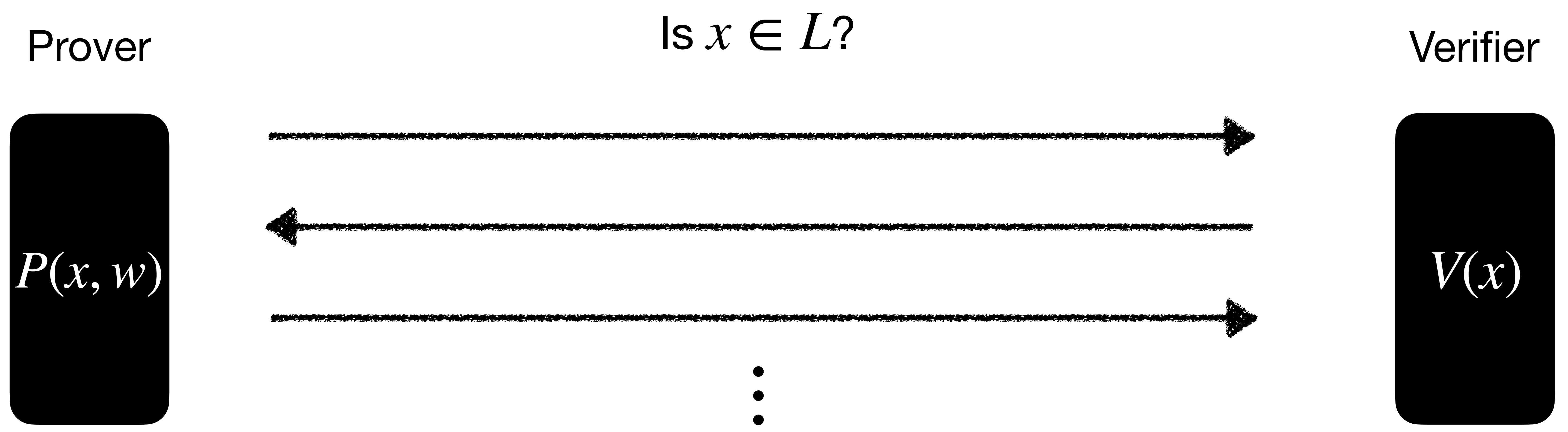
Quantum Rewinding for IOP-Based Succinct Arguments

Ziyi Guan

Joint work with Alessandro Chiesa, Marcel Dall'Agnol, Zijing Di, and Nick Spooner

What are succinct arguments?

Interactive proofs



Completeness: $\forall x \in L, \Pr\left[\langle P(x,w), V(x)\rangle = 1\right] = 1$

Soundness: $\forall x \notin L$ and adversary $\tilde{P}$, $\Pr\left[\langle \tilde{P}, V(x)\rangle = 1\right] \leq \epsilon$

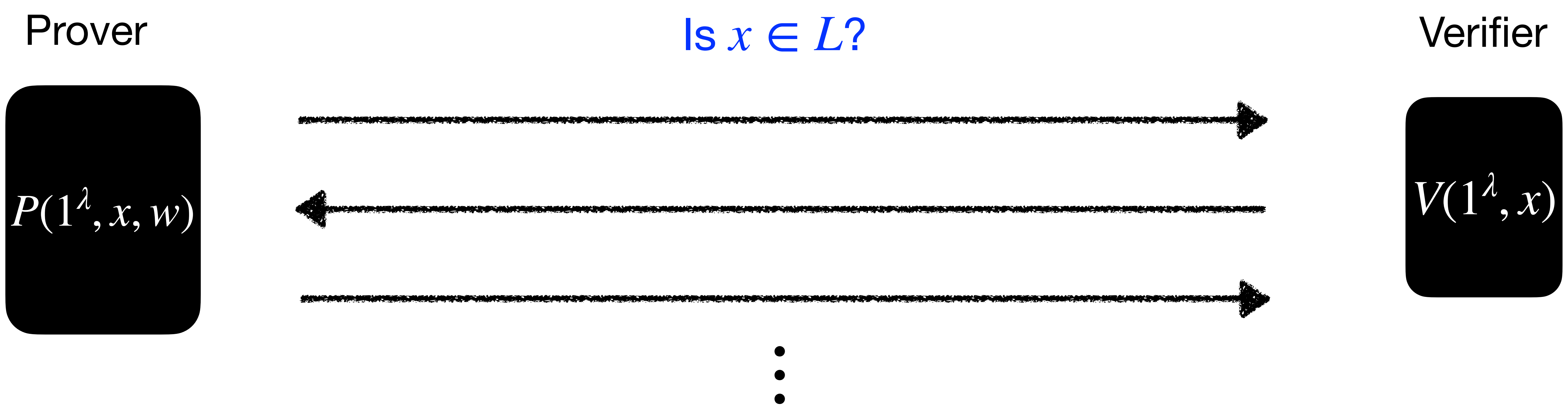
Target metric: **COMMUNICATION COMPLEXITY**

Limitation: NP-complete languages do not have IPs with **CC** $\ll |w|$

[GH97]: IP[CC] $\subseteq$ BPTIME[2^{CC}]

Interactive arguments

Interactive proofs with computational soundness



Computational soundness: $\forall\, x \notin L$ and t_{ARG}-time adversary $\tilde{P}$, $\Pr\left[\langle \tilde{P}, V(x)\rangle = 1\right] \leq \epsilon_{\mathsf{ARG}}(t_{\mathsf{ARG}})$

AMAZING: $\exists$ interactive arguments for NP with **CC** $\ll |w|$ (given basic cryptography)

Today's protagonist:
Succinct Interactive Arguments

$\mathsf{CC} \ll |w|$

Why study succinct interactive arguments?

$\mathrm{time}(V) \ll |w|$

They exist based on simple crypto assumptions...

... so they play a role in numerous cryptotheory results.

zero-knowledge with non-black-box simulation

malicious MPC

...

They are a stepping stone for SNARGs, which have numerous real-world applications.

Succinct

RISC ZERO

Aztec

VALIDA

Irreducible

STARKWARE

polygon

NEXUS

Ligero

Matter Labs

...

Today: only soundness
Knowledge soundness similar

Roadmap

[Kilian92]

Kilian's protocol:
PCP + VC → ARG

Classical Security [CDGSY24]

Post-quantum Security [CMSZ21]

Challenge for post-quantum analyses in standard model:
Quantum rewinding barrier
No-cloning theorem

Prior work

This work

[BCS16;CDGS23]

IBCS protocol:
IOP + VC → ARG

Classical Security [CDGS23,CGKY25]

Post-quantum Security

$\Longrightarrow$ **Best** post-quantum secure succinct arguments in the standard model (no oracles)

Another post-quantum security approach

[CMS19]

Micali/BCS in the QROM
PCP/IOP + VC + Fiat-Shamir → SNARG

Side information

Straightline extraction (no rewinding)

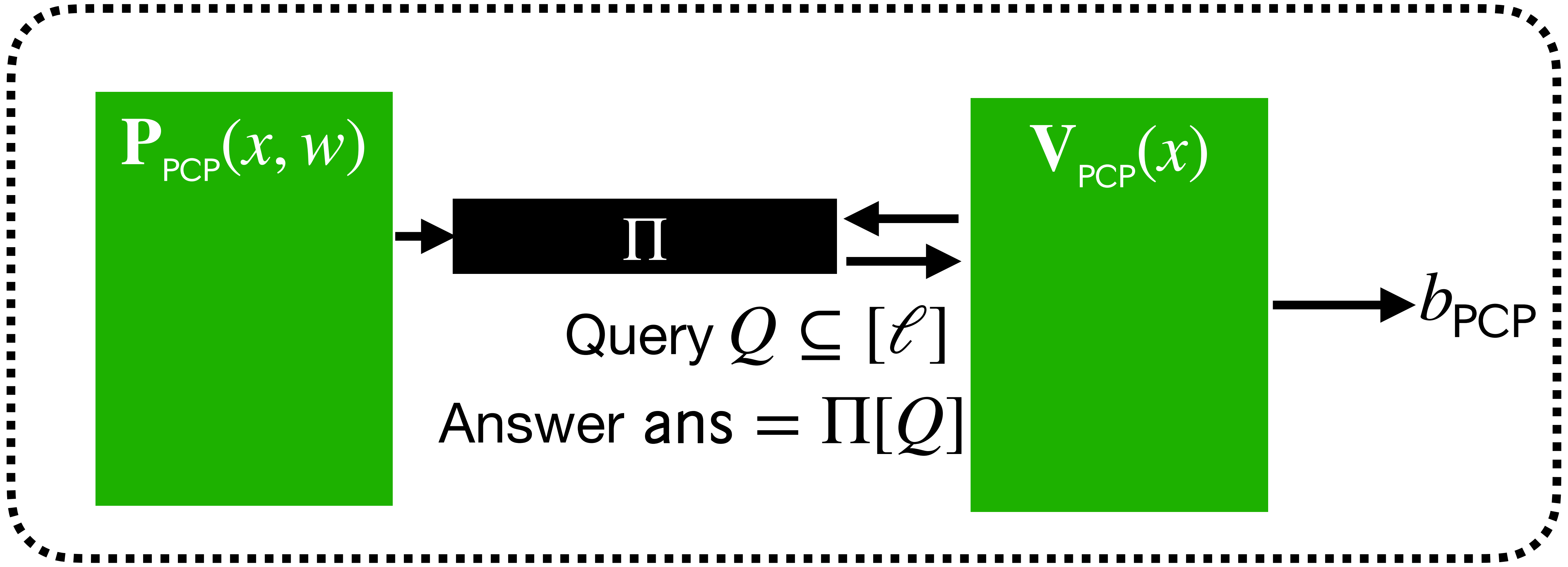
Idealized model

Warm-up: Kilian's protocol
The first and simplest succinct argument

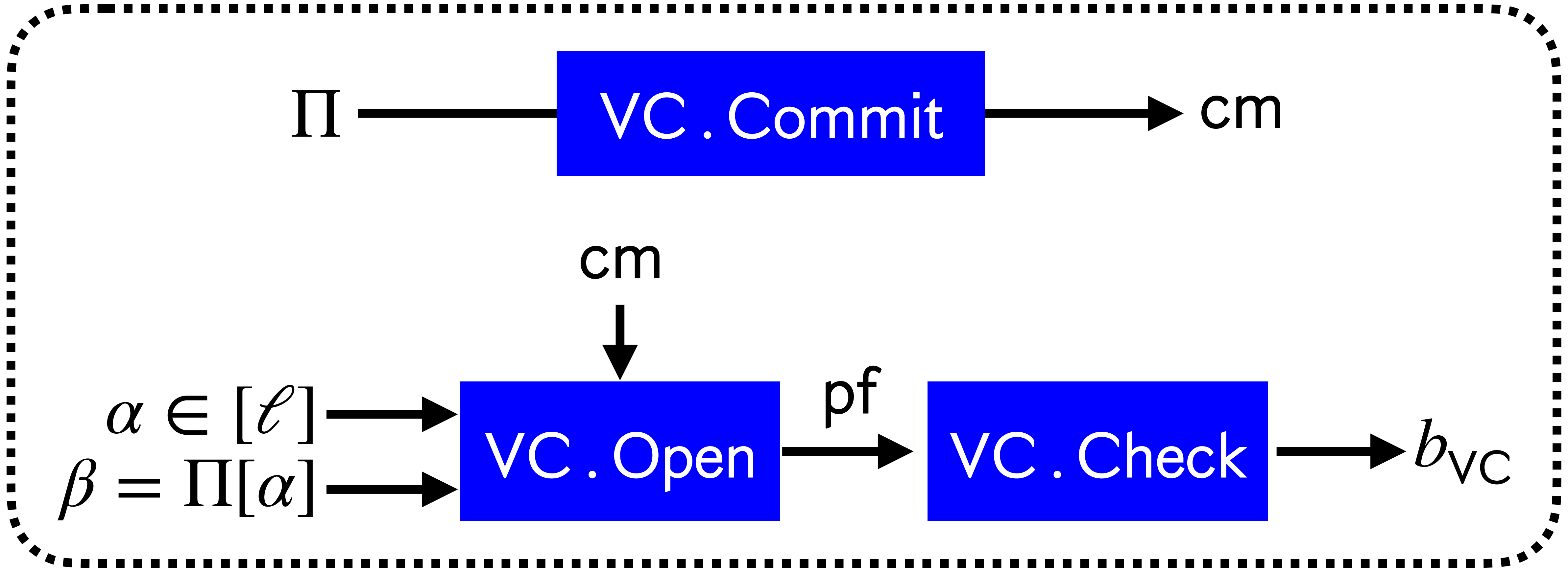
[Kilian92]

How to construct succinct arguments?

