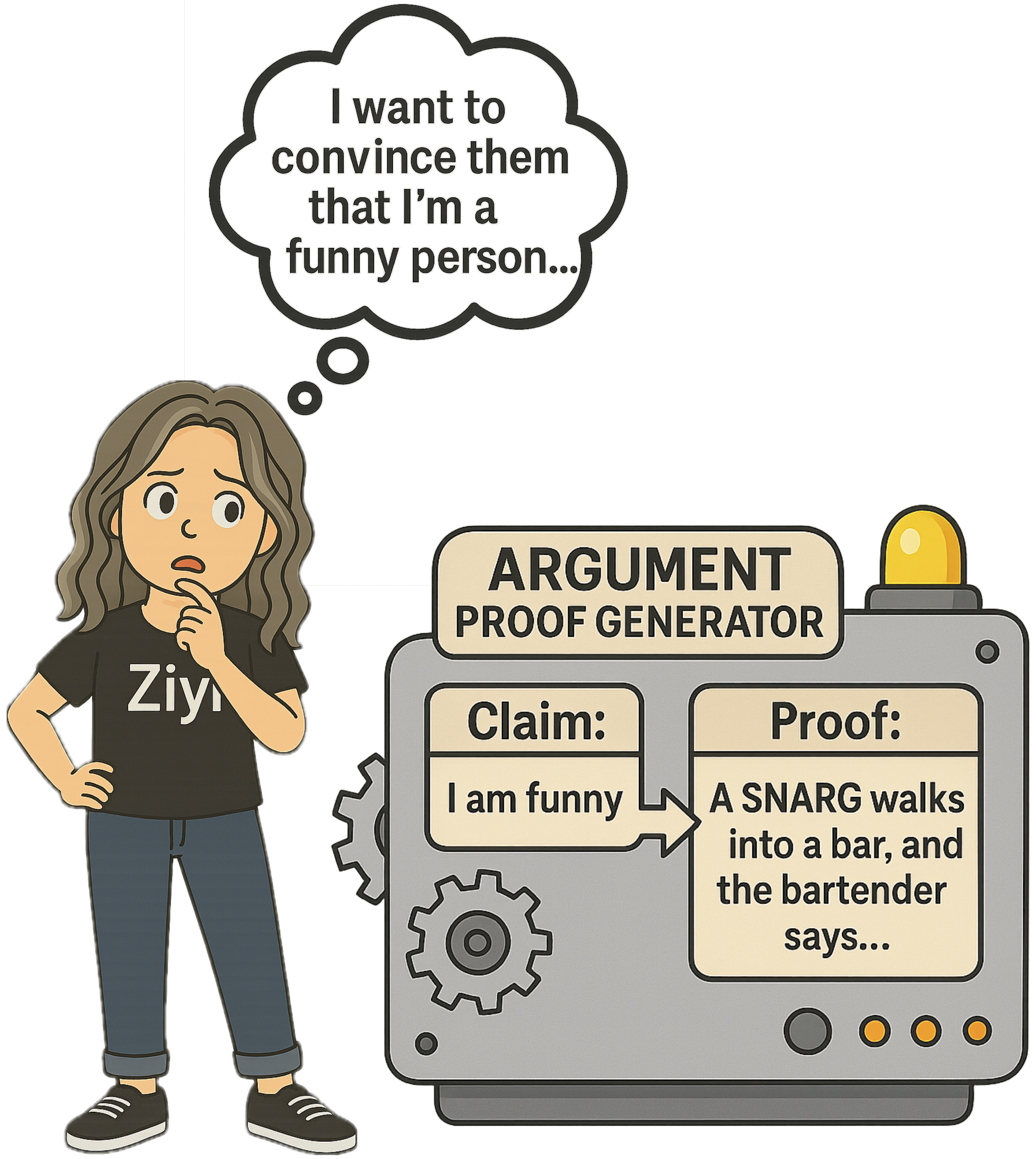
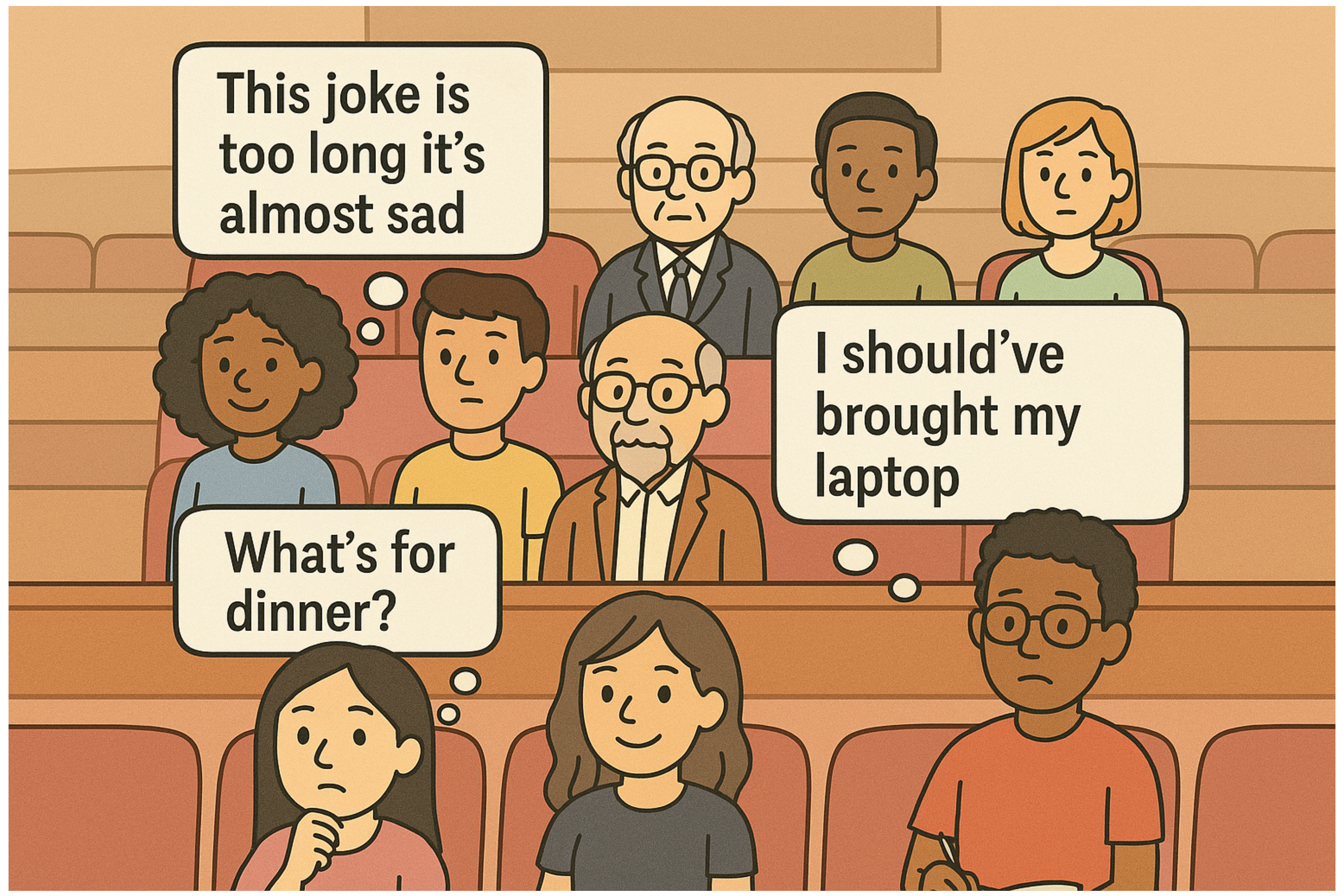
On the Security of Succinct Arguments from Probabilistic Proofs



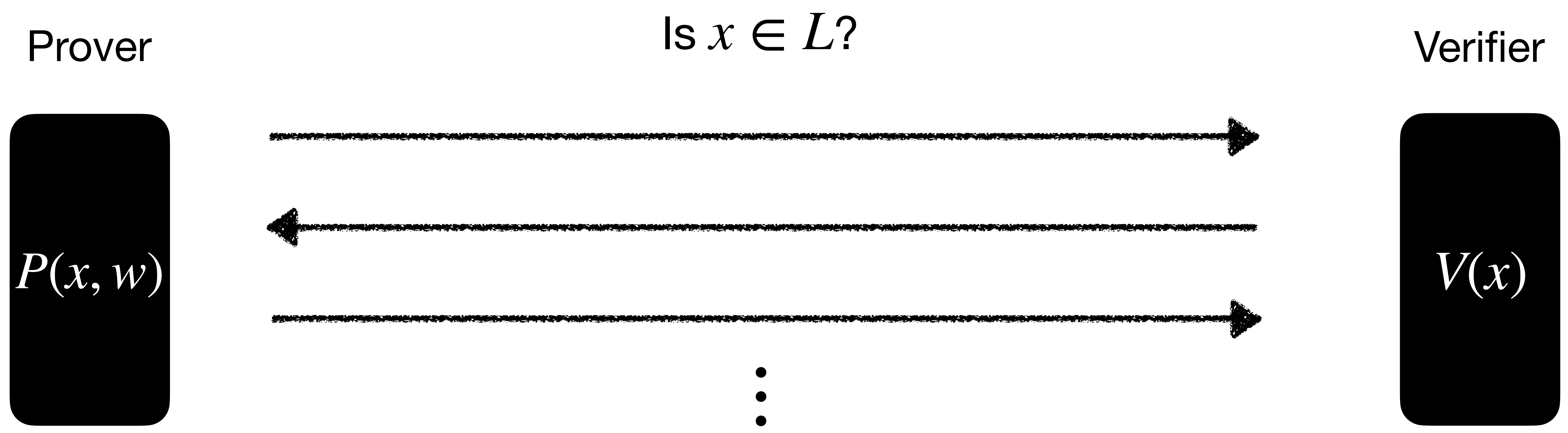
Ziyi Guan



EPFL

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 $\tilde{P}, \Pr\left[\langle \tilde{P}, V(x)\rangle = 1\right] \leq \epsilon$

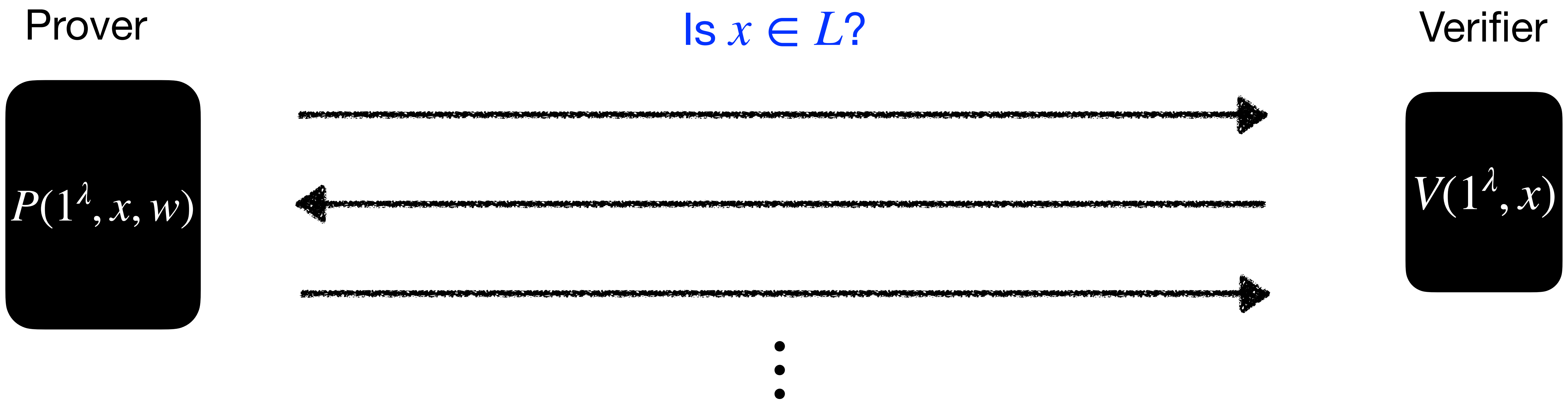
Target metric: **COMMUNICATION COMPLEXITY**

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.

