]:

quantum tree commitments + quantum PCP → quantum succinct arguments

Corollary: 3-msg succinct arguments for NP from less-than-OWF assumptions.

recall Kilian's classical protocol:

- assumes collision-resistant hash functions (CRHFs)
- needs 4 messages (extra message to send CHRF key)

Corollary: 3-msg succinct arguments for QMA from less-than-OWF assumptions + quantum PCP conjecture.

We'll prove soundness by showing how to extract a *quantum PCP* from any (successful) malicious prover.

We'll prove soundness by showing how to extract a *quantum PCP* from any (successful) malicious prover.

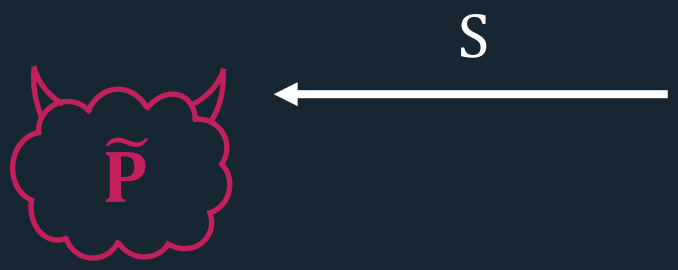
First: recall how this works for Kilian's *classical* protocol.

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{s}$.

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



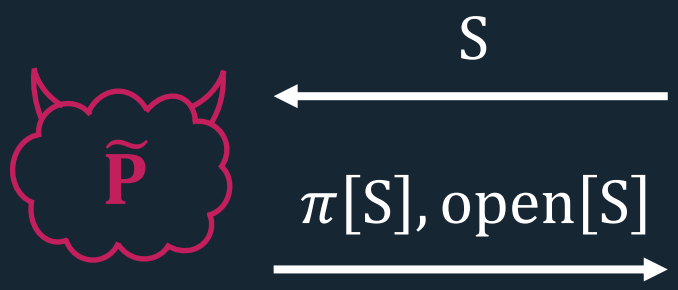
Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathbf{S}]$.

extracted proof

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



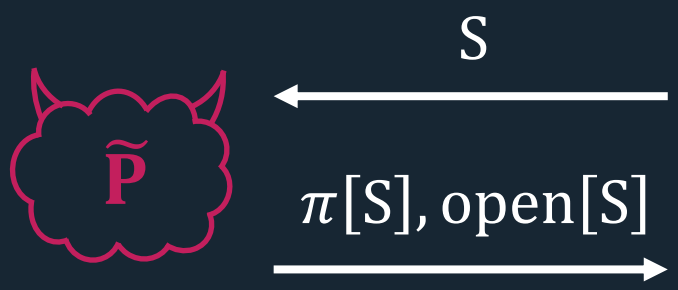
Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathrm{S}]$.

extracted proof

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



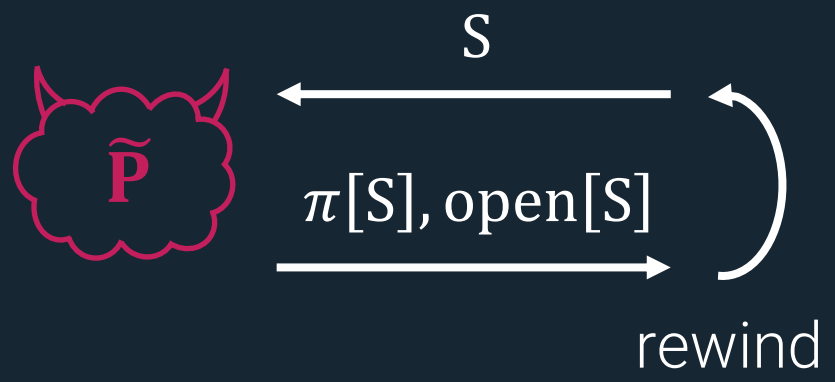
Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathrm{S}]$.

extracted proof

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



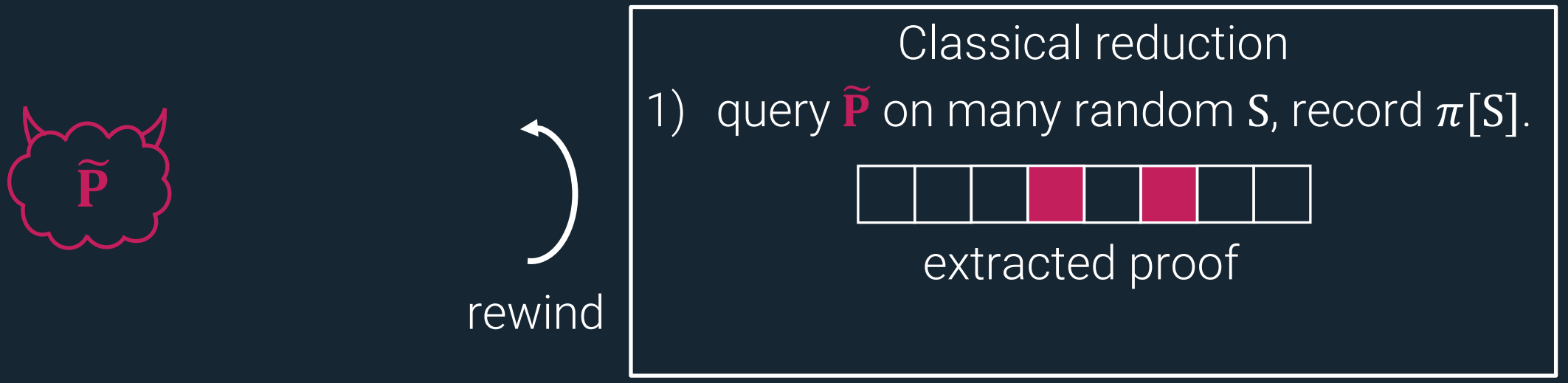
Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathrm{S}]$.