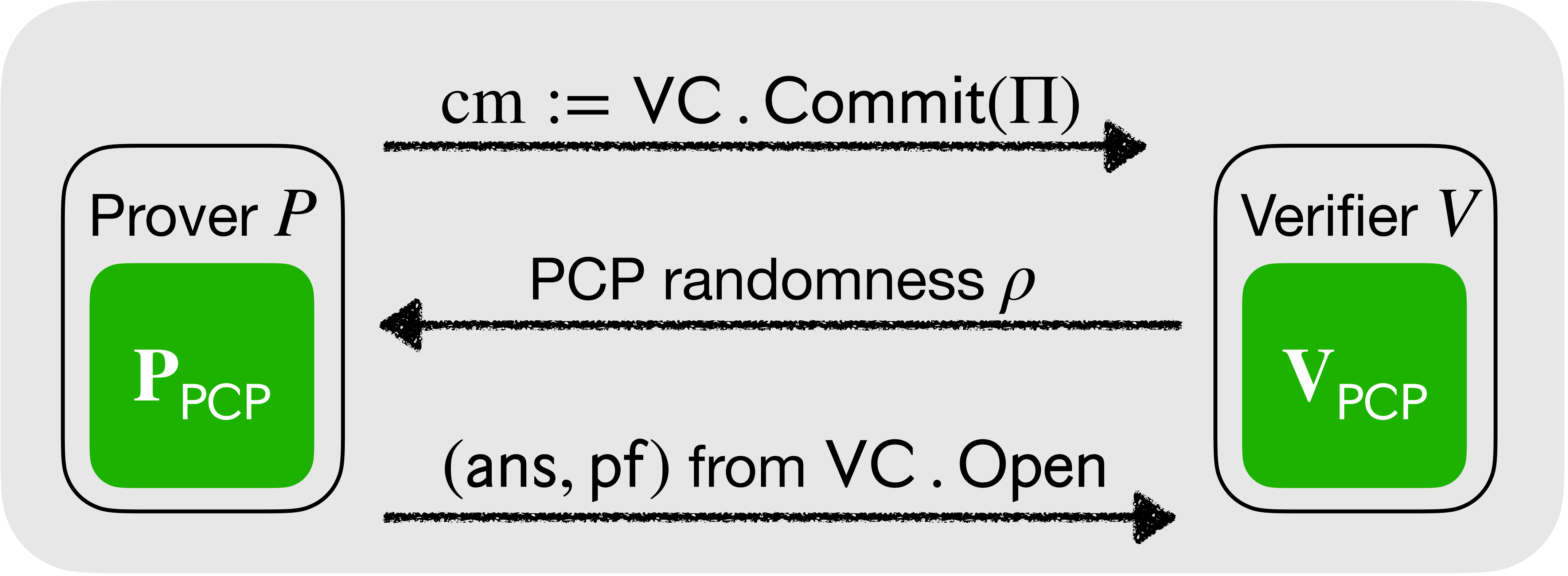
Building block #1: probabilistically checkable proof (PCP)



Building block #2: vector commitment scheme (VC)

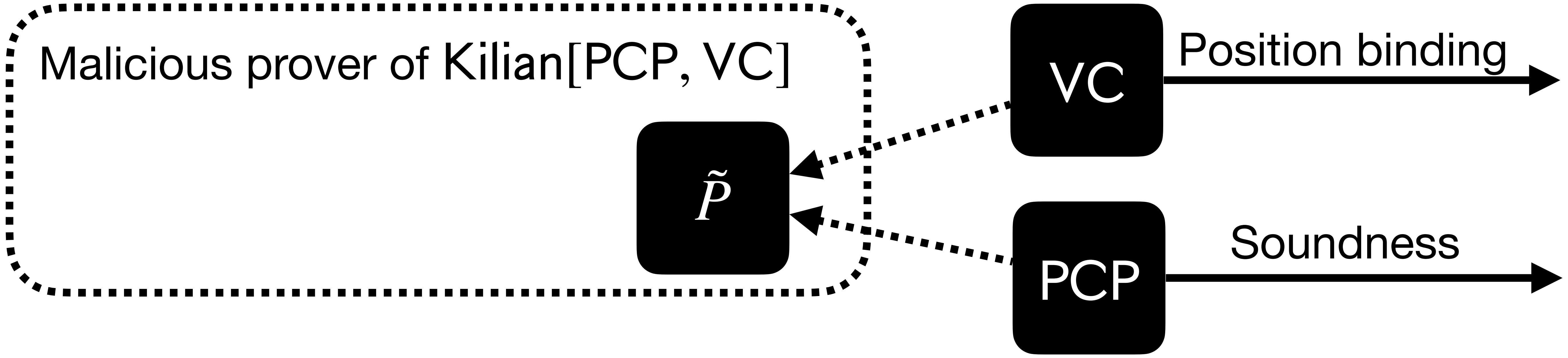


Kilian's protocol



Classical security analysis

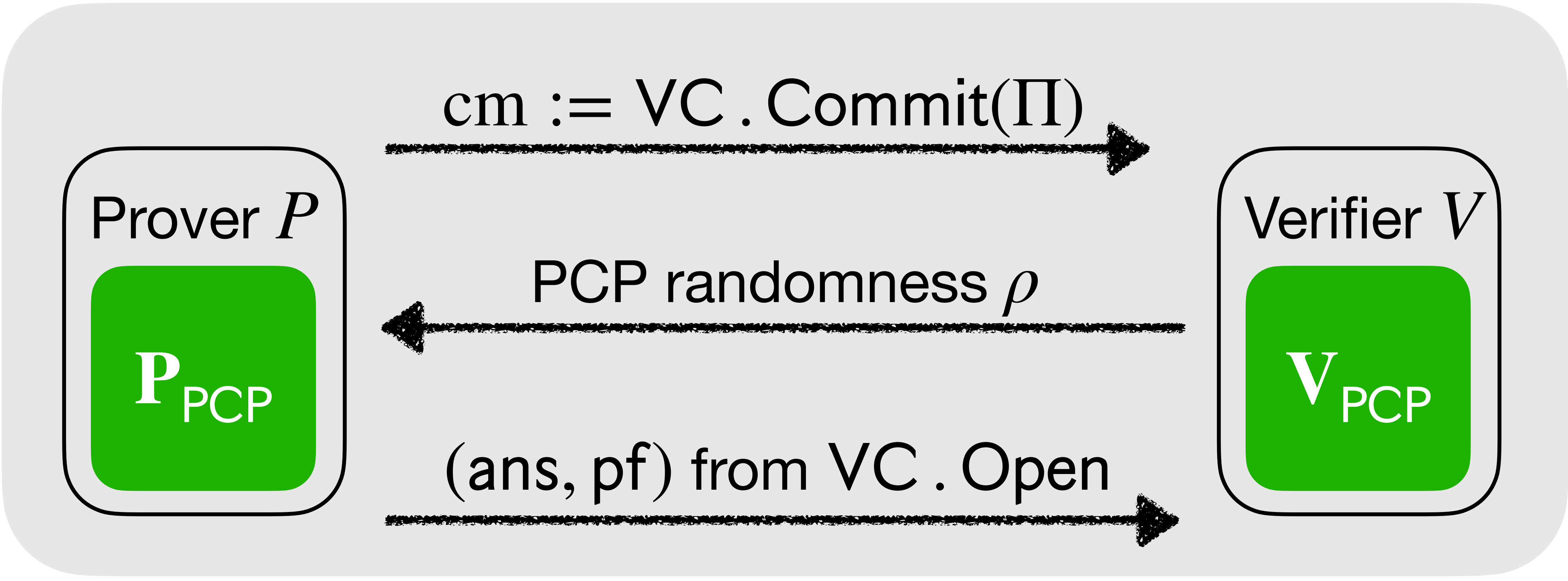
Goal: relate the soundness error of Kilian[PCP, VC]
to the soundness error of PCP and the position binding error of VC.



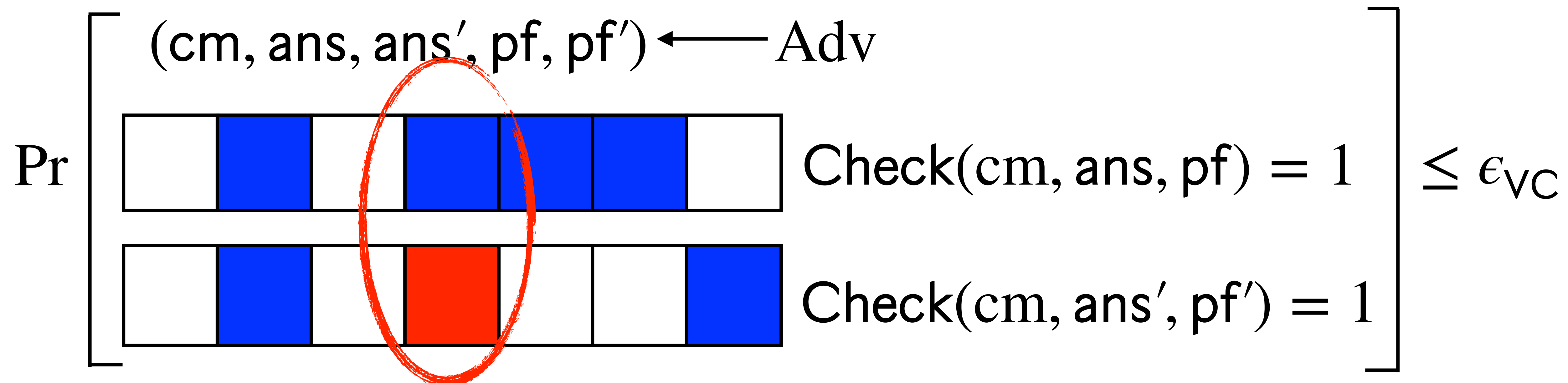
$\tilde{P}$ is forced to open locations of the committed PCP string $\tilde{\Pi}$

Rewind $\tilde{P}$ a number of times to get a bunch of $(Q, \mathsf{ans}, \mathsf{pf})$
$\Longrightarrow$ recover $\tilde{\Pi}$
$\Longrightarrow$ upper bound the success probability of $\tilde{\Pi}$ by soundness of PCP

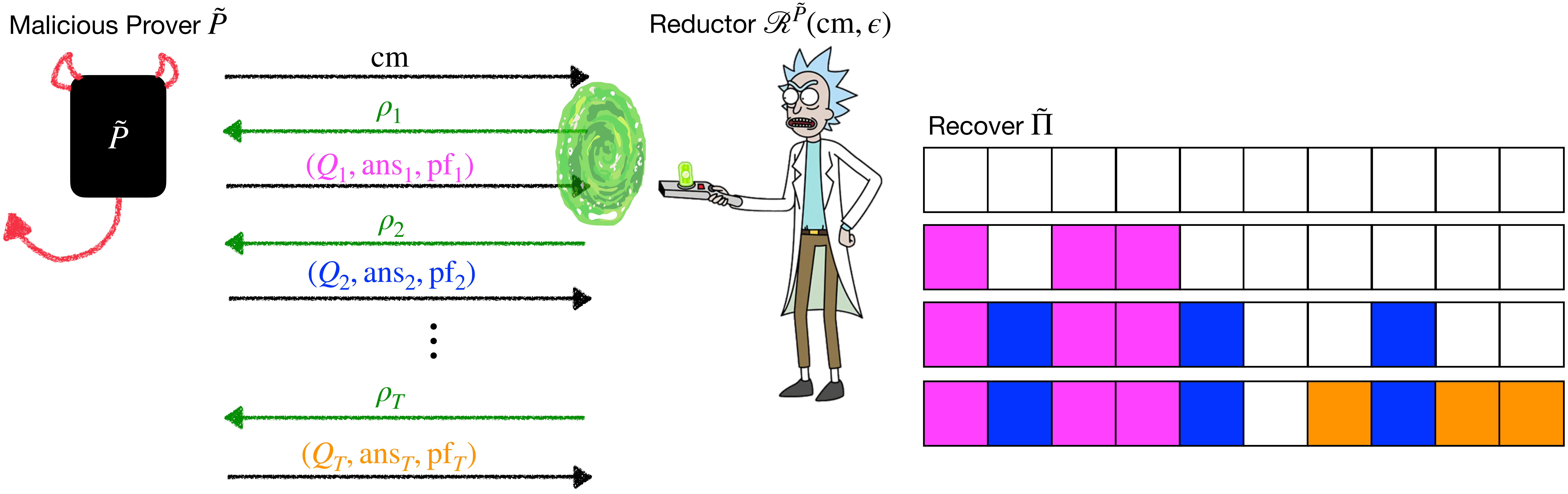
Kilian's protocol



Position binding



Approach: rewind the prover



Theorem [CDGSY24]. $\forall$ PCP $(\epsilon_{\mathsf{PCP}}, \ell_{\mathsf{PCP}})$, VC (ϵ_{VC}), $\epsilon > 0$,

$$\epsilon_{\mathsf{ARG}}(t_{\mathsf{ARG}}) \leq \epsilon_{\mathsf{PCP}} + \epsilon_{\mathsf{VC}}(t_{\mathsf{VC}}) + \epsilon, \text{ where } t_{\mathsf{VC}} = O\left(t_{\mathsf{ARG}} \cdot \ell_{\mathsf{PCP}} \cdot 1/\epsilon\right).$$

Overhead from rewinding.
Possibly inherent [CDGSY24]

How about post-quantum security?

Post-quantum soundness: same as classical soundness but adversary is quantum:

$\forall\, t_{\mathsf{ARG}}$-time QUANTUM adversary $\tilde{P}^\star$, $\Pr\left[\langle \tilde{P}^\star, V\rangle = 1\right] \leq \epsilon^\star_{\mathsf{ARG}}(t_{\mathsf{ARG}})$

Ethereum Unlocks Millions To Prepare For The Post-quantum Era

Sun 11 May 2025 ▪ 4 min read ▪ by Mikaia A.

The building blocks need to be post-quantum secure at the minimum

PCP for language L with soundness error ϵ_{PCP}

PCP has statistical soundness!