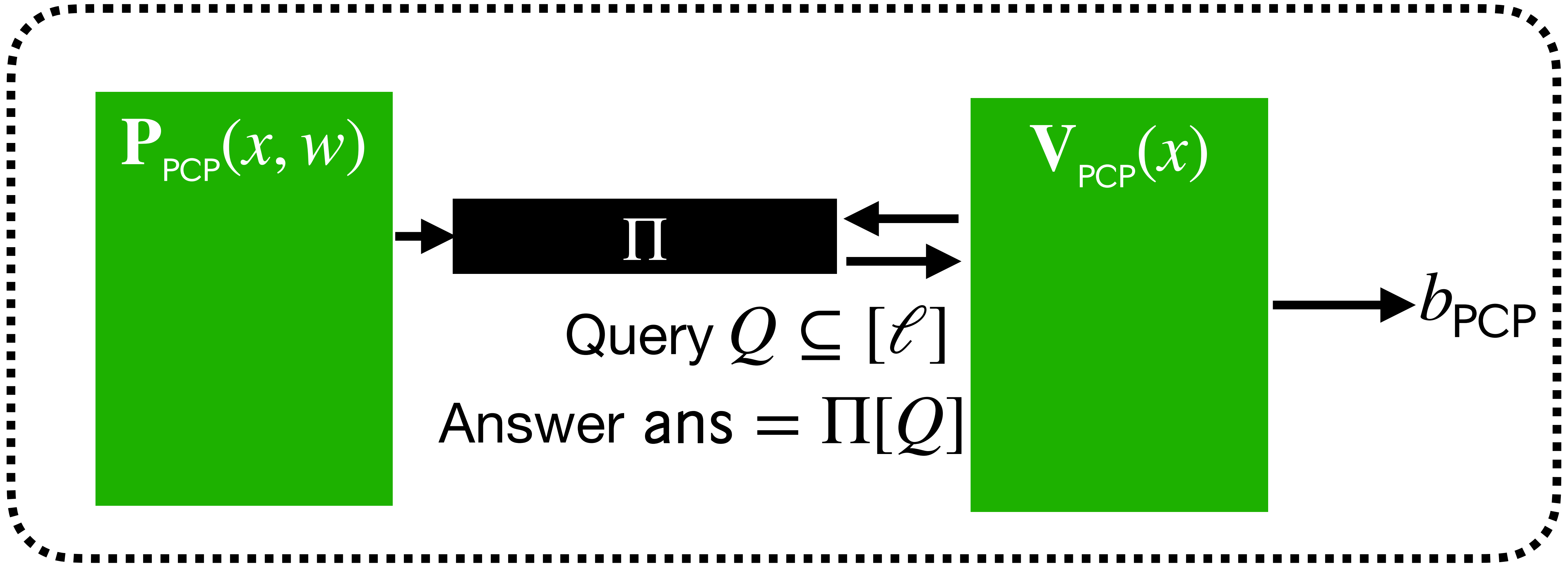
Succinct | RISC ZERO | Aztec | VALIDA | Irreducible

STARKWARE | polygon | NEXUS | Ligero | MatterLabs | ...

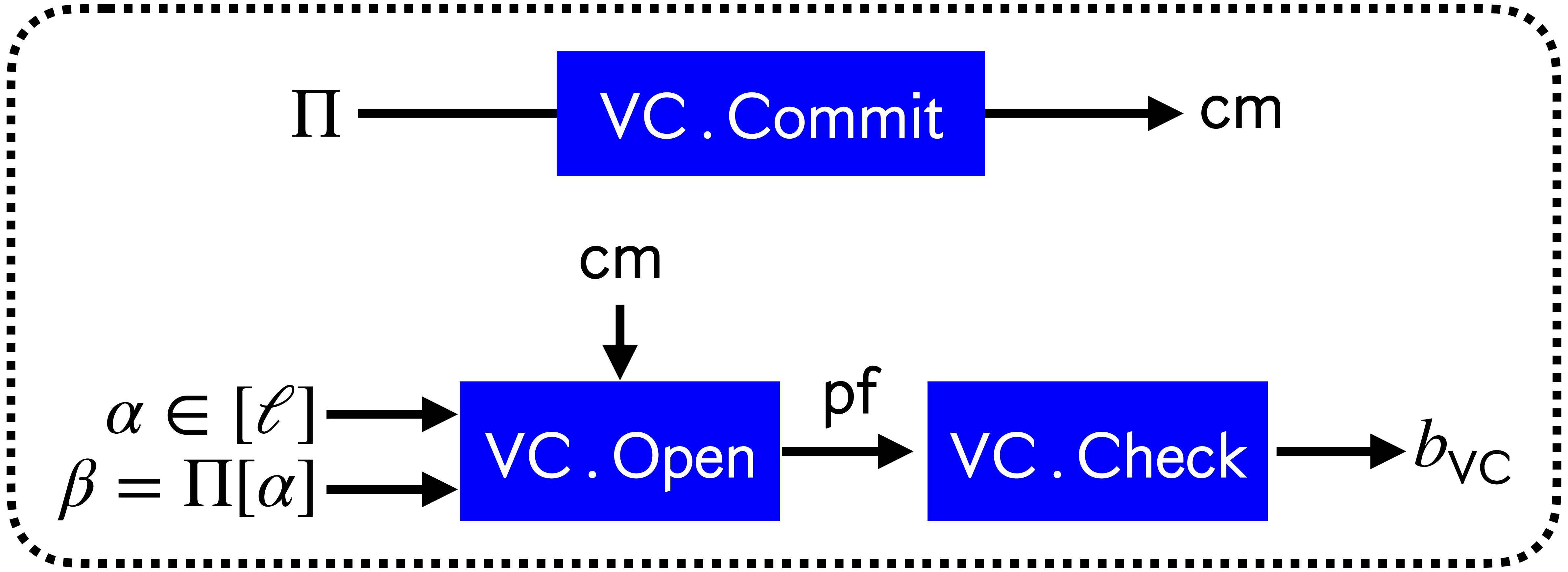
Kilian's protocol:
The first and simplest succinct argument

How to construct succinct arguments?

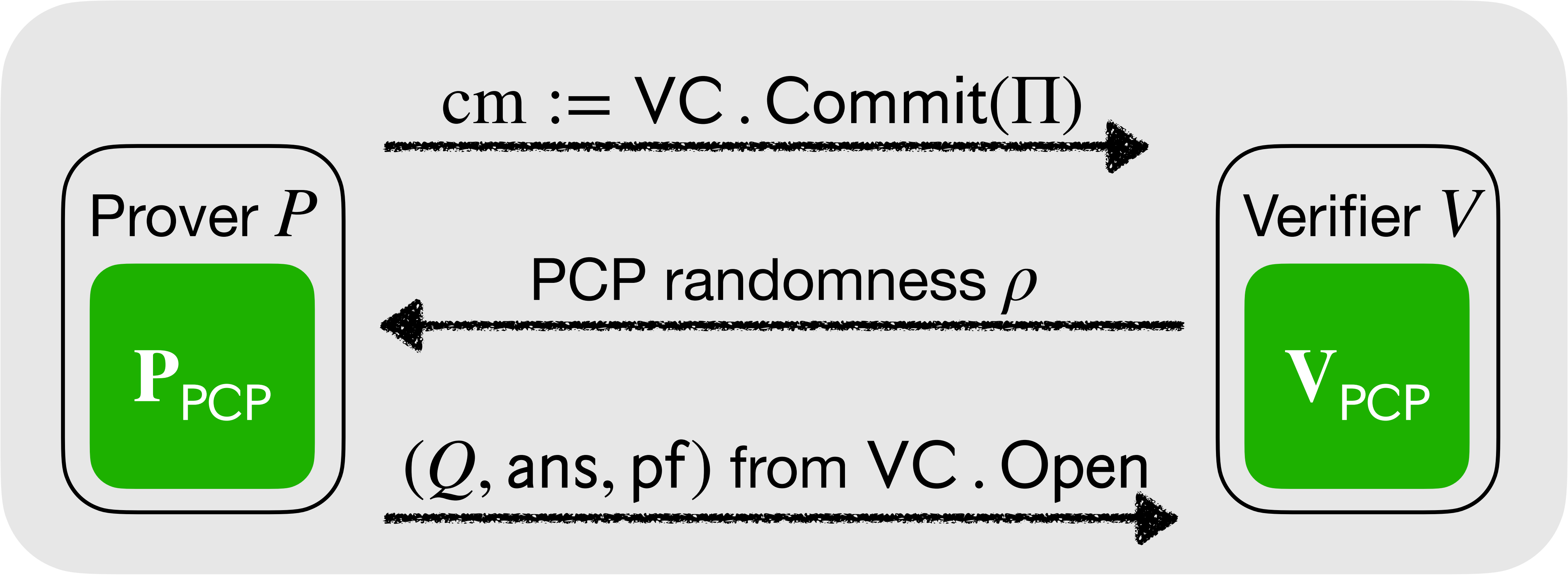
Building block #1: probabilistically checkable proof (PCP)



Building block #2: vector commitment scheme (VC)