extracted proof

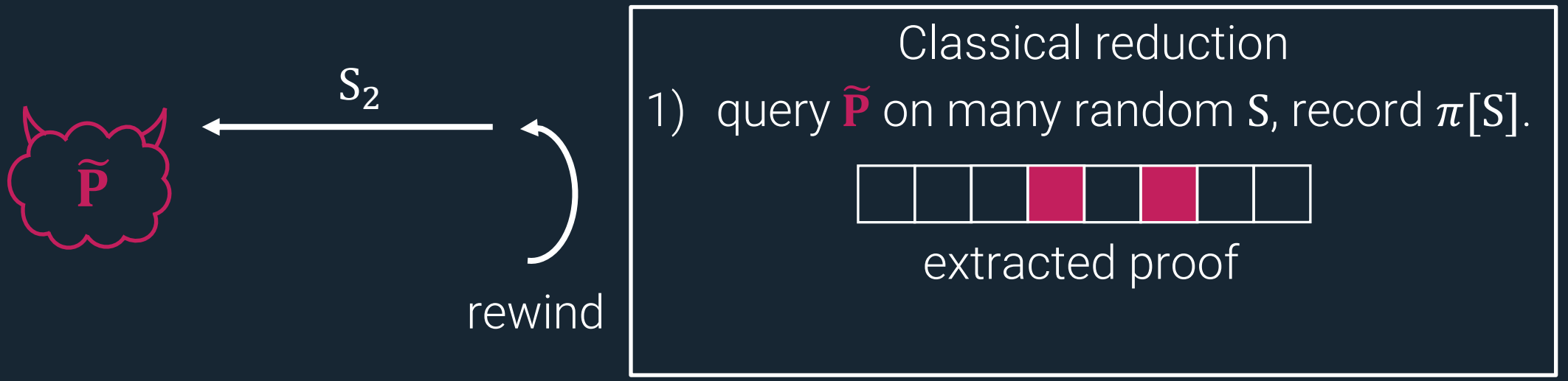
Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



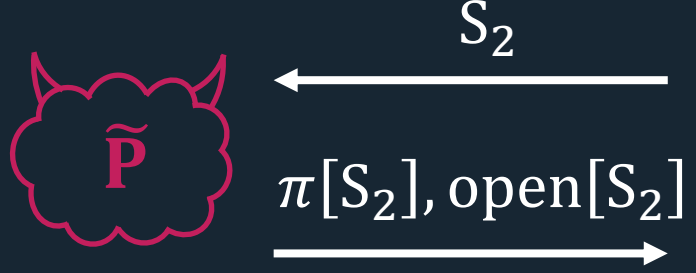
Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



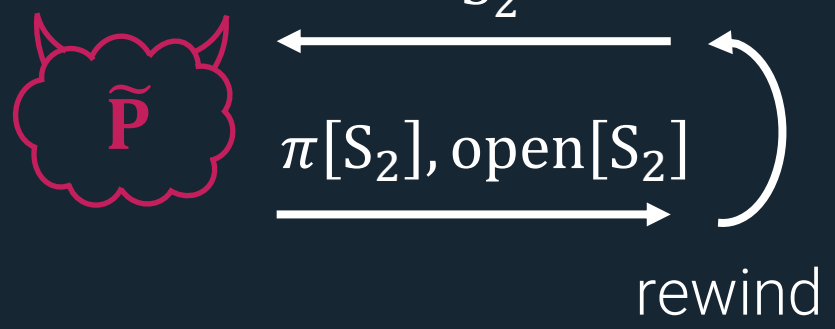
Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathbf{S}]$.

extracted proof

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathbf{S}]$.

extracted proof

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.

rewind

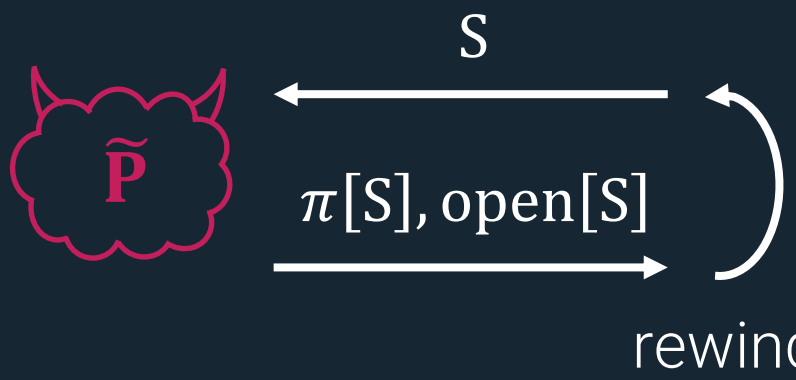
Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathbf{S}]$.

extracted proof

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{P}$'s answers to many random S.