$\Longrightarrow \forall\, x \notin L$ and quantum adversary $\tilde{P}$, $\Pr\left[\langle \tilde{P}, V(x)\rangle = 1\right] \leq \epsilon$

Vector commitment scheme with position binding error ϵ_{VC}

post-quantum

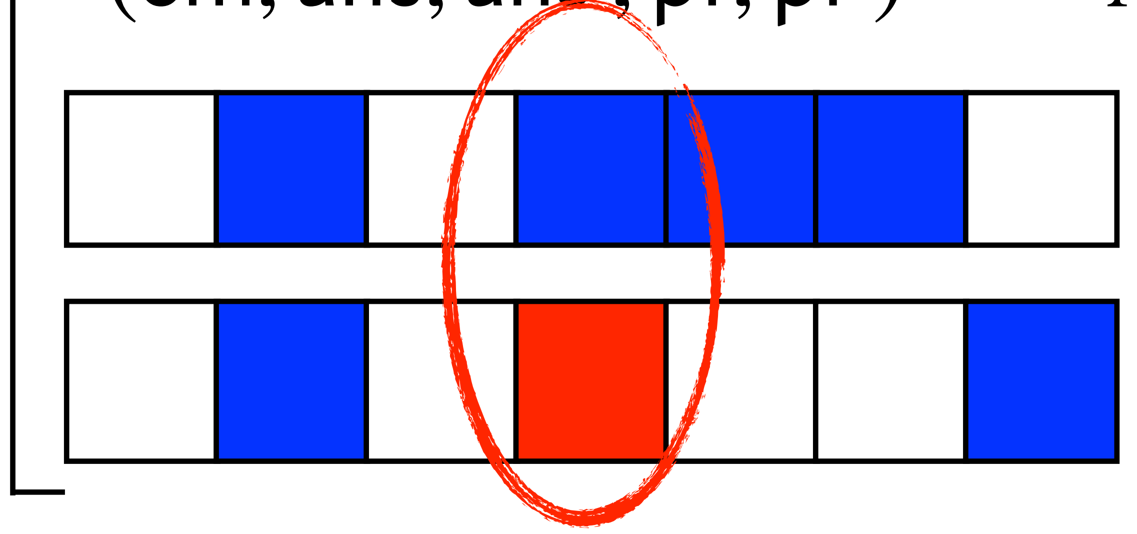
post-quantum

Position binding

Classical messages

Quantum algorithm

$$\Pr\left[\begin{array}{l} (\mathsf{cm}, \mathsf{ans}, \mathsf{ans}', \mathsf{pf}, \mathsf{pf}') \leftarrow \mathrm{Adv} \\ \mathsf{Check}(\mathsf{cm}, \mathsf{ans}, \mathsf{pf}) = 1 \\ \mathsf{Check}(\mathsf{cm}, \mathsf{ans}', \mathsf{pf}') = 1 \end{array}\right] \leq \epsilon_{\mathsf{VC}}$$

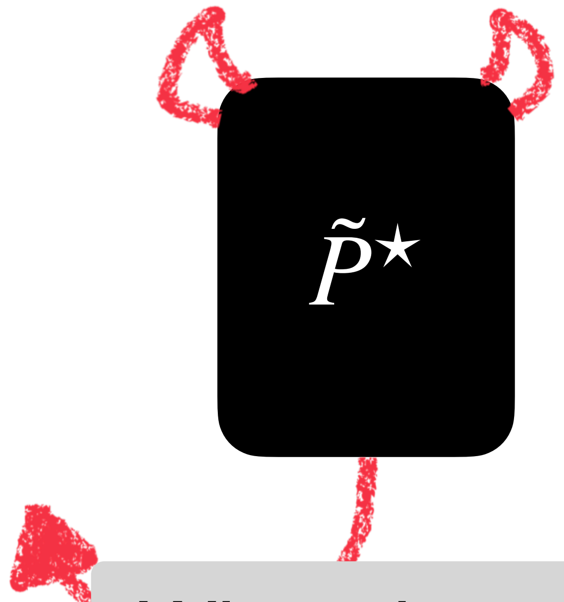


Is this sufficient?
Not with current rewinding techniques…

Key property for rewinding: Collapsing

Quantum reductor

Malicious Prover $\tilde{P}^\star$



Quantum algorithms, but output classical messages

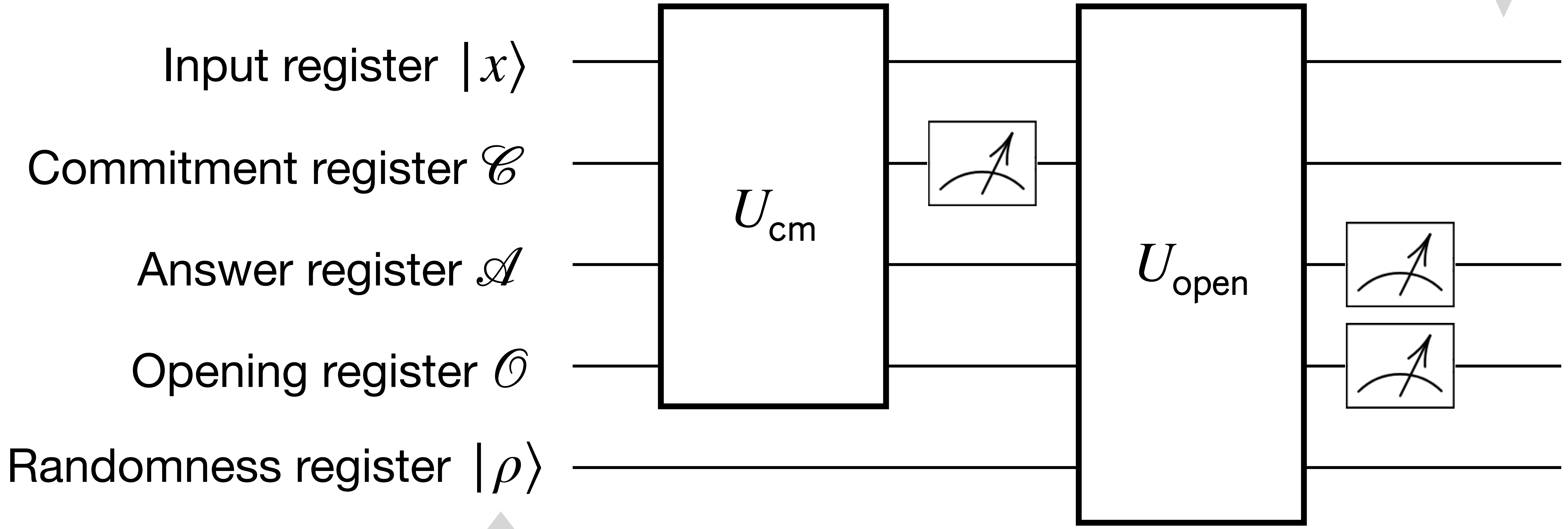
$$\tilde{P}^\star = (U_{\mathrm{cm}}, U_{\mathrm{open}})$$

What does it mean to have black-box access to $\tilde{P}^\star$?

Reductor $\mathscr{R}^{\tilde{P}^\star}(\mathrm{cm}, \epsilon)$

Black-box simulation of $\langle \tilde{P}^\star, V \rangle$

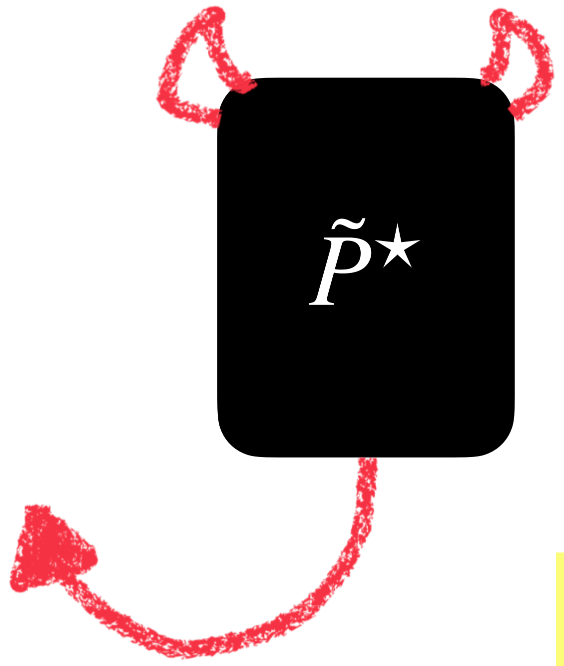
Send measured outcome to V



Uniformly sampled

On quantum rewinding

Malicious Prover $\tilde{P}^{\star}$



Prover state $|\phi\rangle$

cm

ρ_1

Prover state $|\phi'\rangle$

$(\mathscr{A}, \mathscr{O})$

Measure!

ρ_2

How to go back to $|\phi\rangle$?

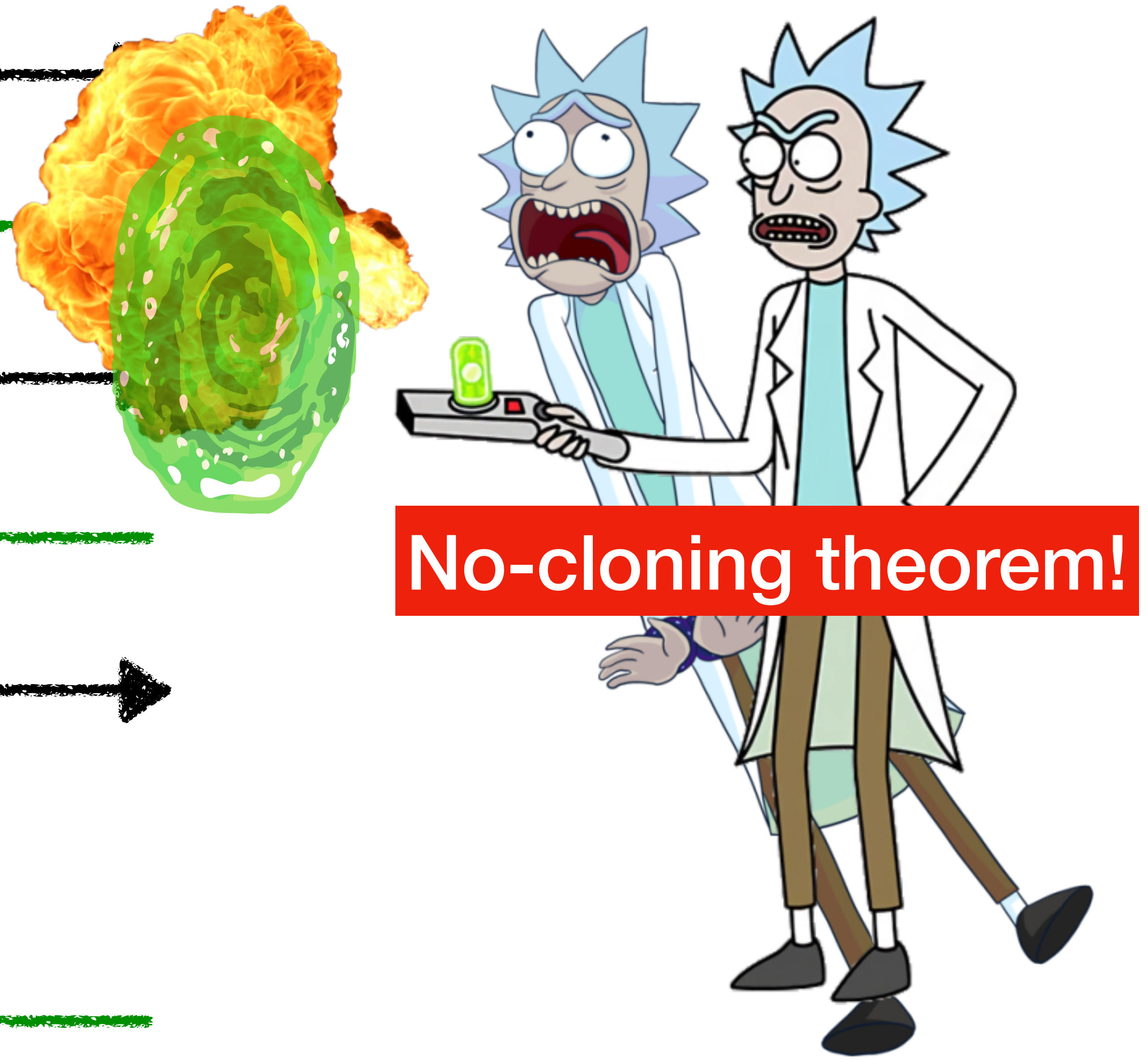
$(\mathscr{A}, \mathscr{O})$

$\vdots$

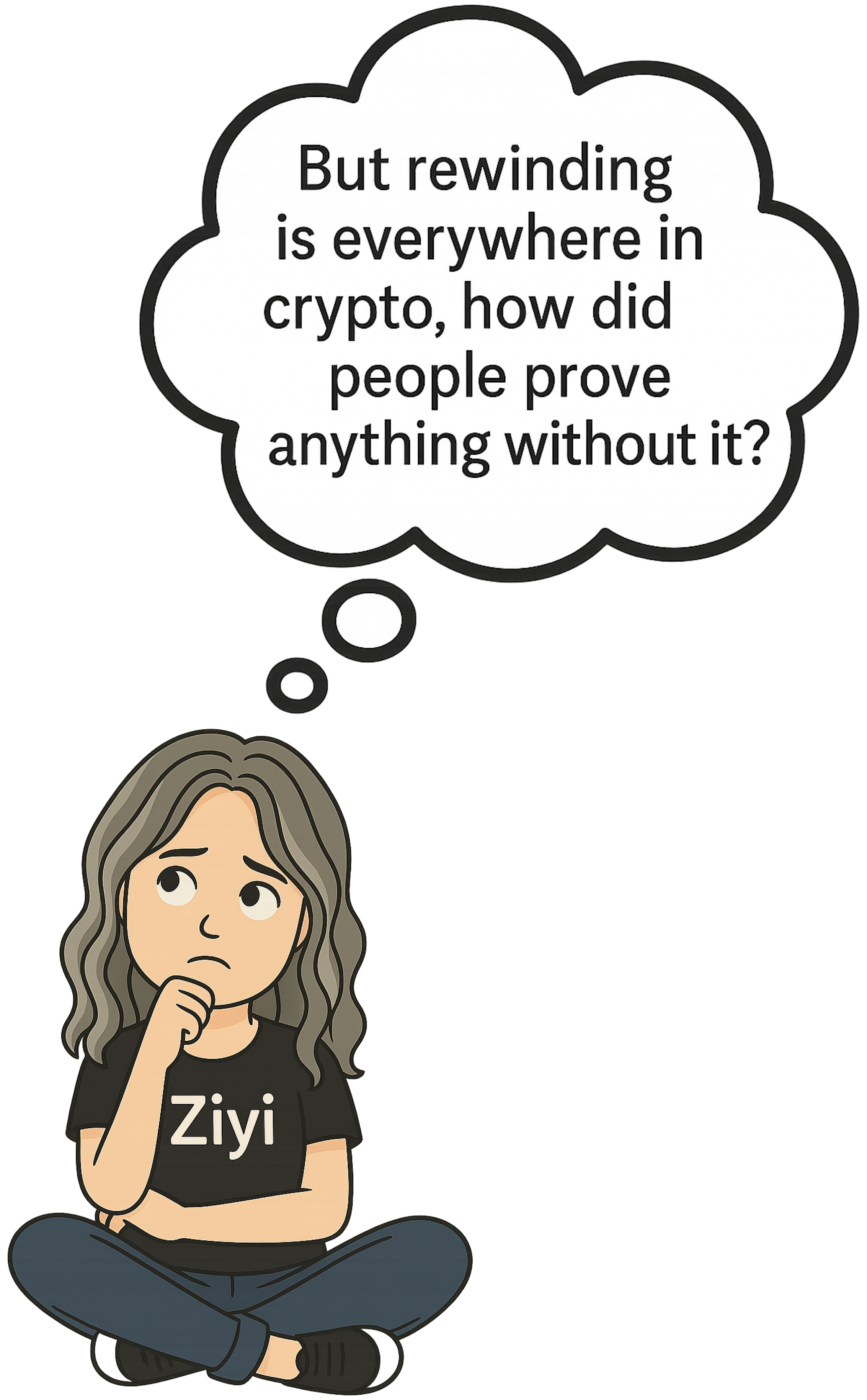
ρ_T

$(\mathscr{A}, \mathscr{O})$

Reductor $\mathscr{R}^{\tilde{P}^{\star}}(\mathrm{cm}, \epsilon)$



No-cloning theorem!