Kilian's protocol

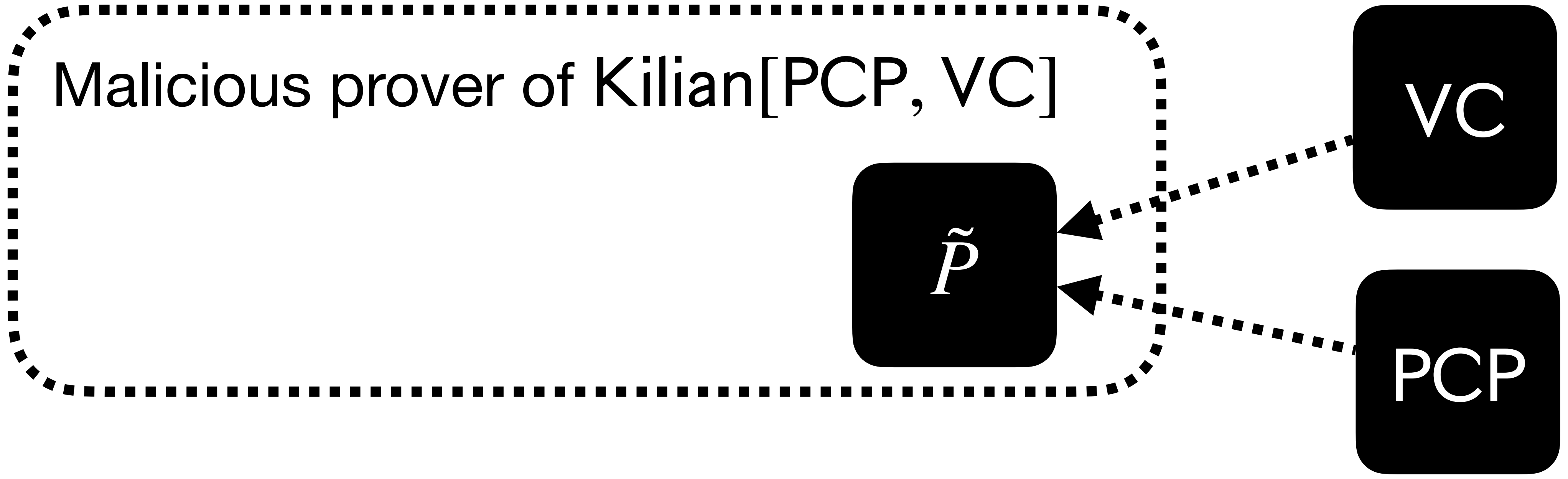


T-step computation:
- Prover time: poly(T)
- Verifier time: polylog(T)

(**CC**: polylog(T))

Simple (and only known) security analysis

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

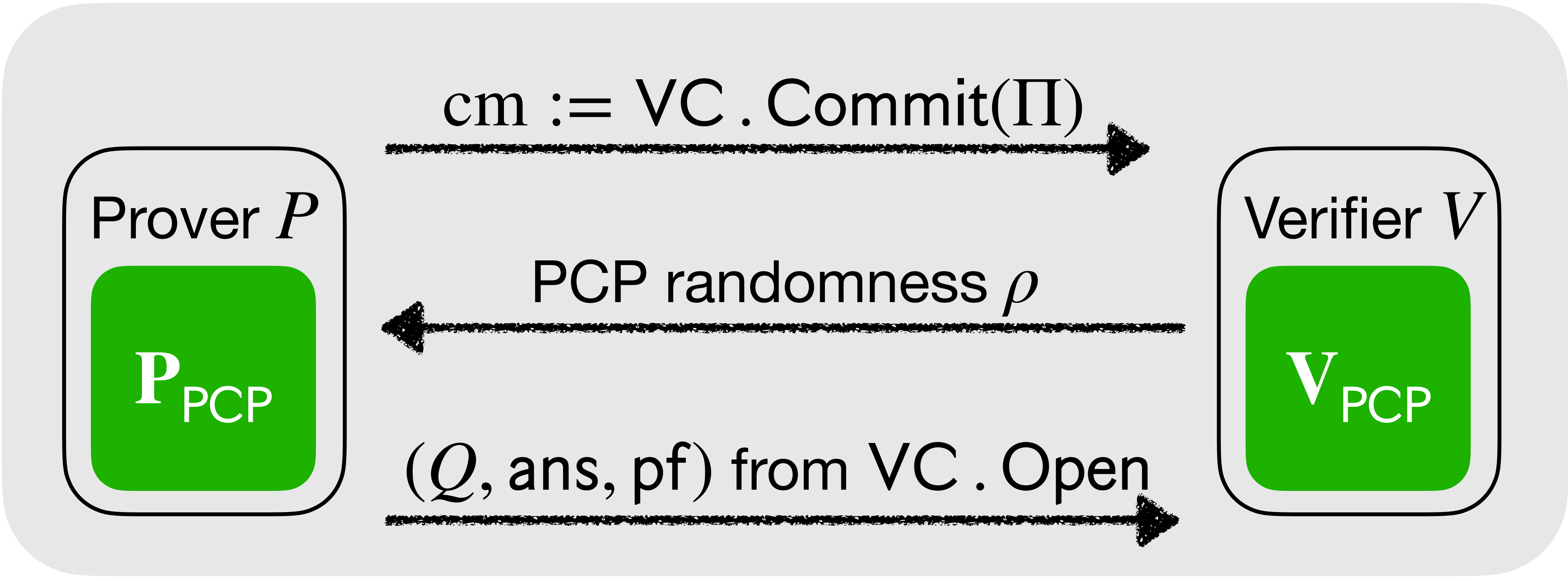


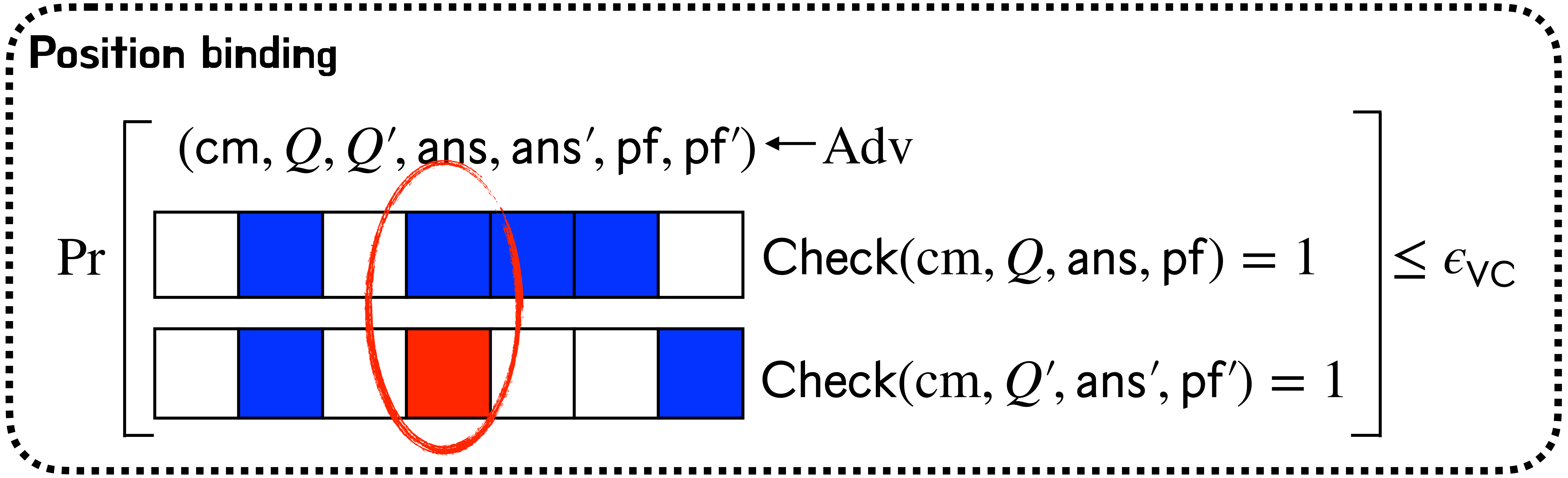
Rewind $\tilde{P}$ to get a malicious PCP string $\tilde{\Pi}$

$\Longrightarrow$ (PCP soundness) upper bound the success probability of $\tilde{\Pi}$

$\Longrightarrow$ (Position binding) $\tilde{\Pi}$ cannot be too different from $\tilde{P}$