Classical reduction

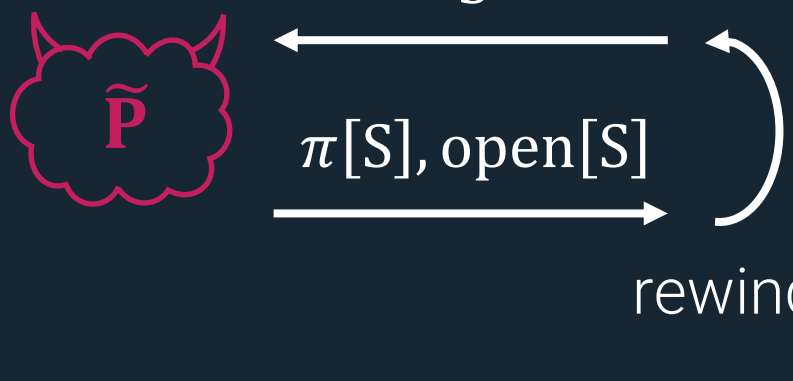
1) query $\widetilde{P}$ on many random S, record $\pi[S]$.

extracted proof

2) get convincing PCP *or* CRHF collision.

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathrm{S}]$.

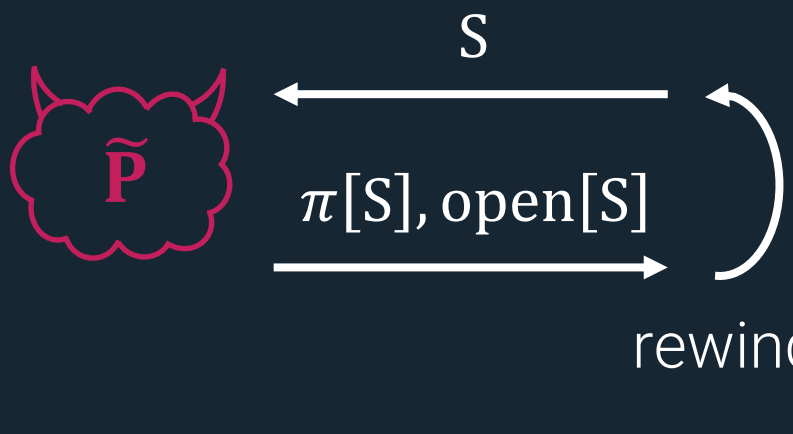
extracted proof

2) get convincing PCP *or* CRHF collision.

Quantum adversary: recording $\widetilde{\mathbf{P}}$'s answers is not straightforward because measurement can disturb $\widetilde{\mathbf{P}}$'s state (rendering it useless for future queries).

Soundness of Kilian's *classical* protocol

Classical adversary: record $\widetilde{\mathbf{P}}$'s answers to many random $\mathbf{S}$.



Classical reduction

1) query $\widetilde{\mathbf{P}}$ on many random $\mathbf{S}$, record $\pi[\mathbf{S}]$.

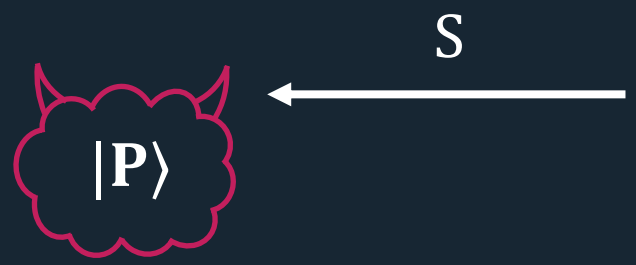
extracted proof

2) get convincing PCP *or* CRHF collision.

Quantum adversary: recording $\widetilde{\mathbf{P}}$'s answers is not straightforward because measurement can disturb $\widetilde{\mathbf{P}}$'s state (rendering it useless for future queries).

Recent work [CMSZ22]: there is a way for "disturbed" $\widetilde{\mathbf{P}}$ to answer later queries

Quantum soundness of Kilian's *classical* protocol [CMSZ22]

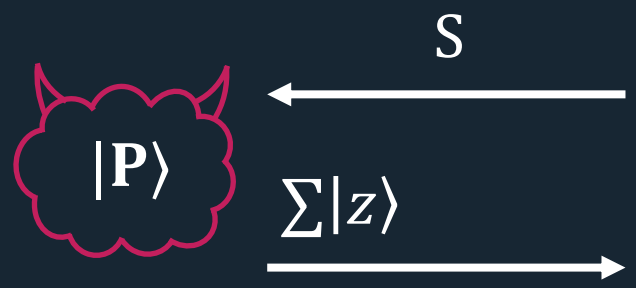


Reduction

Repeat:

1) Run $\tilde{\mathbf{P}} \to z$ in superposition, measure if response is valid.

Quantum soundness of Kilian's *classical* protocol [CMSZ22]

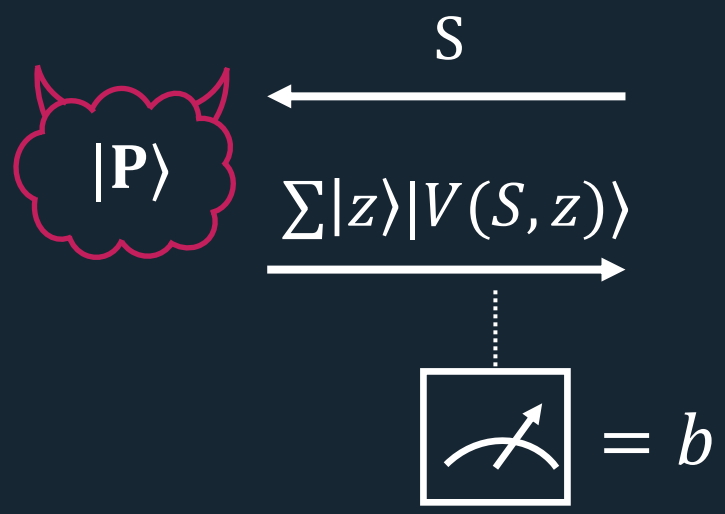


Reduction

Repeat:

1) Run $\tilde{\mathbf{P}} \to z$ in superposition, measure if response is valid.