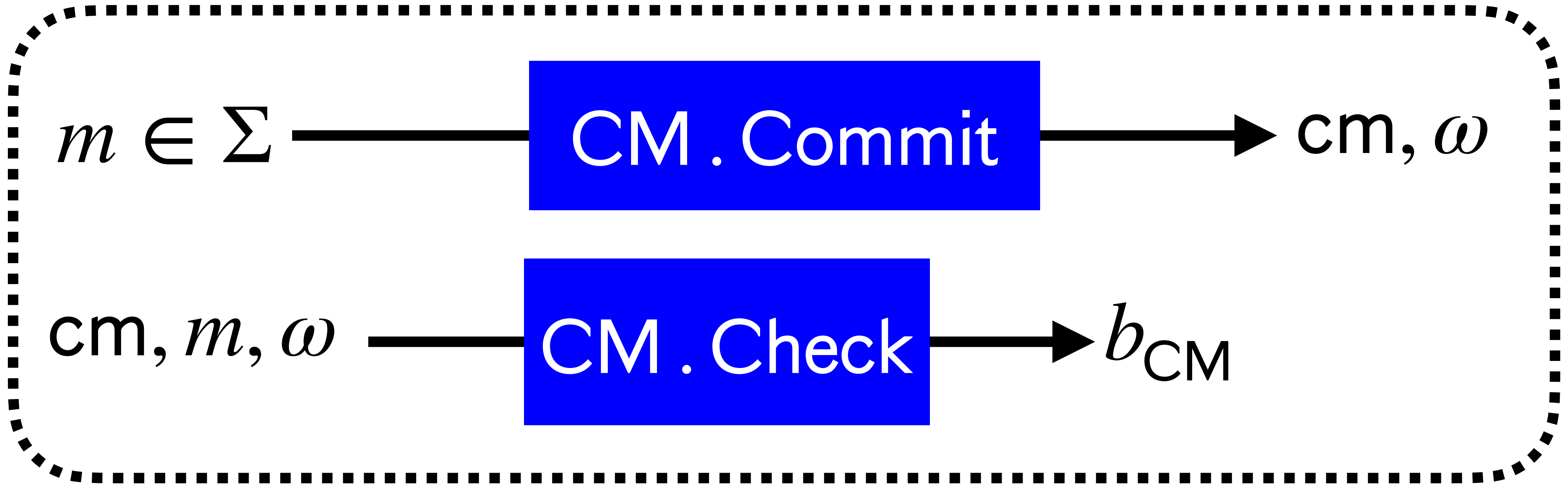


[Unruh16]: standard commitment scheme gives quantum proofs of knowledge

Collapse binding commitment scheme $\Longrightarrow$ quantum rewinding for $O(1)$ times

Quantum rewinding with commitment schemes

Commitment scheme (CM)



Collapse binding Undetectable measurement

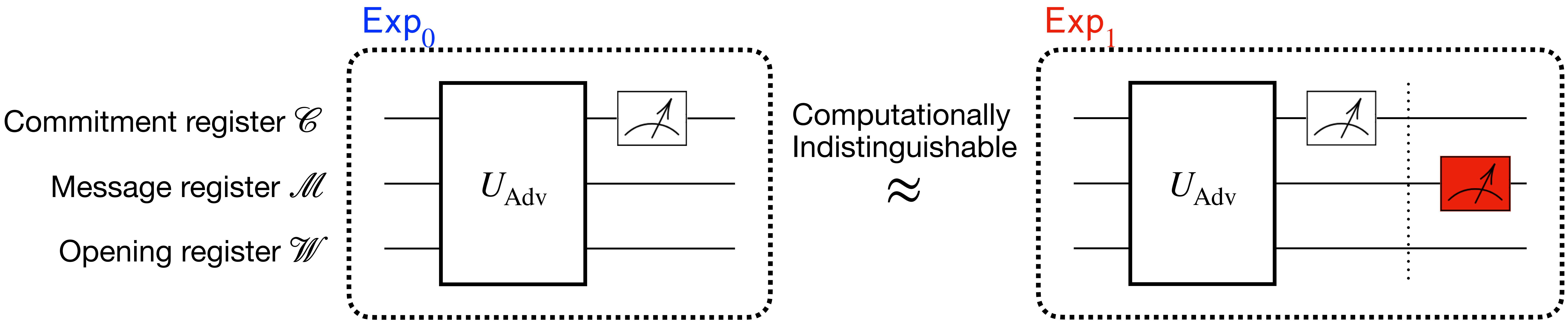
cm, $(\mathscr{M}, \mathscr{W}) \leftarrow \mathrm{Adv}$

Exp$_0$: does nothing

Exp$_1$: measure $\mathscr{M}$

$(\mathscr{M}, \mathscr{W}) \longrightarrow \mathrm{Adv}$

$\Pr[\mathrm{Adv}$ distinguishes Exp$_0$ and Exp$_1] \leq \epsilon^{\star}_{\mathsf{CMCollapse}}$



Collapse binding $\Longrightarrow$ binding
(Adv cannot give different openings for one cm)

How about vector commitments?

CMSZ collapsing

$(\mathsf{cm}, Q), (\mathscr{A}, \mathscr{O}) \longleftarrow \mathrm{Adv}$

Exp$_0$: does nothing

Exp$_1$: measure $(\mathscr{A}, \mathscr{O})$

$(\mathscr{A}, \mathscr{O}) \longrightarrow \mathrm{Adv}$

$\Pr[\mathrm{Adv}$ distinguishes Exp$_0$ and Exp$_1] \leq \epsilon^{\star}_{\mathsf{CMSZCollapse}}$

Why measure $\mathscr{O}$? CM only measure $\mathscr{M}$
[CMSZ21] security analysis needs $\mathscr{O}$

Issue: does not imply position binding
- CMSZ collapsing - one single query set
- Position binding - two query sets Q, Q'