Kilian's protocol



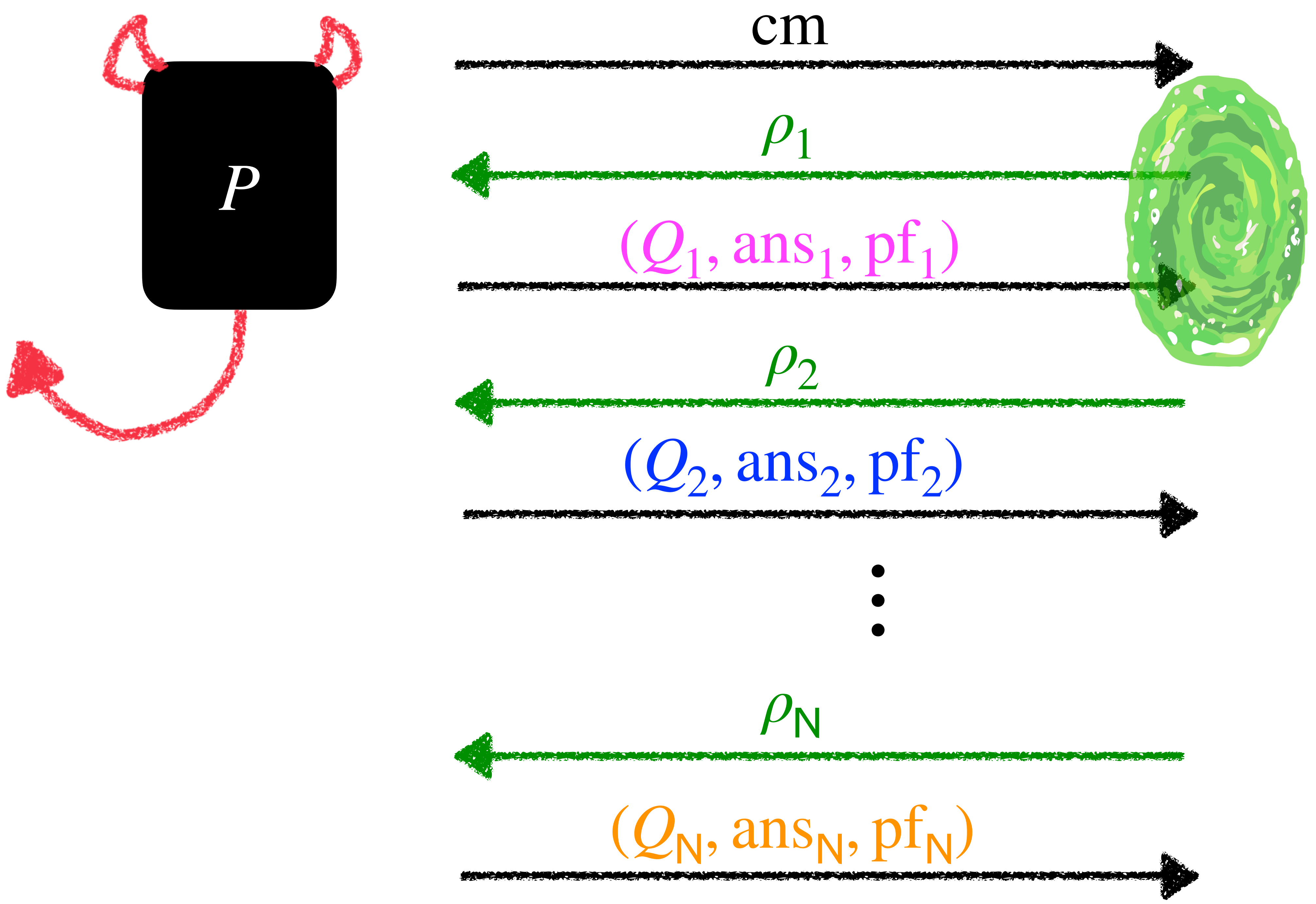


Security from rewinding

How to rewind?

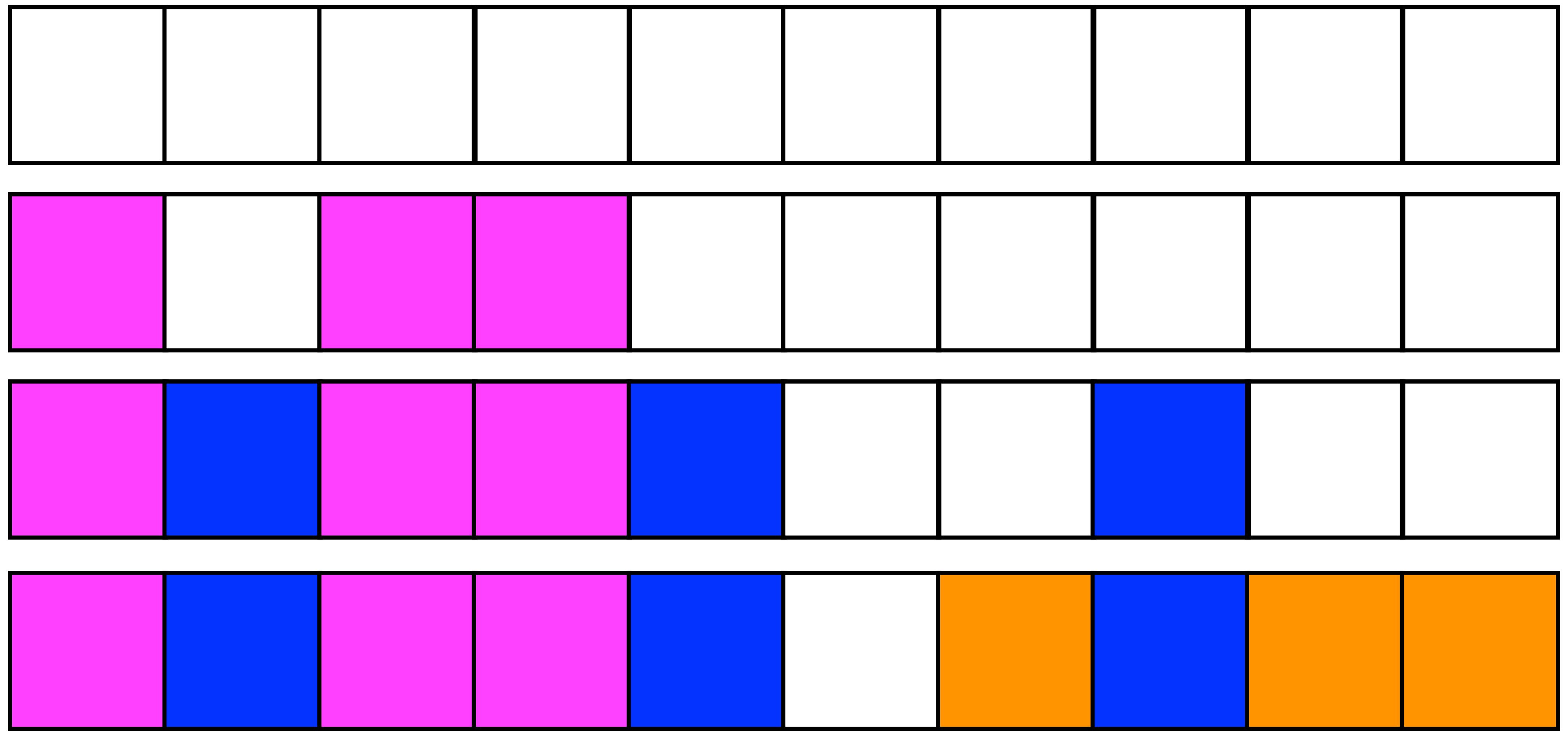
Malicious Prover $\tilde{P}$

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

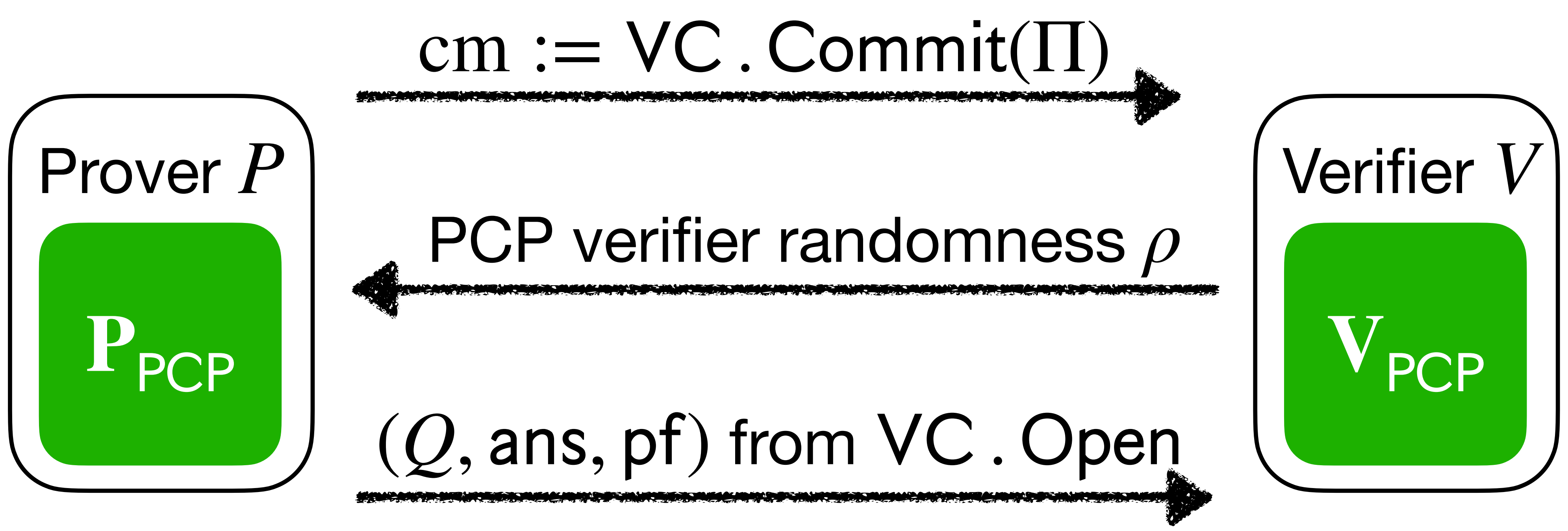


Subtle design choices:
- Strict time vs. expected time
- Sample with/without replacement
- Stopping conditions
- …

Recover $\tilde{\Pi}$



What is the security of Kilian's protocol?



Previously:

non-trivial restrictions

- [Kilian92] gives an informal analysis
- [BG08] $\epsilon_{\mathsf{ARG}} \leq 8 \cdot \epsilon_{\mathsf{PCP}} + \sqrt[3]{\epsilon_{\mathsf{VC}}}$ and **assuming** PCP is non-adaptive & reverse-samplable
- [CMSZ21] Kilian is secure when ϵ_{PCP} negligible (in a paper about post-quantum security)

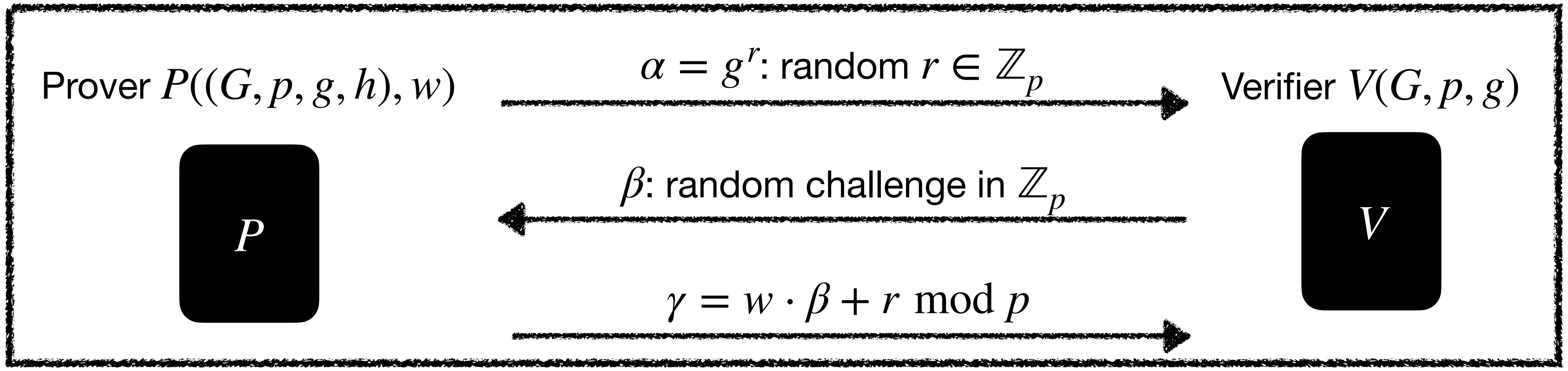
We expect that $\epsilon_{\mathsf{ARG}} \leq \epsilon_{\mathsf{PCP}} + \epsilon_{\mathsf{VC}}$ ... right?