Quantum soundness of Kilian's *classical* protocol [CMSZ22]

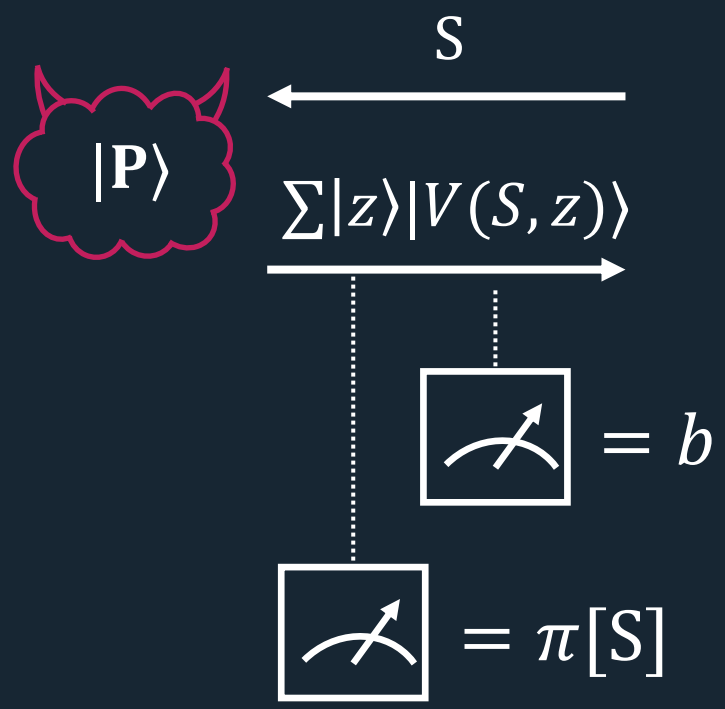


Reduction

Repeat:

1) Run $\widetilde{\mathbf{P}} \to z$ in superposition, measure if response is valid.

Quantum soundness of Kilian's *classical* protocol [CMSZ22]



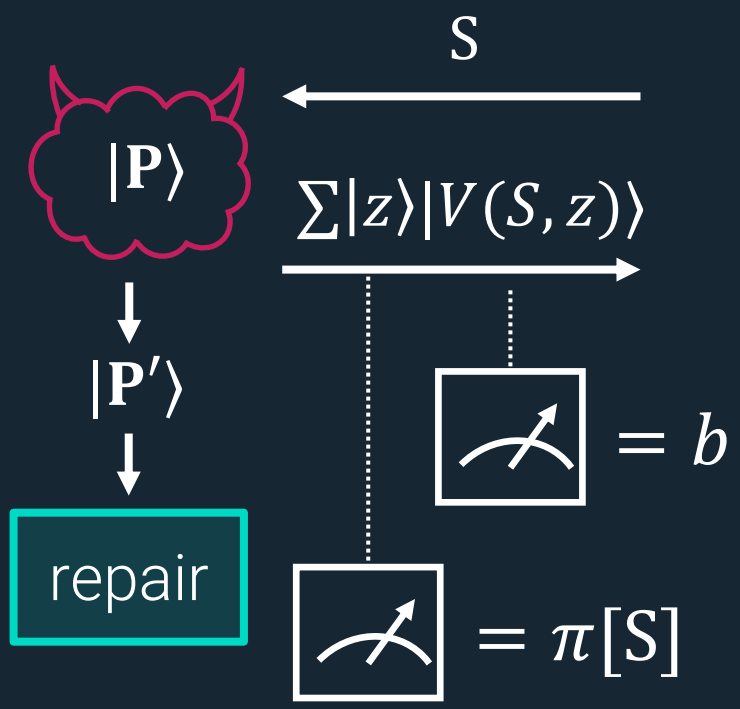
Reduction

Repeat:

1) Run $\widetilde{\mathbf{P}} \to z$ in superposition, measure if response is valid.

2) If valid, measure $\pi[\mathrm{S}]$.

Quantum soundness of Kilian's *classical* protocol [CMSZ22]



Reduction

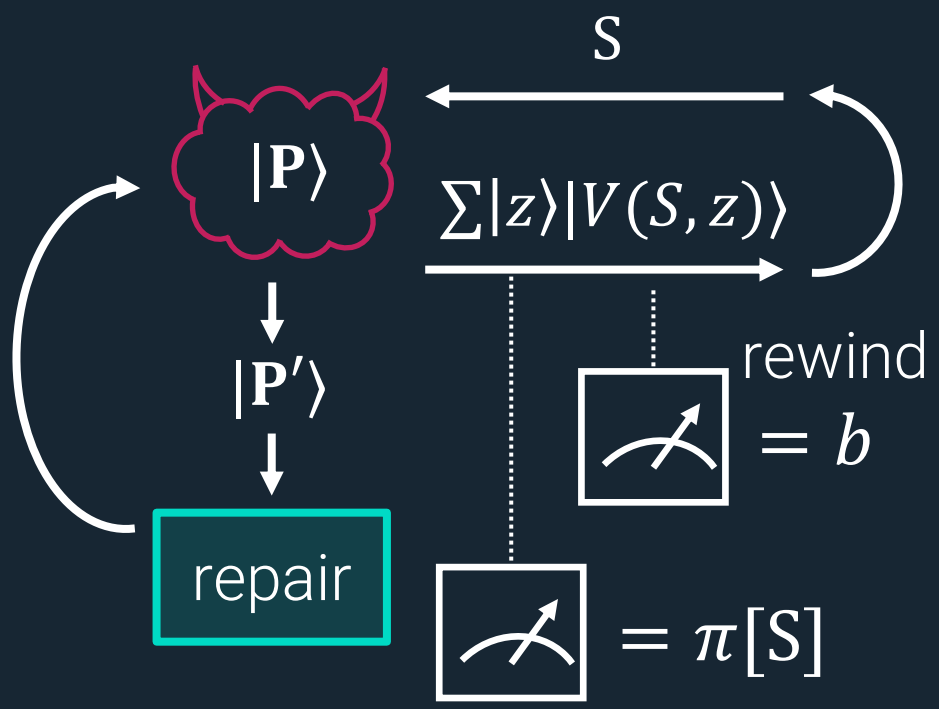
Repeat:

1) Run $\widetilde{\mathbf{P}} \to z$ in superposition, measure if response is valid.

2) If valid, measure $\pi[\mathrm{S}]$.

3) Run "repair" procedure.

Quantum soundness of Kilian's *classical* protocol [CMSZ22]



Reduction

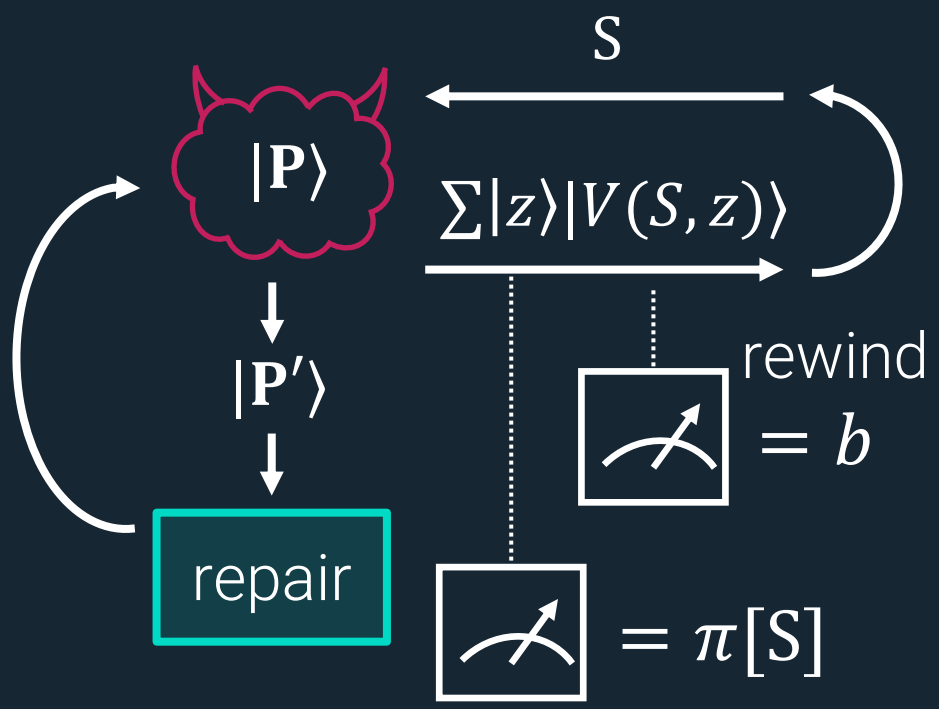
Repeat:

1) Run $\widetilde{\mathbf{P}} \to z$ in superposition, measure if response is valid.

2) If valid, measure $\pi[\mathrm{S}]$.

3) Run "repair" procedure.

Quantum soundness of Kilian's *classical* protocol [CMSZ22]



Reduction

Repeat:

1) Run $\widetilde{\mathbf{P}} \to z$ in superposition, measure if response is valid.

2) If valid, measure $\pi[\mathbf{S}]$.

3) Run "repair" procedure.

Main idea [Unruh16, CMSZ22]

- Collapse-binding → step 2 causes no detectable disturbance
- If step 2 doesn't disturb state, "repair" will restore prover's success prob.

Our setting: we need to extract a ***quantum proof***,
so measuring the response isn't enough.

Our setting: we need to extract a ***quantum proof***,
so measuring the response isn't enough.

But our definition suggests what to do instead!