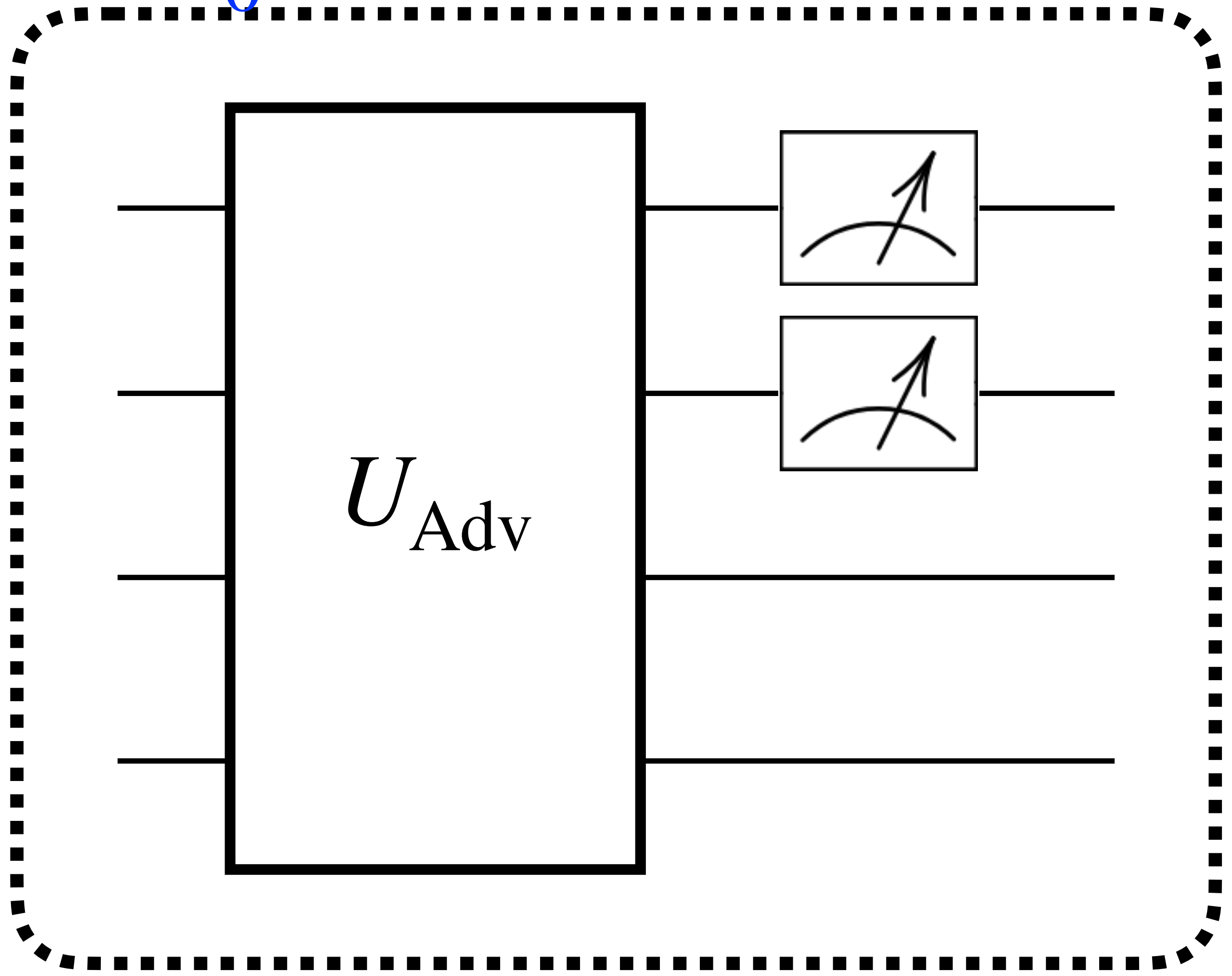
Commitment register $\mathscr{C}$

Query register $\mathscr{Q}$

Answer register $\mathscr{A}$

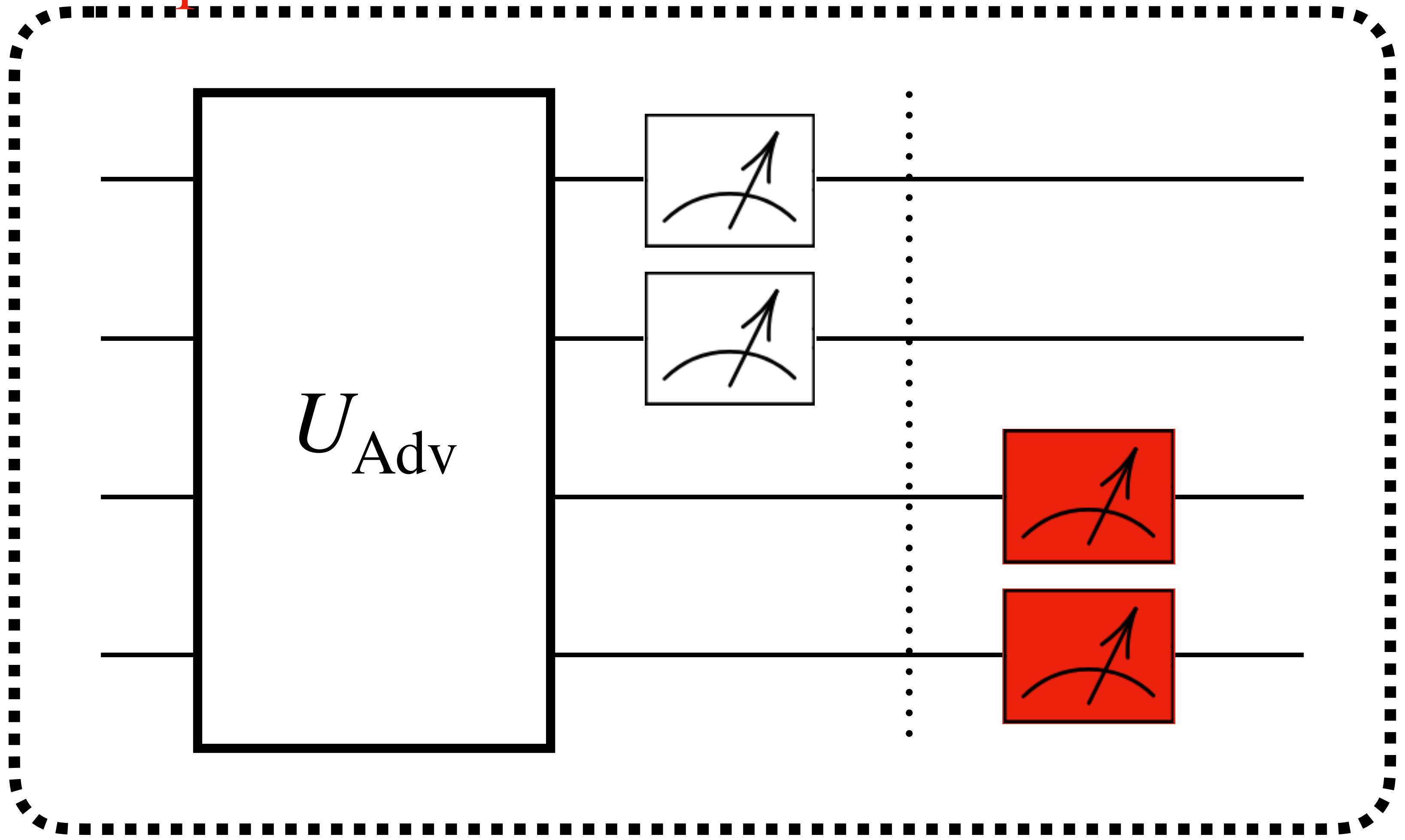
Opening register $\mathscr{O}$

Exp$_0$



Computationally Indistinguishable
$\approx$

Exp$_1$



Merkle tree from collapsing hash is CMSZ collapsing

Post-quantum security of Kilian's protocol

Queries only depend on randomness

Theorem [CMSZ21]. $\forall$ non-adaptive PCP, VC (negligible $\epsilon^{\star}_{\mathsf{PQPB}}$, negligible $\epsilon^{\star}_{\mathsf{CMSZCollapse}}$),

$$\epsilon^{\star}_{\mathsf{ARG}} \leq \epsilon_{\mathsf{PCP}} + \mathsf{negl}$$

Can we get a more robust VC collapsing def?
(VC collapsing that implies position binding)

PCP is not concretely efficient - Can we use IOPs?

Can we get concrete bound as classical case?

Can we handle adaptive PCPs?

A new collapsing definition for VC: Collapse position binding

Naive attempt: openings to different subsets

Recall:
- CMSZ collapsing - one single query set
- Position binding - two query sets Q, Q'

Naive-attempt collapsing

Impossible to achieve!

cm, $(\mathscr{Q}, \mathscr{A}, \mathscr{O}) \longleftarrow \mathrm{Adv}$

Exp_0: does nothing

Exp_1: measure $(\mathscr{Q}, \mathscr{A}, \mathscr{O})$

$(\mathscr{Q}, \mathscr{A}, \mathscr{O}) \longrightarrow \mathrm{Adv}$

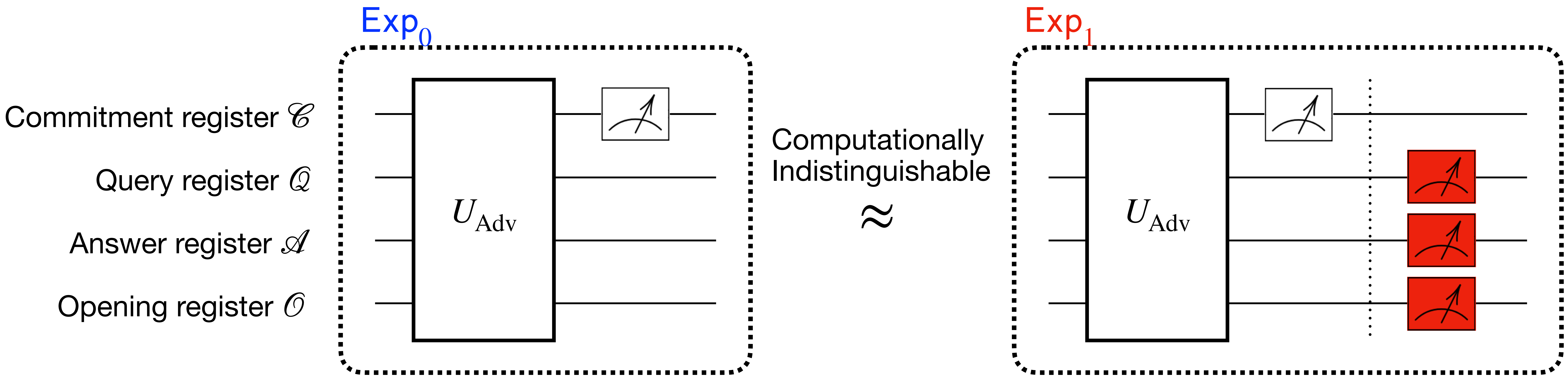
$\Pr[\mathrm{Adv}$ distinguishes Exp_0 and $\text{Exp}_1] \leq \epsilon^{\star}_{\text{NaiveCollapse}}$

Assume cm has two valid openings $(Q, \text{ans}, \text{pf})$, $(Q', \text{ans}', \text{pf}')$

$\mathrm{Adv} \to \text{cm}, |Q, \text{ans}, \text{pf}\rangle + |Q', \text{ans}', \text{pf}'\rangle$

Measuring $(\mathscr{Q}, \mathscr{A}, \mathscr{O}) \Longrightarrow (Q, \text{ans}, \text{pf})$ or $(Q', \text{ans}', \text{pf}')$

$\Longrightarrow$ Easily distinguishable from uniform superposition



Collapse position binding

Lifting from commitment schemes

Vector commitment scheme VC for length ℓ

$\downarrow$

$\forall i \in [\ell]$, commitment scheme CM_i

Collapse position binding

$(\mathsf{cm}, \mathsf{idx}), (\mathscr{A}, \mathscr{O}) \longleftarrow \mathrm{Adv}$

Exp_0: does nothing

Exp_1: measure $\mathscr{A}$ at location idx

$(\mathscr{A}, \mathscr{O}) \longrightarrow \mathrm{Adv}$

$\Pr[\mathrm{Adv}$ distinguishes Exp_0 and $\mathsf{Exp}_1] \leq \epsilon^{\star}_{\mathsf{VCCollapsePB}}$

Known:

- VC position binding $\iff \forall i$, CM_i binding
- CM collapse binding $\implies$ CM binding

Goal: VC collapse position binding $\iff \forall i$, CM_i collapse binding

VC collapse position binding $\implies$ VC position binding

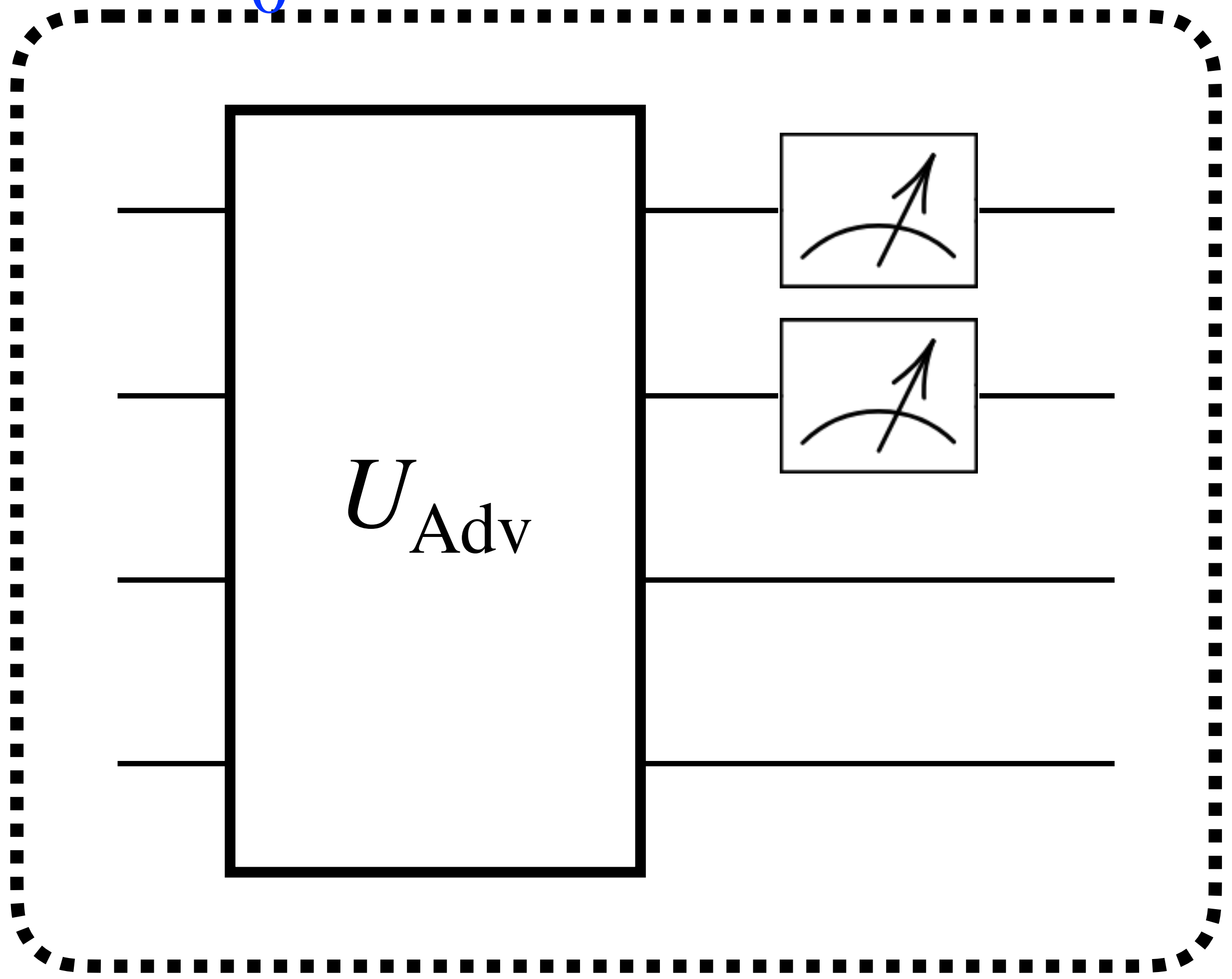
Commitment register $\mathscr{C}$

Index register $\mathscr{I}$

Answer register $\mathscr{A}$

Opening register $\mathscr{O}$

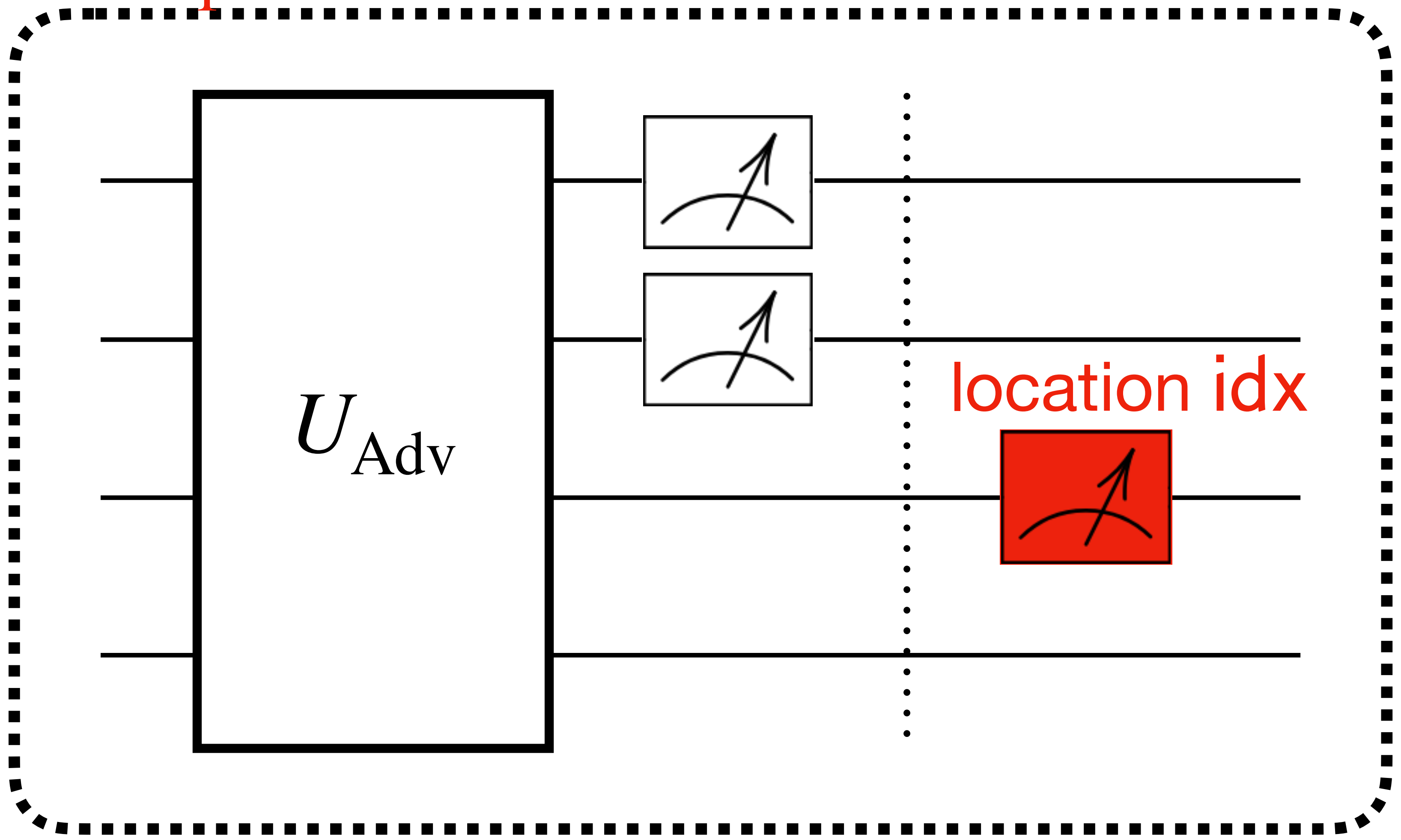
Exp_0



Computationally Indistinguishable

$\approx$

Exp_1



Improved post-quantum security of Kilian's protocol

Queries only depend on randomness

Theorem [CMSZ21]. $\forall$ non-adaptive PCP, VC (negligible ~~$\epsilon^\star_{\mathrm{PQPB}}$, neg~~ **negligible $\epsilon^\star_{\mathrm{VCCollapsePB}}$**

$$\epsilon^\star_{\mathrm{ARG}} \leq \epsilon_{\mathrm{PCP}} + \mathrm{negl}$$

Can we get a more robust VC collapsing def?
(VC collapsing that implies position binding)

YES!