Surprise! A limitation:

$\epsilon_{\text{ARG}} \leq \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}$
$\implies$ **breakthrough on Schnorr**

More on this later...

Schnorr's identification scheme



Lots of work on Schnorr security [Sho97,PS00,BP02,FPS20,BD20,RS21,SSY23] ...
... and yet there are still open questions on its optimal security!

Theorem. $\exists$ PCP and VC s.t.

$$\epsilon_{\text{Schnorr}}(t) \leq \epsilon_{\text{ARG}}(t).$$

Similar bound holds for expected-time adversary

Improved security for Kilian

PCP for language L with
- proof length l
- query complexity q
- soundness error ϵ_{PCP}

$\longrightarrow$ ARG := Kilian[PCP, VC] $\longleftarrow$

Vector commitment scheme with position binding error ϵ_{VC}

Theorem. $\forall\, \epsilon > 0$,

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

This seems large…
Can we improve it?

Why $l \cdot 1/\epsilon$ overhead?
- l locations in Π

$\Longrightarrow$ Rewind at least l times (e.g. maybe all PCP queries but 1 are fixed)
- Some rewinds yield garbage:
  - The locations were already found
  - VC check fails

$\Longrightarrow$ Need $1/\epsilon$ times for each location as buffer

Folklore may remain legend for now...

$\epsilon_{\text{ARG}} \le \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}$

$\implies$ breakthrough on Schnorr!

λ: security parameter

Suppose $\epsilon_{\text{VC}}(t) \le O(t^2/2^\lambda)$ (e.g. an ideal Merkle tree)

By **Theorem**: $\epsilon_{\text{ARG}}(t_{\text{ARG}}) \le \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}(t_{\text{ARG}} \cdot l/\epsilon) + \epsilon \le \epsilon_{\text{PCP}} + l^{2/3} \cdot O\left(\sqrt[3]{t_{\text{ARG}}^2/2^\lambda}\right)$

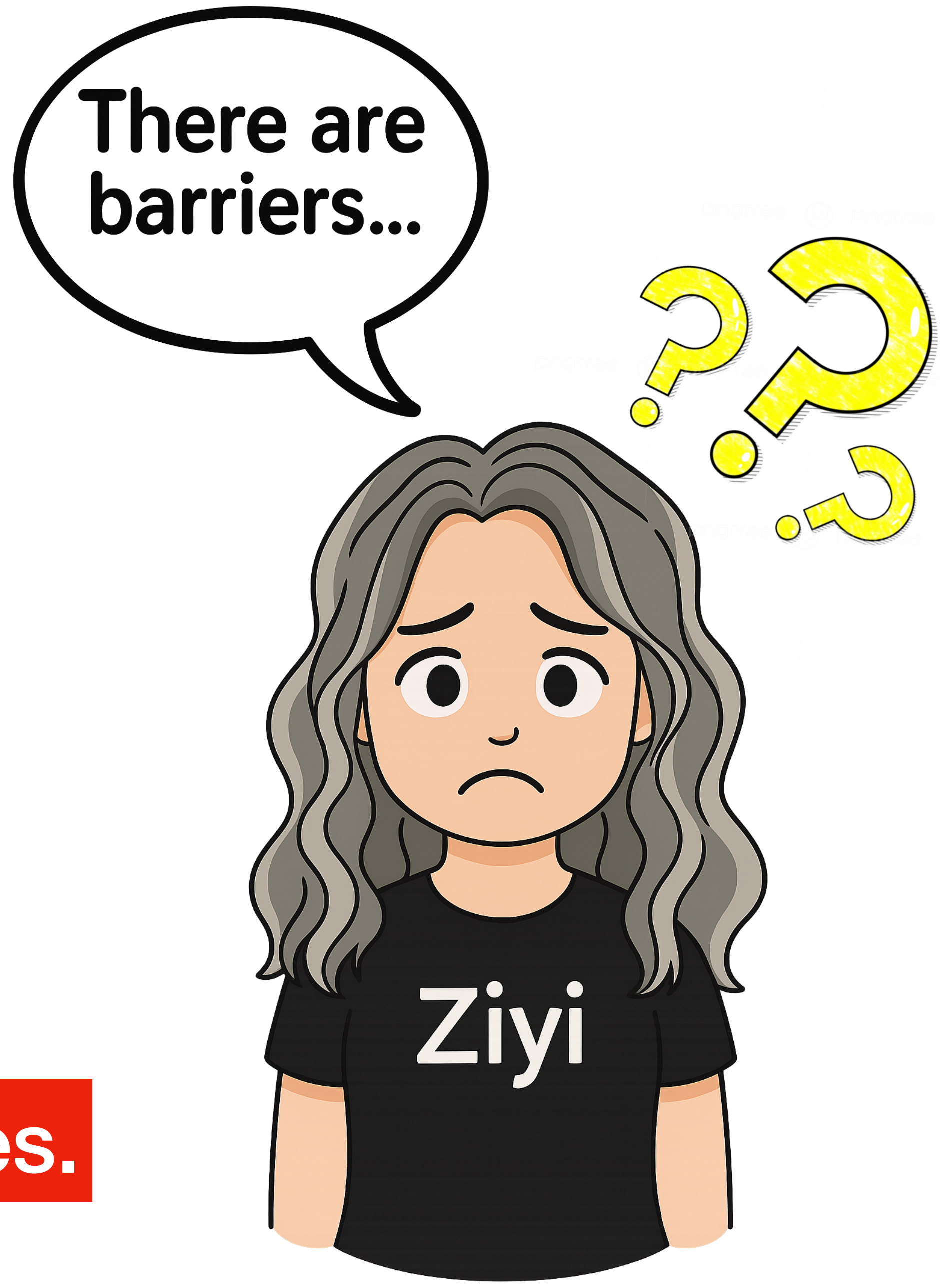
That is, $\epsilon_{\text{ARG}} \le \epsilon_{\text{PCP}} + \sqrt[3]{\epsilon_{\text{VC}}}$

Our lower bound		Suppose
$\epsilon_{\text{Schnorr}}(t) \le \epsilon_{\text{ARG}}(t)$	+	$\epsilon_{\text{ARG}} \le \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}$

$\implies$ $\epsilon_{\text{Schnorr}}(t_{\text{Schnorr}}) \le \epsilon_{\text{DLOG}}(O(t_{\text{Schnorr}}))$

Best analysis of Schnorr [PS00]: $\epsilon_{\text{Schnorr}}(t_{\text{Schnorr}}) \le \sqrt{\epsilon_{\text{DLOG}}(O(t_{\text{Schnorr}}))}$

... so the folklore is beyond current rewinding techniques.



Alternative route: expected-time regime

PCP for language L with
- proof length l
- query complexity q
- soundness error ϵ_{PCP}

$\rightarrow$ ARG := Kilian[PCP, VC] $\leftarrow$

Vector commitment scheme with expected-time position binding error $\epsilon^{\star}_{\mathsf{VC}}$

Theorem. $\forall\, \epsilon > 0$,

$$\epsilon^{\star}_{\mathsf{ARG}}(t^{\star}_{\mathsf{ARG}}) \leq \epsilon_{\mathsf{PCP}} + \epsilon^{\star}_{\mathsf{VC}}(t^{\star}_{\mathsf{VC}}) + \epsilon, \text{ where } t^{\star}_{\mathsf{VC}} = O\left(t^{\star}_{\mathsf{ARG}} \cdot \log(\mathsf{q}/\epsilon)\right).$$

λ: security parameter

Set $\epsilon^{\star}_{\mathsf{VC}}(t^{\star}) \leq O\left(\sqrt{(t^{\star})^2/2^{\lambda}}\right)$ (e.g. an ideal Merkle tree)

Theorem $\Longrightarrow$

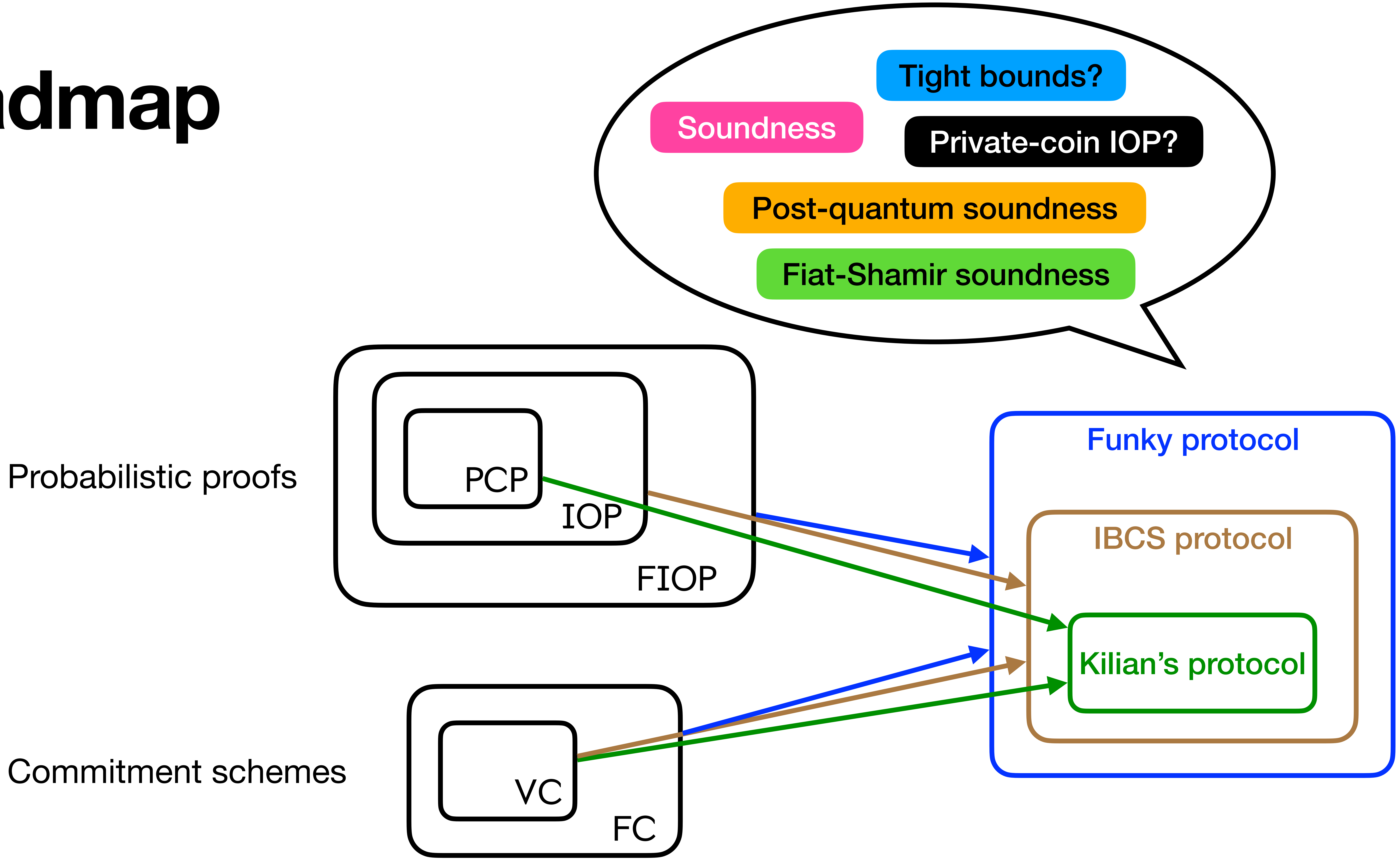
$$\epsilon^{\star}_{\mathsf{ARG}}(t^{\star}_{\mathsf{ARG}}) \leq \epsilon_{\mathsf{PCP}} + \epsilon^{\star}_{\mathsf{VC}}(t^{\star}_{\mathsf{ARG}} \cdot \log(\mathsf{q}/\epsilon)) + \epsilon$$