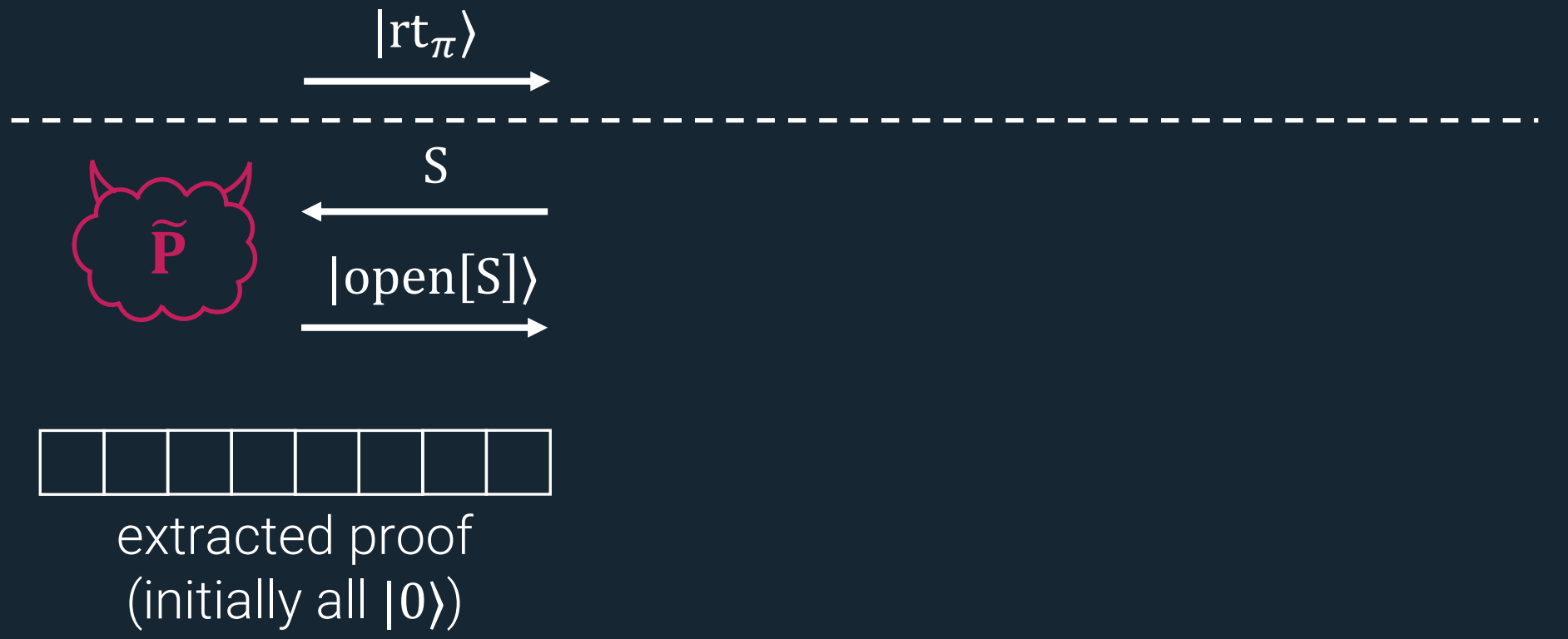
Swap-based rewinding: on each accepting response, swap out message onto external register

Swap-based rewinding: on each accepting response, swap out message onto external register

The hope: eventually, external registers contain quantum PCP.

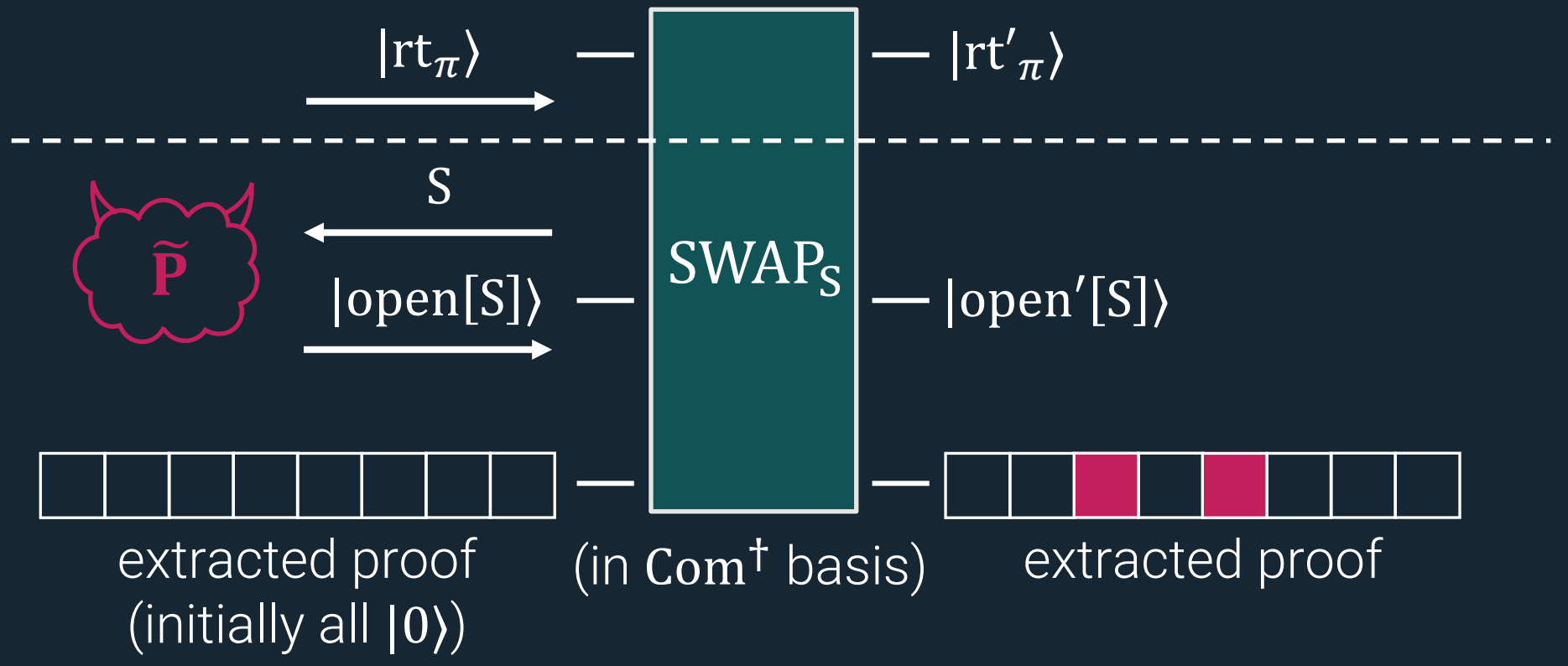
Swap-based rewinding: on each accepting response, swap out message onto external register

The hope: eventually, external registers contain quantum PCP.