PCP is not concretely efficient - Can we use IOPs?

Can we get concrete bound as classical case?

Can we handle adaptive PCPs?

IBCS protocol:
Using IOPs instead of PCPs

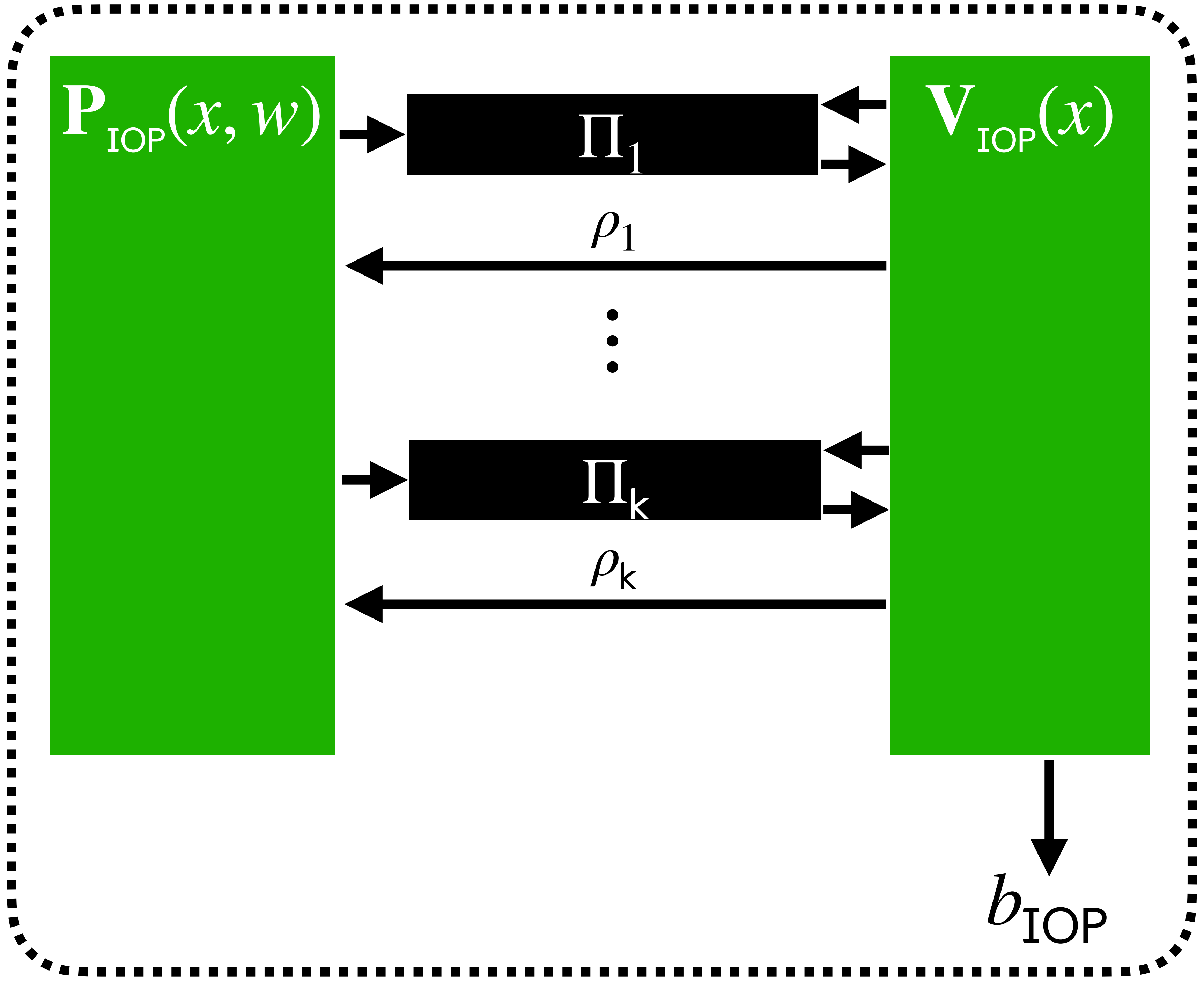
[BCS16; CDGS23]

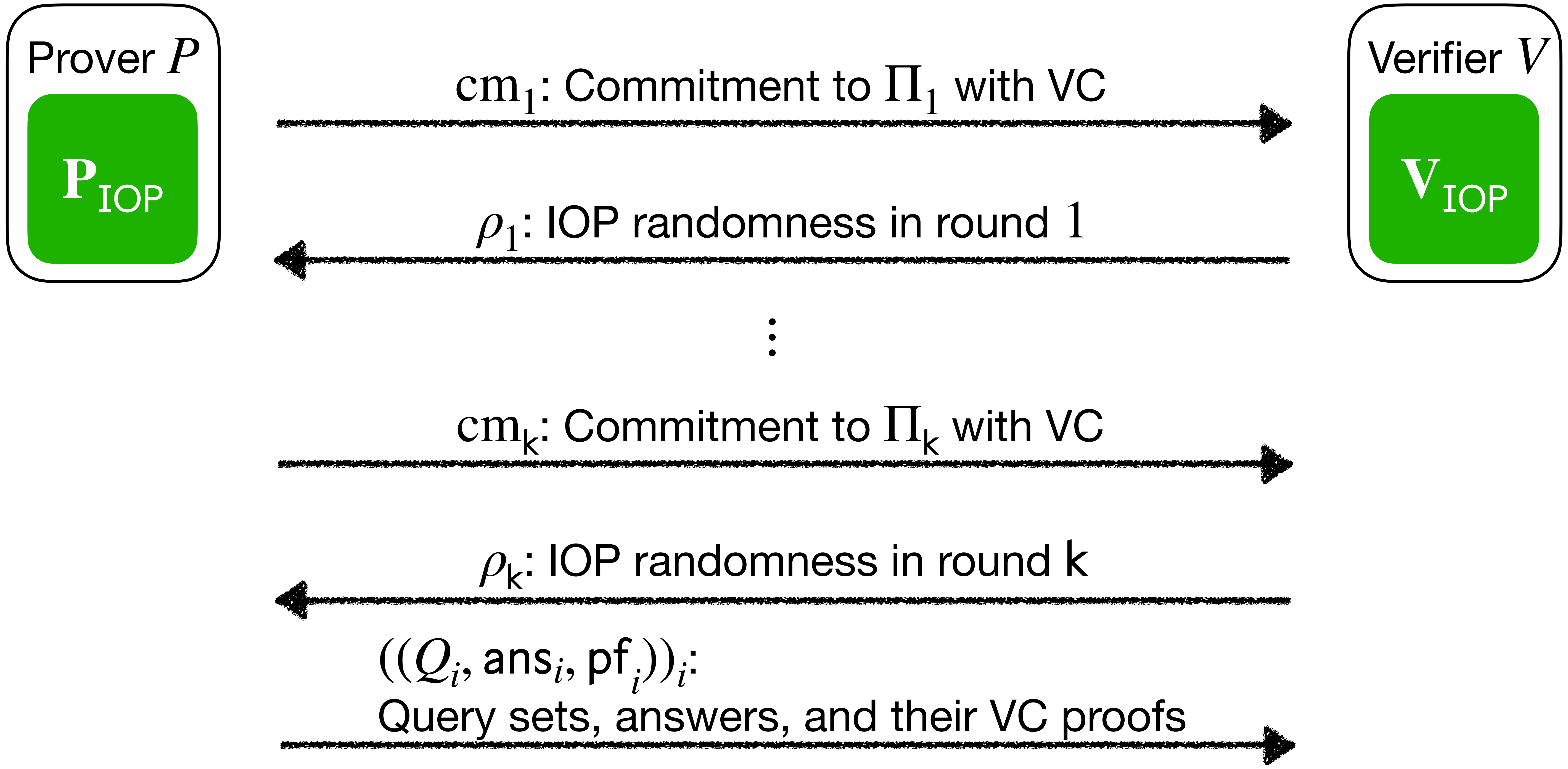
IBCS protocol

Existing PCPs are not concretely efficient: prover time too big

People use IOPs

Public-coin interactive oracle proof (IOP)





Our result

Queries depend on randomness and answers to queries to previous proofs

Theorem. $\forall$ semi-adaptive IOP, VC, $\epsilon > 0$,

$$\epsilon^\star_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{IOP}} + \mathsf{k} \cdot \ell_{\max} \cdot \mathsf{q}_{\max} \cdot \epsilon^\star_{\text{VCCollapsePB}}(t_{\text{VC}}) + \epsilon, \text{ where } t_{\text{VC}} = \text{poly}(\ell/\epsilon) \cdot t_{\text{ARG}}.$$

Quantum rewinding can fail

$\text{poly}(\ell/\epsilon)$ attempts $\Longrightarrow \ell/\epsilon$ valid rewindings

Extra $l_{\max} \cdot \mathsf{q}_{\max}$ factor: cost of quantum rewinding

IBCS soundness [CDGS23,CGKY25]: $\epsilon_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{IOP}} + \mathsf{k} \cdot \epsilon_{\text{VC}}(t_{\text{VC}}) + \epsilon$, where $t_{\text{VC}} = O\left(t_{\text{ARG}} \cdot \ell/\epsilon\right)$.

Corollary: post-quantum secure succinct arguments in the standard model (no oracles), with **the best asymptotic complexity known**.

Corollary for Kilian's protocol. $\forall$ adaptive PCP, VC, $\epsilon > 0$,

$$\epsilon^\star_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{IOP}} + \ell \cdot \mathsf{q} \cdot \epsilon^\star_{\text{VCCollapsePB}}(t_{\text{VC}}) + \epsilon, \text{ where } t_{\text{VC}} = \text{poly}(\ell/\epsilon) \cdot t_{\text{ARG}}.$$

Theorem [CMSZ21]. $\forall$ non-adaptive PCP, VC (negligible $\epsilon^\star_{\text{PQPB}}$, negligible $\epsilon^\star_{\text{CMSZCollapse}}$),

$$\epsilon^\star_{\text{ARG}} \leq \epsilon_{\text{PCP}} + \text{negl}$$

YES!

Can we get a more robust VC collapsing def?

PCP is not concretely efficient - Can we use IOPs?

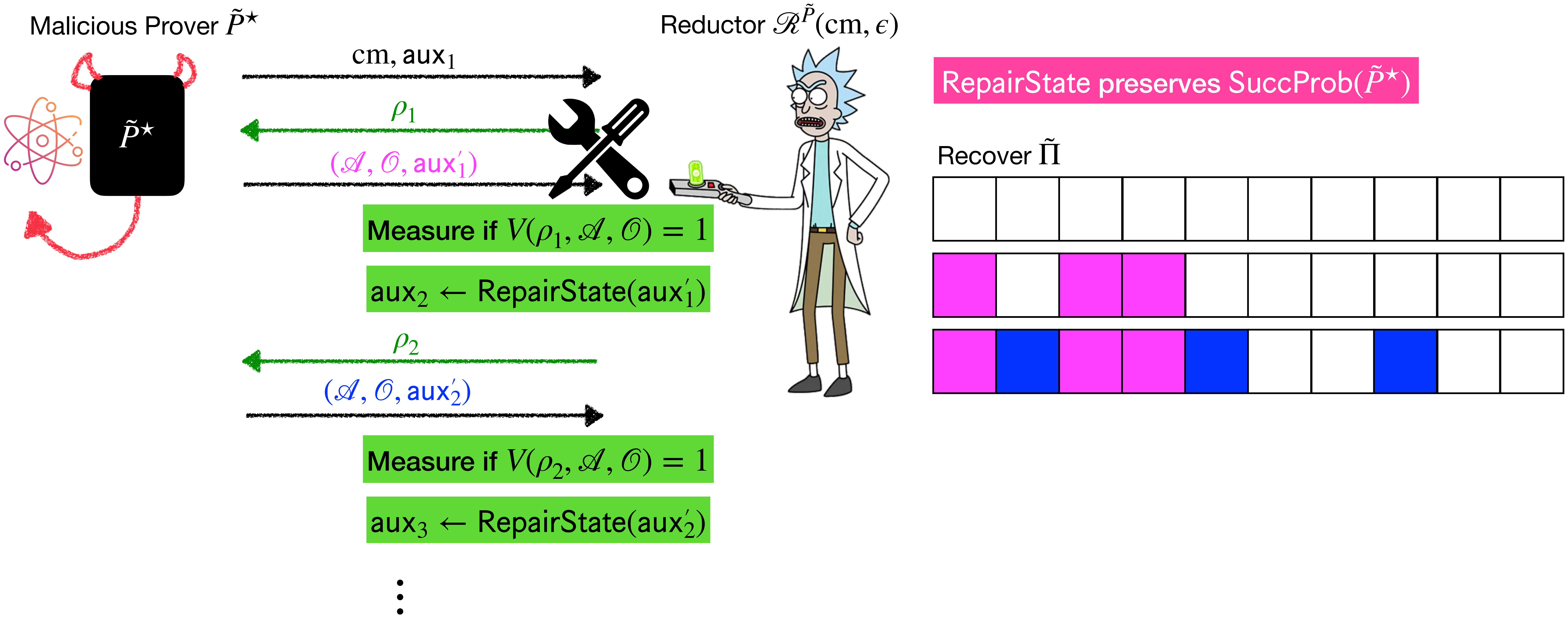
Can we get concrete bound as classical case?