$$\leq \epsilon_{\mathsf{PCP}} + \mathsf{polylog}\left(\mathsf{q} \cdot \sqrt{(t^{\star}_{\mathsf{ARG}})^2/2^{\lambda}}\right) \cdot O\left(\sqrt[2]{(t^{\star}_{\mathsf{ARG}})^2/2^{\lambda}}\right)$$

small factor

We achieved $\epsilon^{\star}_{\mathsf{ARG}} \leq \epsilon_{\mathsf{PCP}} + \epsilon^{\star}_{\mathsf{VC}}$!

Roadmap



Today: only in the standard model (no oracles)
i.e. interactive arguments in (Q)ROM out of scope

On security notions of arguments

Today: focus on soundness only

Classical | Post-quantum

Soundness

Fiat-Shamir soundness

Post-quantum soundness

Actually: many properties/nuances to care about

Knowledge soundness

Fiat-Shamir knowledge soundness

Post-quantum knowledge soundness

...

Simulation extractability

...

Zero knowledge

...

Ethereum Unlocks Millions To Prepare For The Post-quantum Era

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

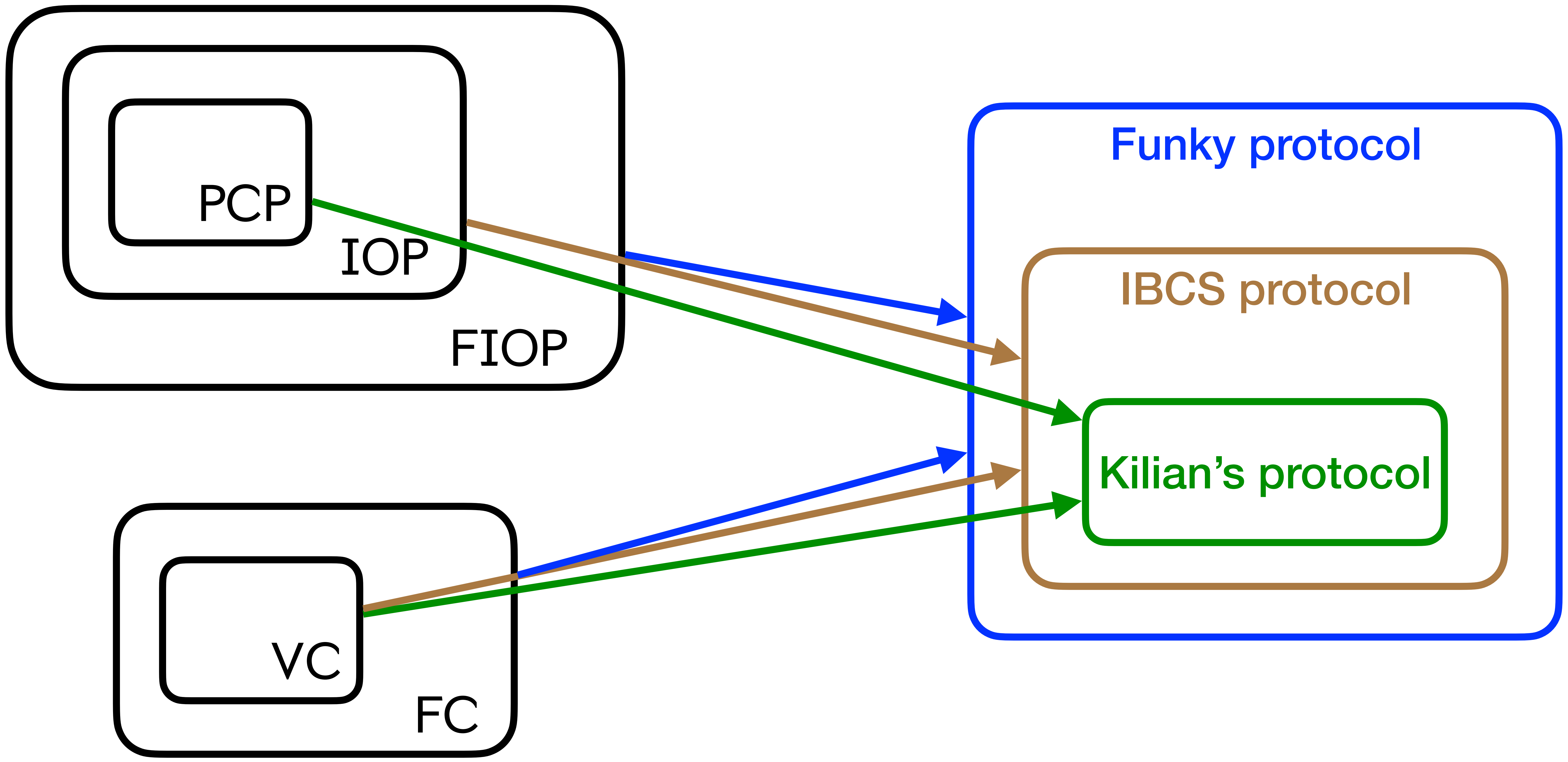
Strict-time adversary
vs.
Expected-time adversary

e.g., [BL02] zero-knowledge protocols do not have strict poly-time (black-box) extractor

zkEVM Formal Verification Project

A project by the Ethereum Foundation to accelerate the application of formal verification methods to zkEVMs