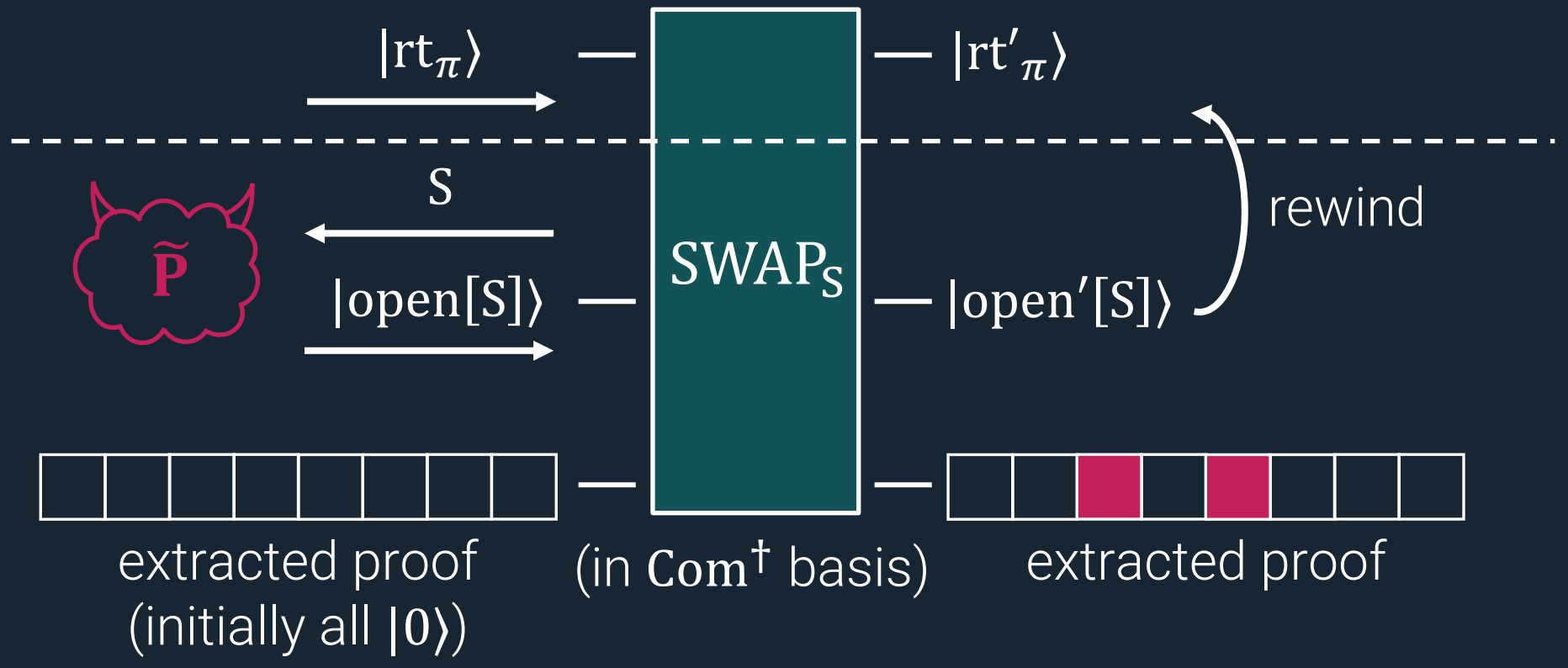


Swap-based rewinding: on each accepting response, swap out message onto external register

The hope: eventually, external registers contain quantum PCP.