Can we handle adaptive PCPs?

Post-quantum security for Kilian

Starting point: [CMSZ21]

[CMSZ21] reductor



[CMSZ21] security reduction

Goal: relate the soundness error of Kilian[PCP, VC]

to the soundness error of PCP and the post-quantum security of VC.

Malicious prover

$\tilde{P}^\star$

VC

PCP

Post-quantum position binding

$\tilde{P}$ is forced to open locations of the committed PCP string $\tilde{\Pi}$

CMSZ collapsing

Soundness

Rewind and Repair $\tilde{P}^\star$ a number of times to get a bunch of (ans, pf)

$\Longrightarrow$ recover $\tilde{\Pi}$

$\Longrightarrow$ success probability of $\tilde{\Pi}$ is similar to success probability of $\tilde{P}^\star$

RepairState preserves SuccProb($\tilde{P}^\star$)

Consider $\hat{\Pi}$ s.t. SuccProb($\hat{\Pi}$) $<$ SuccProb($\tilde{P}^\star$)$/20$

$\Longrightarrow$ (Chernoff) $\Pr[\tilde{\Pi} = \hat{\Pi}] \ll |\Sigma|^{-\ell}$

$\Longrightarrow$ (Union bound) Pr[SuccProb($\tilde{\Pi}$) $<$ SuccProb($\tilde{P}^\star$)$/20$] very small

$\Longrightarrow$ $\epsilon^\star_{\mathrm{ARG}} =$ SuccProb($\tilde{P}^\star$) $\leq \epsilon_{\mathrm{PCP}} +$ negl

Doesn't work for IOP!

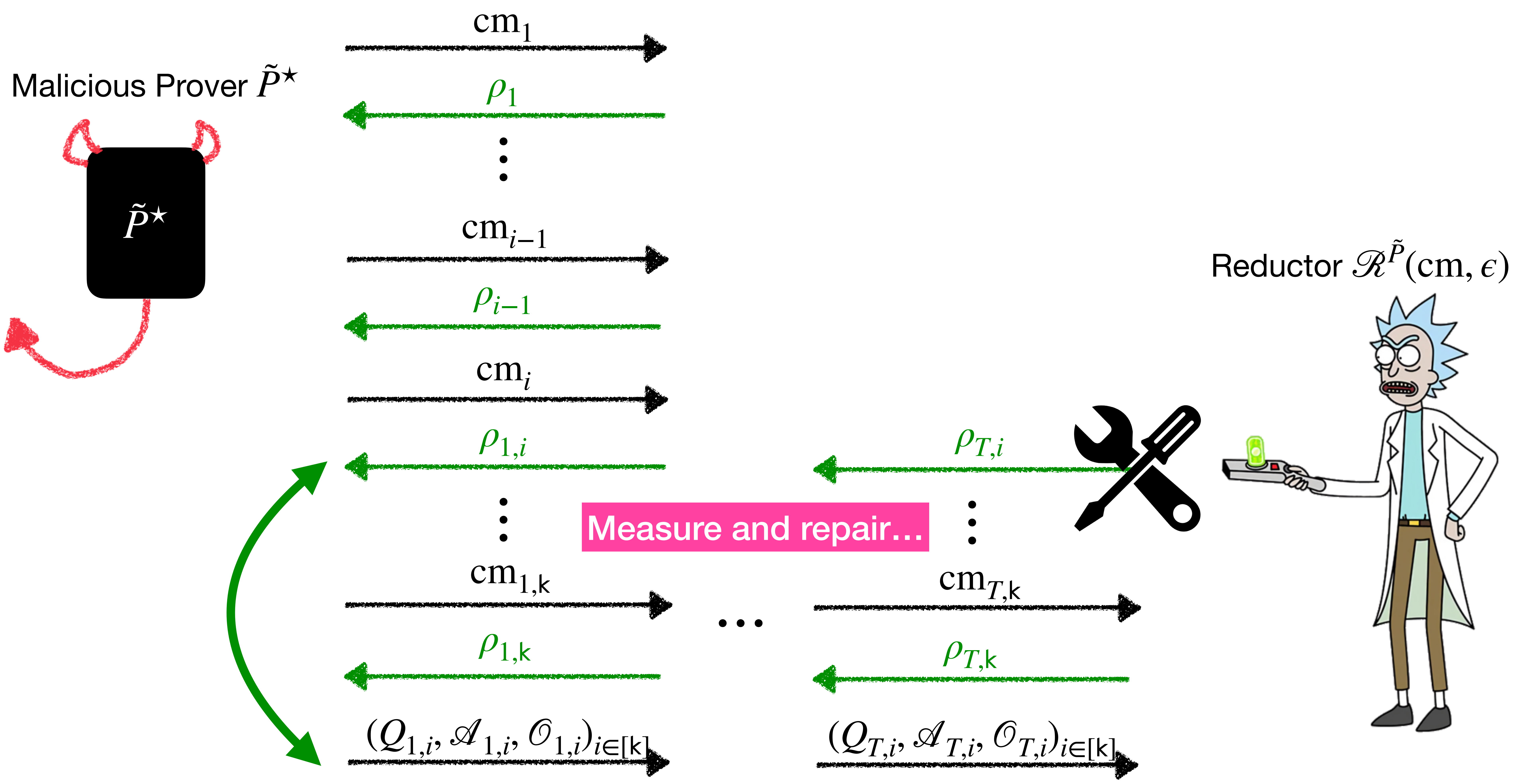
How many possible IOP strings?

- Alphabet Σ
- Proof length ℓ
- Verifier randomness complexity r

$\Longrightarrow \ |\{f : \{0,1\}^{\mathsf{r}} \to \Sigma^{\ell}\}| = |\Sigma|^{\ell \cdot 2^{\mathsf{r}}}$

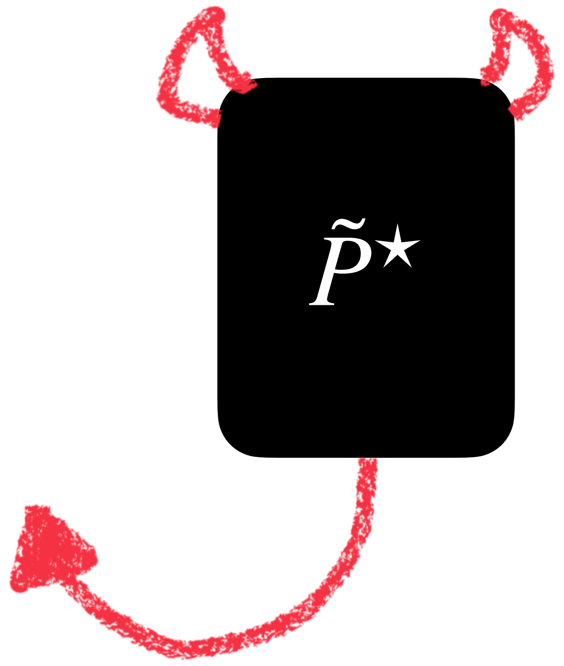
Our security reduction

Our quantum reductor



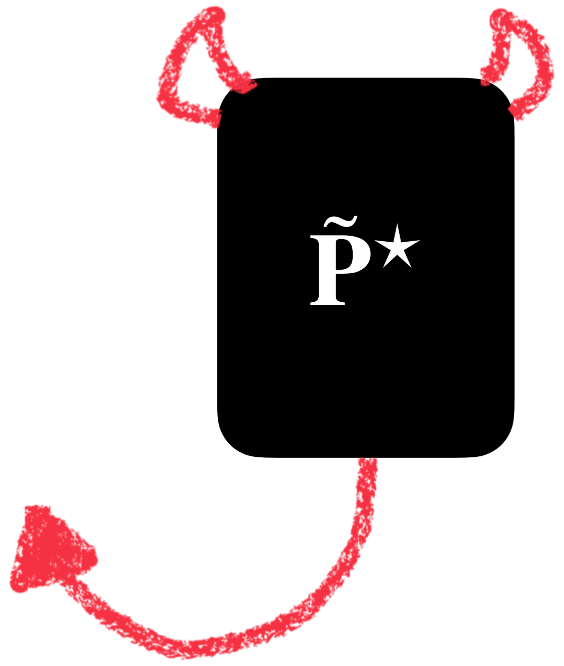
Hybrid argument

Malicious Prover $\tilde{P}^\star$



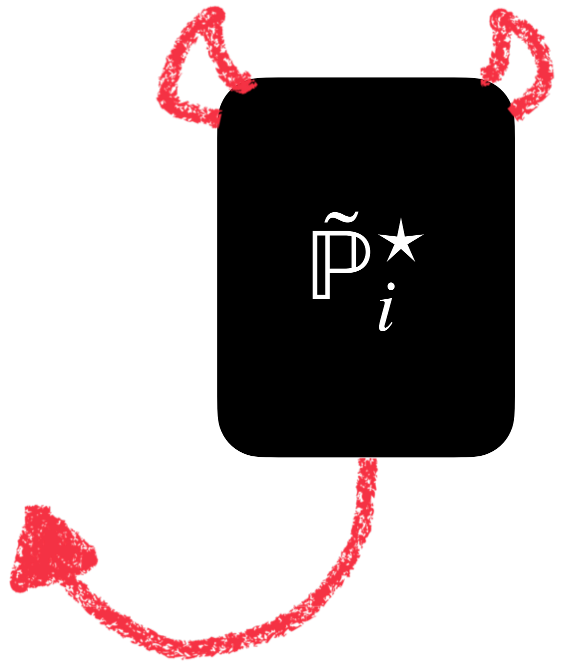
Security reduction using $\mathscr{R}^{\tilde{P}^\star}$

Malicious IOP Prover $\tilde{\mathbf{P}}^\star$



Goal: SuccProb$(\tilde{P}^\star) \approx$ SuccProb$(\tilde{\mathbf{P}}^\star)$

Hybrid Prover $\tilde{\mathbb{P}}_i^\star$

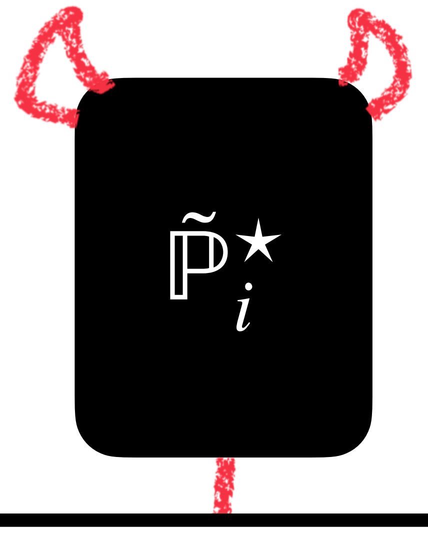


- First i rounds: output IOP strings output by $\mathscr{R}^{\tilde{P}^\star}$
- Rest of the rounds: same as $\tilde{P}^\star$

We show: $\forall i$, SuccProb$(\tilde{\mathbb{P}}_i^\star) \approx$ SuccProb$(\tilde{\mathbb{P}}_{i+1}^\star)$

Our security reduction

Hybrid Prover $\tilde{\mathbb{P}}^\star_i$

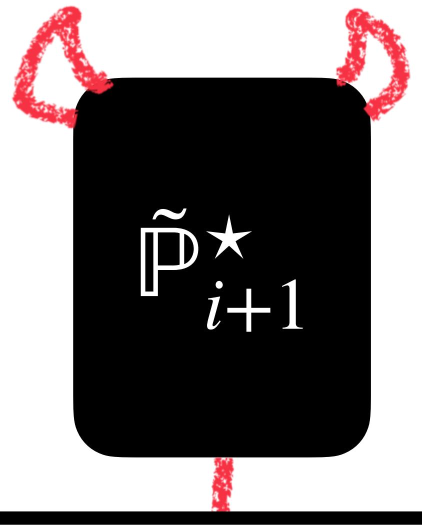


$\tilde{\Pi}_1, \ldots, \tilde{\Pi}_i, \mathsf{cm}_{i+1}, \ldots, \mathsf{cm}_k$

$\mathscr{R}^{\tilde{P}^\star}$ for round $i+1$

$\mathsf{SuccProb}(\tilde{\mathbb{P}}^\star_i) \approx \mathsf{SuccProb}(\tilde{\mathbb{P}}^\star_{i+1})$

Hybrid Prover $\tilde{\mathbb{P}}^\star_{i+1}$



$\tilde{\Pi}_1, \ldots, \tilde{\Pi}_i, \tilde{\Pi}_{i+1}, \mathsf{cm}_{i+2}, \ldots, \mathsf{cm}_k$

$\mathsf{SuccProb}(\tilde{\mathbb{P}}^\star_i) \not\approx \mathsf{SuccProb}(\tilde{\mathbb{P}}^\star_{i+1})$

Errors from measurements and RepairState

At most $\ell_{\mathsf{max}} \cdot \mathsf{q}_{\mathsf{max}}$ measurements each round

$\implies \leq \ell_{\mathsf{max}} \cdot \mathsf{q}_{\mathsf{max}} \cdot \epsilon^\star_{\mathsf{VCCollapsePB}}(t_{\mathsf{VC}})$

Openings for cm_{i+1} different from $\tilde{\Pi}_{i+1}$

VC position binding

V queries a location not filled in $\tilde{\Pi}_{i+1}$

Missing queries

Missing queries

V queries a location not filled in $\tilde{\Pi}_{i+1}$

Hybrid Prover $\tilde{\mathbb{P}}^{\star}_{i}$

$\tilde{\mathbb{P}}^{\star}_{i}$

$\tilde{\Pi}_1, \ldots, \tilde{\Pi}_i$, $\mathsf{cm}_{i+1}, \ldots, \mathsf{cm}_\mathsf{k}$

$\mathscr{R}^{\tilde{P}^{\star}}$ for round $i+1$

SuccProb($\tilde{\mathbb{P}}^{\star}_{i}$) $\approx$ SuccProb($\tilde{\mathbb{P}}^{\star}_{i+1}$)

Hybrid Prover $\tilde{\mathbb{P}}^{\star}_{i+1}$

$\tilde{\mathbb{P}}^{\star}_{i+1}$

$\tilde{\Pi}_1, \ldots, \tilde{\Pi}_i, \tilde{\Pi}_{i+1}$, $\mathsf{cm}_{i+2}, \ldots, \mathsf{cm}_\mathsf{k}$

Run $\tilde{\mathbb{P}}^{\star}_{i}$ one more time, get openings for cm_{i+1}

$\Longrightarrow$ The $(T+1)$-th rewind

Rewind $\tilde{\mathbb{P}}^{\star}_{i}$ T times to get $\tilde{\Pi}_{i+1}$

Classical approach

- δ_q: prob $q \in [\ell_i]$ queried by V and correctly opened by $\tilde{P}^{\star}$
- $\Pr[\exists q, \tilde{\Pi}_{i+1}[q]$ unfilled, q queried with valid opening$] \leq \ell_i \cdot \delta_q (1-\delta_q)^T \leq \ell_i / T$
- Setting T to get desired bound

Doesn't work for quantum!