IBCS protocol:
Using IOPs instead of PCPs

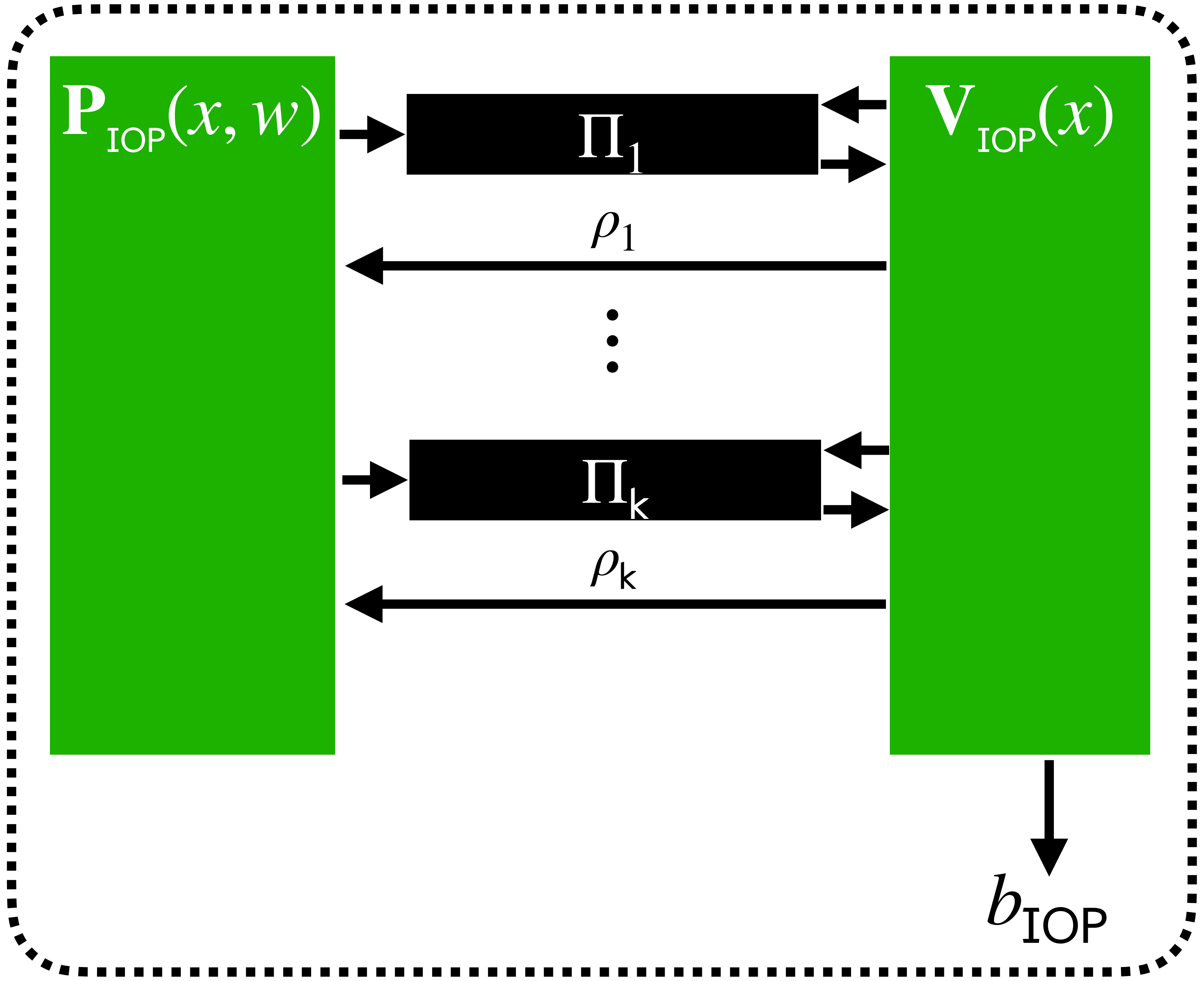


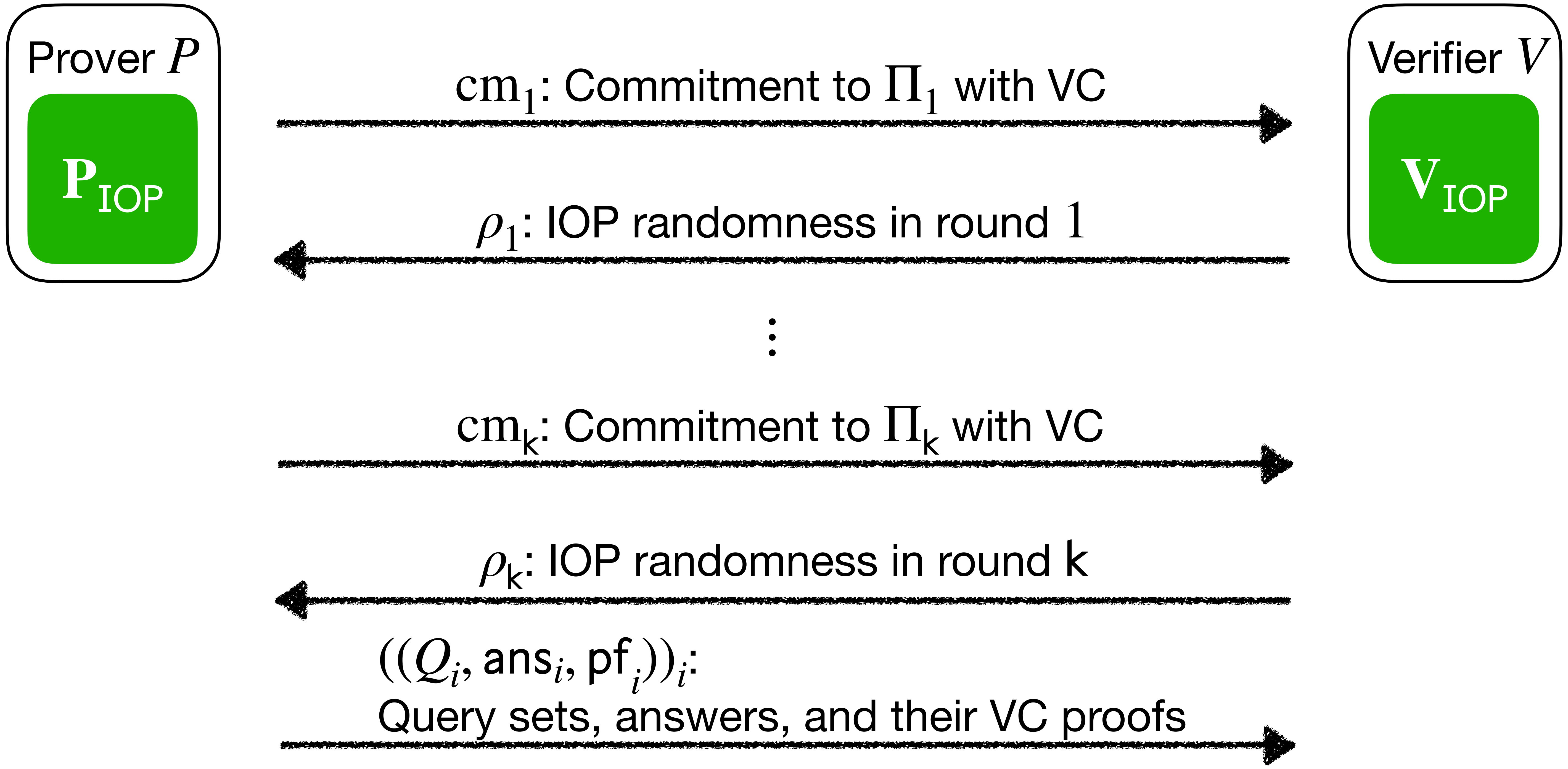
IBCS protocol

Existing PCPs are not concretely efficient: prover time too big

People use IOPs

Public-coin interactive oracle proof (IOP)





Security of IBCS protocol

Public-coin IOP for language L with
- proof length l
- query complexity q
- round complexity k
- soundness error ϵ_{IOP}

→ ARG := IBCS[IOP, VC] ←

Vector commitment scheme with position binding error ϵ_{VC}

The ideal bound $\cancel{\epsilon_{\text{ARG}} \leq \epsilon_{\text{IOP}} + \epsilon_{\text{VC}}}$ is not possible… What can we get?

Theorem. $\forall\, \epsilon > 0$,

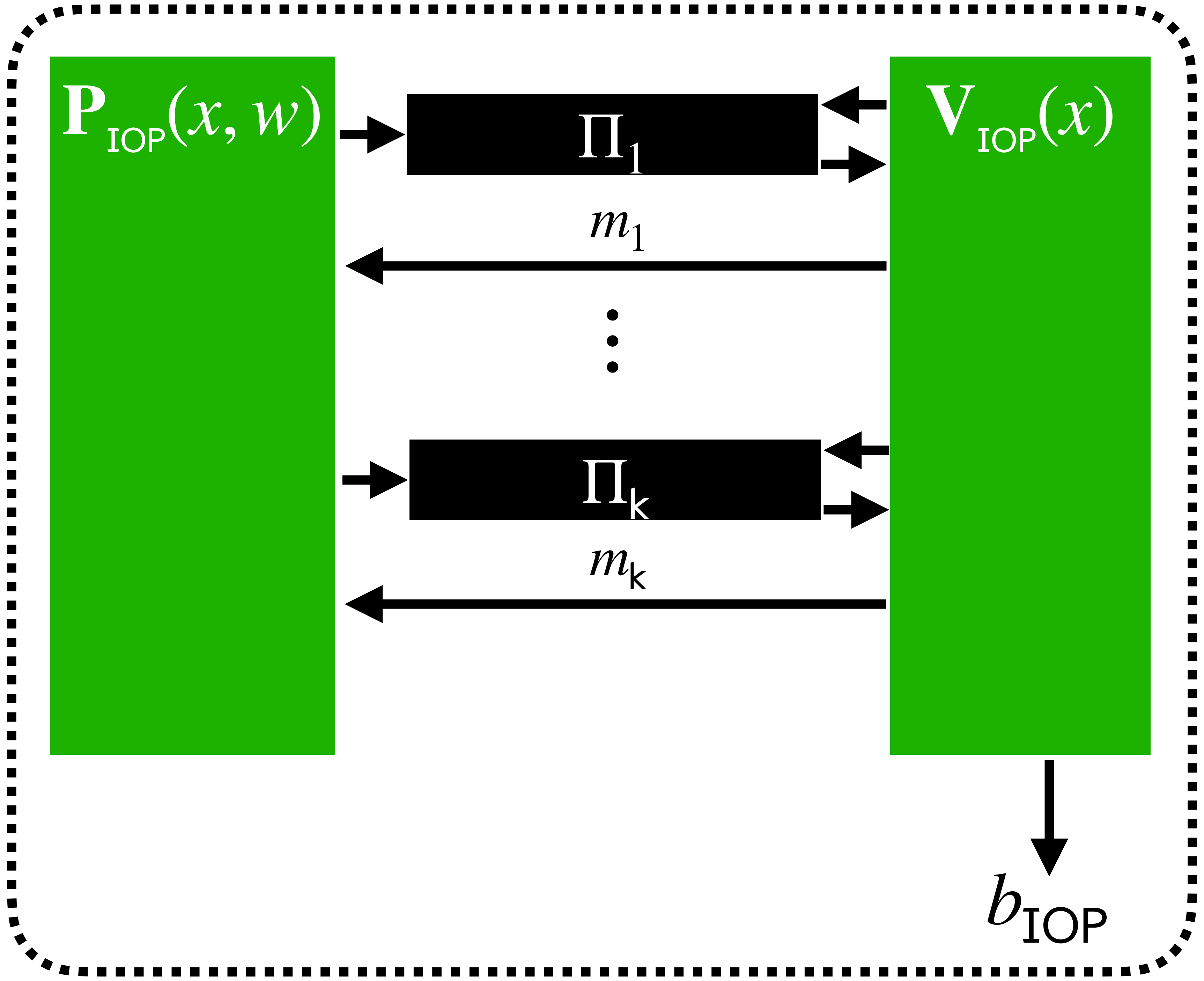
$$\epsilon_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{IOP}} + \text{k} \cdot \epsilon_{\text{VC}}(t_{\text{VC}}) + \epsilon, \text{ where } t_{\text{VC}} = O\left(t_{\text{ARG}} \cdot l/\epsilon\right).$$

Recall, for Kilian's protocol: $\forall\, \epsilon > 0$,

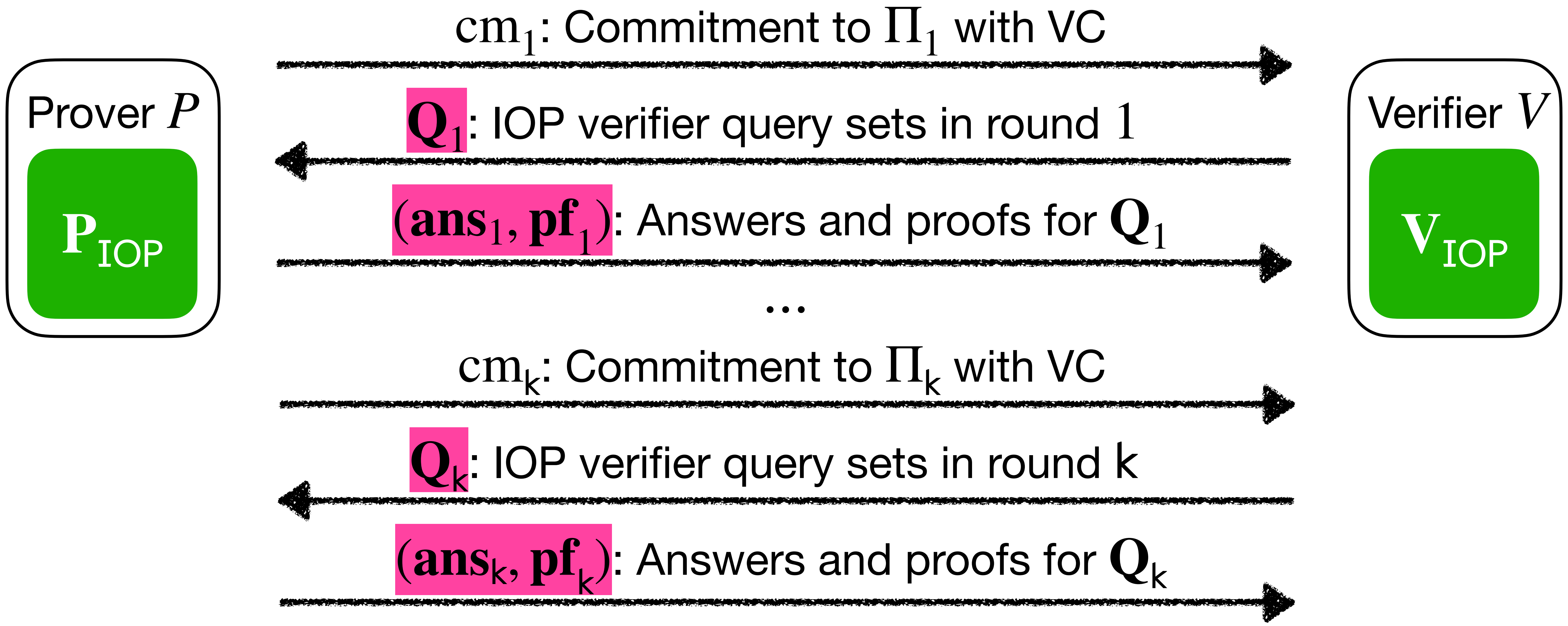
$$\epsilon_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{PCP}} + 1 \cdot \epsilon_{\text{VC}}(t_{\text{VC}}) + \epsilon, \text{ where } t_{\text{VC}} = O\left(t_{\text{ARG}} \cdot l/\epsilon\right).$$

Why do we need public-coin IOPs?