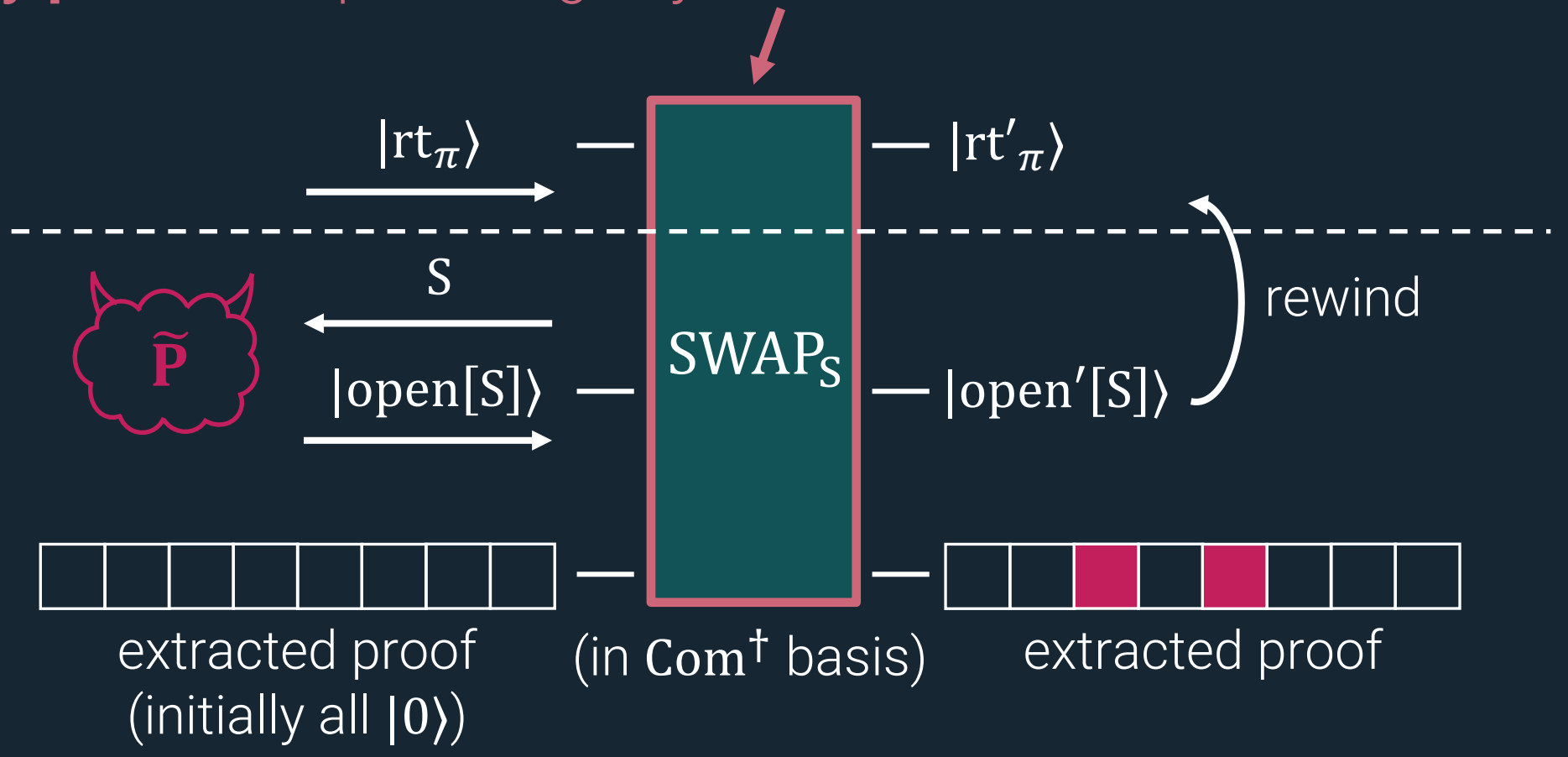


Swap-based rewinding: on each accepting response, swap out message onto external register



Swap-based rewinding: on each accepting response, swap out message onto external register

Key point: swap-binding says this is undetectable!



This approach *nearly* works.

This approach *nearly* works.

Just one problem...

This approach *nearly* works.

Just one problem...

[CMSZ22] repair requires that the reduction/extractor:

(1) **can** verify decommitments

(2) **can't** break binding

This approach *nearly* works.

Just one problem...

[CMSZ22] repair requires that the reduction/extractor:

(1) **can** verify decommitments

(2) **can't** break binding

For quantum commitments (1) and (2) are incompatible!

This approach *nearly* works.

Just one problem...

[CMSZ22] repair requires that the reduction/extractor:

(1) **can** verify decommitments (extractor must have $\mathbf{C}$)

(2) **can't** break binding (extractor must not have $\mathbf{C}$)

For quantum commitments (1) and (2) are incompatible!

This approach *nearly* works.

Just one problem...

[CMSZ22] repair requires that the reduction/extractor:

(1) **can** verify decommitments (extractor must have $\mathbf{C}$)

(2) **can't** break binding (extractor must not have $\mathbf{C}$)

For quantum commitments (1) and (2) are incompatible!

Note: This is an issue even if we're only extracting classical information from quantum commitments.

This approach *nearly* works.

Just one problem...

[CMSZ22] repair requires that the reduction/extractor:

(1) **can** verify decommitments (extractor must have $\mathbf{C}$)

(2) **can't** break binding (extractor must not have $\mathbf{C}$)

Our solution (see paper)

- Main technical step: Prove that swap-binding remains hard even if the adversary is given an oracle to verify commitments + act on the message
- Show that this oracle suffices to implement CMSZ-style rewinding.

Summary

Today:

- binding means the committed state is **erased**

Summary

Today:

- binding means the committed state is **erased**
- definition makes it easy to construct succinct QSCs

Summary

Today:

- binding means the committed state is **erased**
- definition makes it easy to construct succinct QSCs
- quantum succinct arguments via swap-based rewinding

Summary

Today:

- binding means the committed state is **erased**
- definition makes it easy to construct succinct QSCs
- quantum succinct arguments via swap-based rewinding

See paper:

- quantum sigma protocols for QMA from any hiding-binding QSC

Summary

Today:

- binding means the committed state is **erased**
- definition makes it easy to construct succinct QSCs
- quantum succinct arguments via swap-based rewinding

See paper:

- quantum sigma protocols for QMA from any hiding-binding QSC
- hiding-binding duality for quantum commitments to *classical* messages

Summary

Today:

- binding means the committed state is **erased**
- definition makes it easy to construct succinct QSCs
- quantum succinct arguments via swap-based rewinding

See paper:

- quantum sigma protocols for QMA from any hiding-binding QSC
- hiding-binding duality for quantum commitments to *classical* messages

Future Directions:

- do pseudorandom states imply succinct QSCs?

Summary

Today:

- binding means the committed state is **erased**
- definition makes it easy to construct succinct QSCs
- quantum succinct arguments via swap-based rewinding

See paper:

- quantum sigma protocols for QMA from any hiding-binding QSC
- hiding-binding duality for quantum commitments to *classical* messages

Future Directions:

- do pseudorandom states imply succinct QSCs?
- classical communication QSCs?

Summary

Today:

- binding means the committed state is **erased**
- definition makes it easy to construct succinct QSCs
- quantum succinct arguments via swap-based rewinding

See paper:

- quantum sigma protocols for QMA from any hiding-binding QSC
- hiding-binding duality for quantum commitments to *classical* messages

Future Directions:

- do pseudorandom states imply succinct QSCs?
- classical communication QSCs?
- simpler techniques for rewinding quantum protocols?

Thank You!

Questions?