RepairState only preserves SuccProb($\tilde{P}^{\star}$)

$\Longrightarrow$ does not preserve δ_q

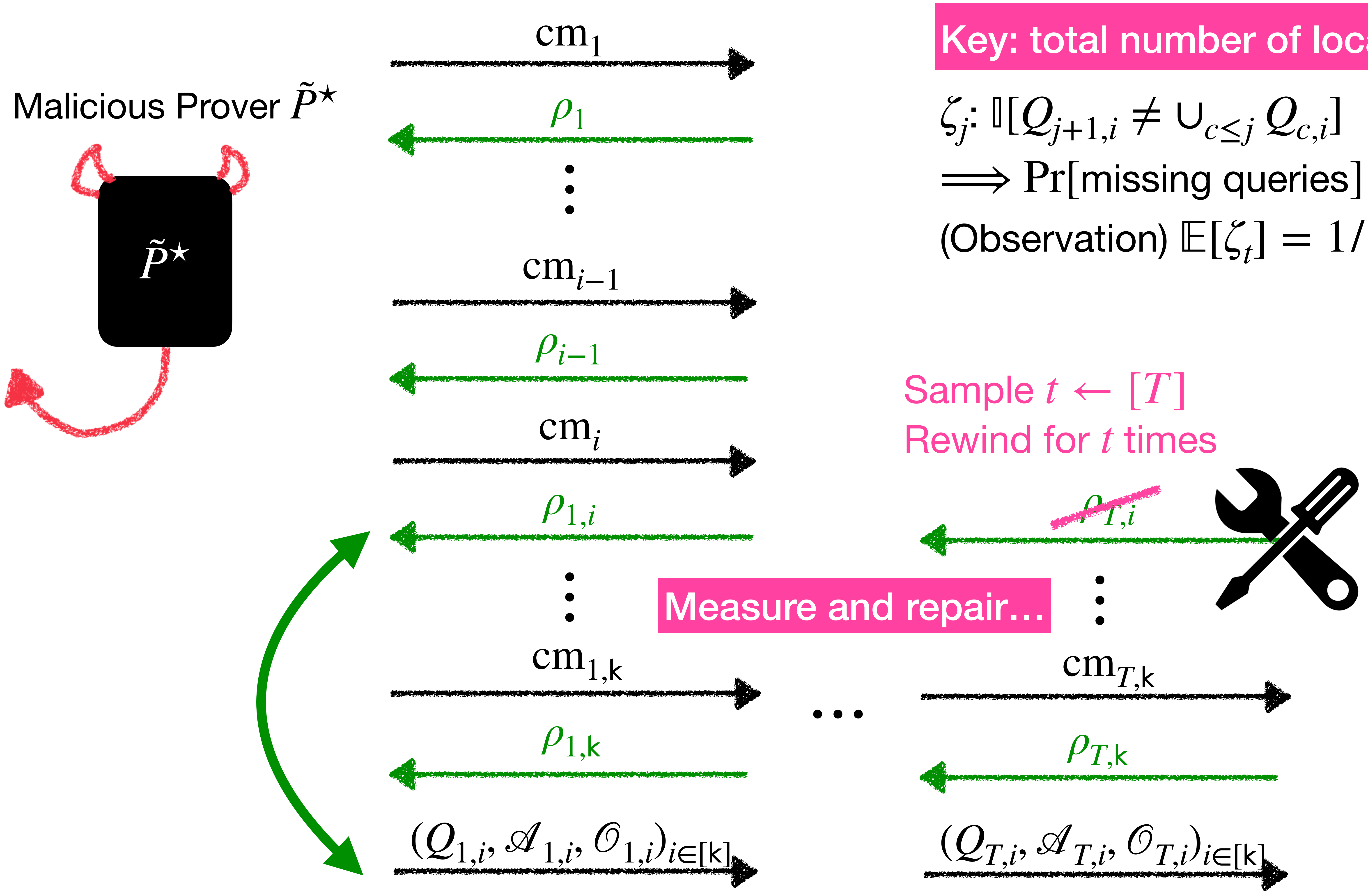
Random stopping time

Key: total number of locations $q \in [\ell_i]$ filled in by $\mathscr{R}$ is ℓ_i

ζ_j: $\mathbb{I}[Q_{j+1,i} \neq \cup_{c \leq j} Q_{c,i}]$

$\implies \Pr[\text{missing queries}] = \mathbb{E}[\zeta_t]$

(Observation) $\mathbb{E}[\zeta_t] = 1/T \cdot \sum_{j \leq T} \mathbb{E}[\zeta_j] \leq \ell_i / T$



Reductor $\mathscr{R}^{\tilde{P}^\star}(\mathrm{cm}, \epsilon)$

Why not adaptive IOP?

Queries to Π_1 depends on answers from Π_2

$(\mathscr{Q}_1, \mathscr{A}_1, \mathscr{O}_1)$ and $(\mathscr{Q}_2, \mathscr{A}_2, \mathscr{O}_2)$ entangled

$\Longrightarrow$ Measuring $(\mathscr{Q}_1, \mathscr{A}_1, \mathscr{O}_1)$ collapses $(\mathscr{Q}_2, \mathscr{A}_2, \mathscr{O}_2)$

Collapse position binding does not allow measurement of $(\mathscr{Q}_2, \mathscr{A}_2, \mathscr{O}_2)$

Collapse position binding

(cm, idx), $(\mathscr{A}, \mathscr{O}) \longleftarrow \mathrm{Adv}$

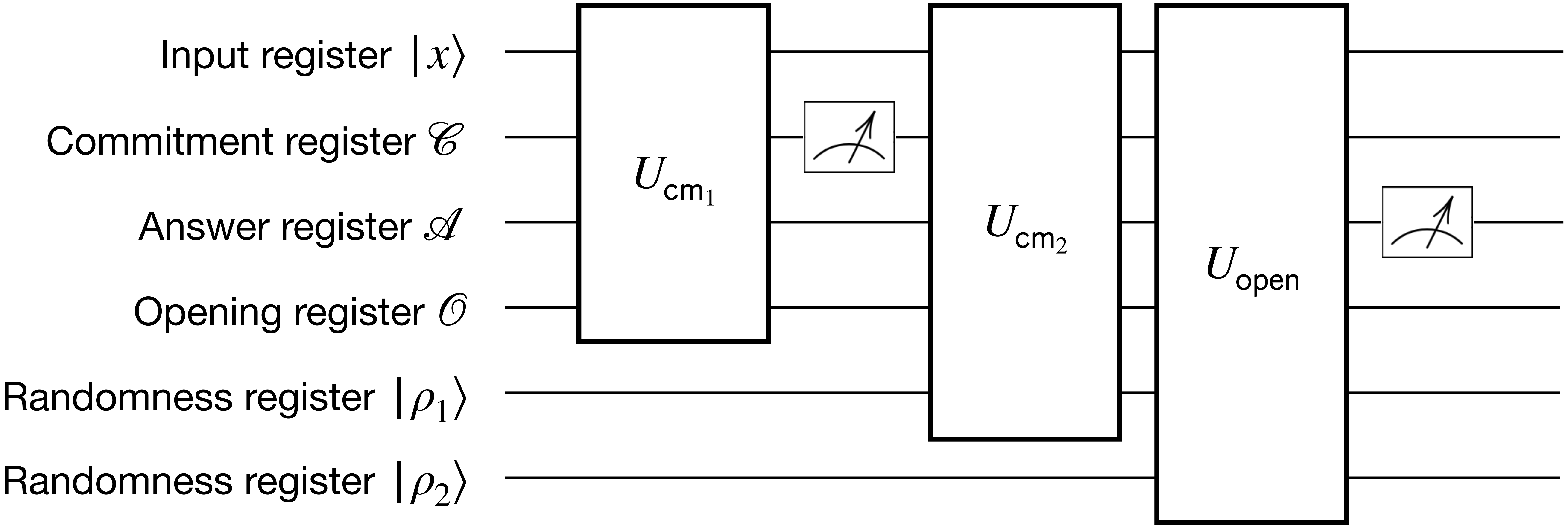
Exp$_0$: does nothing

Exp$_1$: measure $\mathscr{A}$ at location idx

$(\mathscr{A}, \mathscr{O}) \longrightarrow \mathrm{Adv}$

$\Pr[\mathrm{Adv}$ distinguishes Exp$_0$ and Exp$_1] \leq \epsilon^{\star}_{\mathsf{VCCollapse}}$

When $\mathscr{R}^{\tilde{P}^\star}$ rewinds to get $\tilde{\Pi}_1$...



Open problem: extend to adaptive IOP

Recap

[Kilian92]

Kilian's protocol:
PCP + VC → ARG

Classical Security [CDGSY24]

Post-quantum Security [CMSZ21]

Prior work

This work

[BCS16;CDGS23]

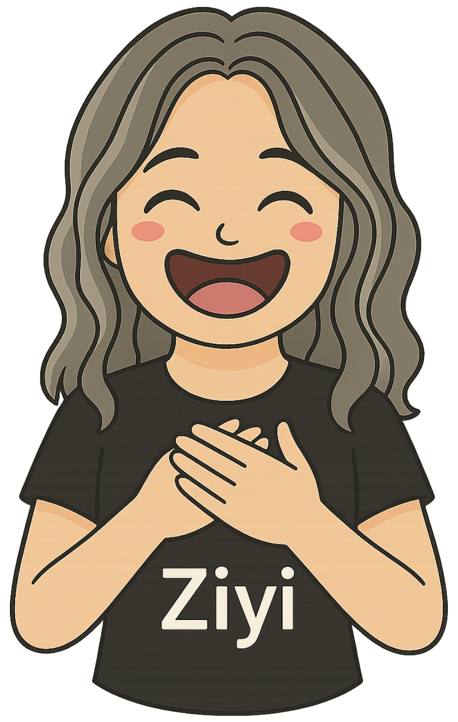
IBCS protocol:
IOP + VC → ARG

Classical Security [CDGS23]

Post-quantum Security

$\Longrightarrow$ **Best** post-quantum secure succinct arguments in the standard model (no oracles)

https://eprint.iacr.org/2025/947



Thank you!

References

[BCS16]: Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. “Interactive Oracle Proofs”. TCC ’16-B.

[CD**G**S23]: Alessandro Chiesa, Marcel Dall’Agnol, **Ziyi Guan**, and Nicholas Spooner. On the Security of Succinct Interactive Arguments from Vector Commitments. ePrint Report 2023/1737.

[CD**G**SY24]: Alessandro Chiesa, Marcel Dall’Agnol, **Ziyi Guan**, Nicholas Spooner, and Eylon Yogev. “Untangling the Security of Kilian’s Protocol: Upper and Lower Bounds”. TCC ’24.

[CDD**G**S24]: Alessandro Chiesa, Marcel Dall’Agnol, Zijing Di, **Ziyi Guan**, and Nicholas Spooner. “Quantum Rewinding for IOP-Based Succinct Arguments”. ePrint Report 2025/947.

[C**G**KY25]: Alessandro Chiesa, **Ziyi Guan**, Christian Knabenhans, Zihan Yu. “On the Fiat–Shamir Security of Succinct Arguments from Functional Commitments”. ePrint Report 2025/902.

[CMS19]: Alessandro Chiesa, Peter Manohar, and Nicholas Spooner. “Succinct Arguments in the Quantum Random Oracle Model”. In: TCC ’19.

[CMSZ21]: Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. “Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier”. FOCS ’21.

[GH97]: Oded Goldreich and Johan Håstad. On the Complexity of Interactive Proofs with Bounded Communication. 1998. Information Processing Letters.

[Kilian92]: Joe Kilian. “A note on efficient zero-knowledge proofs and arguments”. STOC ’92.

[Unr16]: Dominique Unruh. “Computationally binding quantum commitments”. EUROCRYPT ’16.