Private-coin interactive oracle proof (IOP)



$\mathbf{Q}_i$ contains verifier's queries to $\Pi_1, \ldots, \Pi_i$



Not secure!
e.g. IOP verifier accepts if IOP prover guesses all its queries

How about public-query IOPs?

Queries can be learned by the prover (in "real-time")

Clearly, the IBCS protocol is secure whenever the underlying IOP is public-query... right?

Lemma: secure if IOP has an "efficient random continuation sampler"

Open question: can we prove security for ALL public-query IOPs?
(Or maybe there is a black-box barrier?)

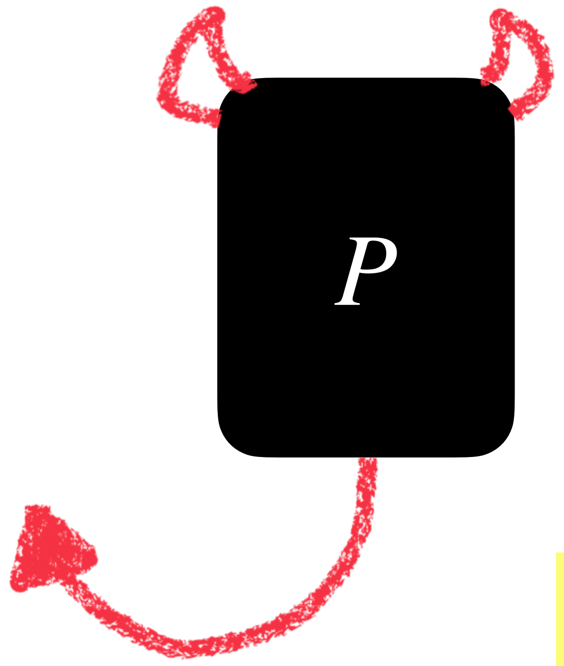
Interlude: post-quantum security

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

$$\forall\ t_{\text{ARG}}\text{-time } \textbf{QUANTUM} \text{ adversary } \tilde{P},\ \Pr\left[\langle \tilde{P}, V\rangle = 1\right] \leq \epsilon_{\text{ARG}}(t_{\text{ARG}})$$

On quantum rewinding

Malicious Prover $\tilde{P}$



Prover state $|\phi\rangle$

cm

ρ_1

Prover state $|\phi'\rangle$

$(Q_1, \mathrm{ans}_1, \mathrm{pf}_1)$

Measure!

ρ_2

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

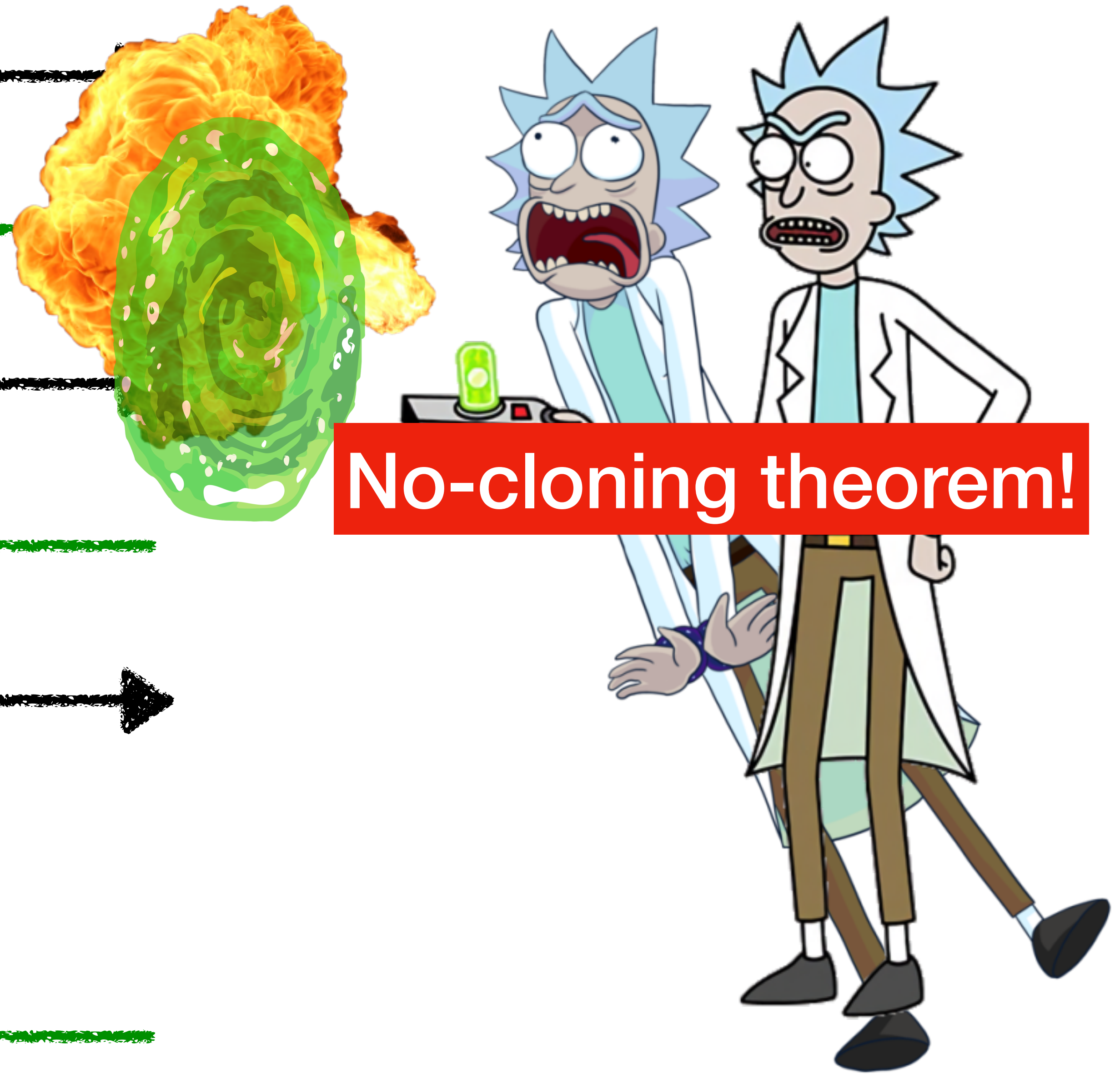
$(Q_2, \mathrm{ans}_2, \mathrm{pf}_2)$

⋮

ρ_N

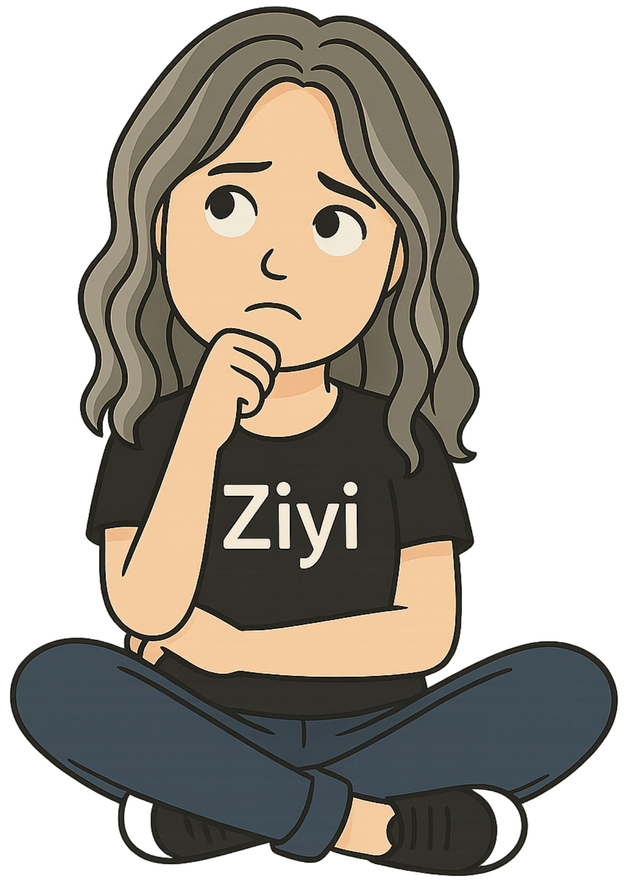
$(Q_\mathrm{N}, \mathrm{ans}_\mathrm{N}, \mathrm{pf}_\mathrm{N})$

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



No-cloning theorem!

But rewinding is everywhere in crypto, how did people prove anything without it?



For many years: can rewind O(1) times [Wat06,Unr12,Unr16b]

Problem: Kilian's protocol needs many rewindings

Recent new tools for quantum rewinding [CMSZ21]: "repair" the state instead of "rewind"
$\Longrightarrow$ post-quantum security of Kilian's protocol

- Quantum rewinding toolset is cumbersome.
- Only other paper studying many-round interactive arguments [LMS22] had to white-box adapt the tools in [CMSZ21]… (work for log rounds)

Adapting for IBCS protocol runs into challenges

Post-quantum security of IBCS protocol

IOP is statistically sound
Post-quantum already

IOP for language L with
- proof length l
- query complexity q
- round complexity k
- soundness error ϵ_{IOP}

ARG := IBCS[IOP, VC]

Quantum analogue of
position binding

Vector commitment scheme with collapsing error $\epsilon_{\mathrm{VCCollapse}}$

Technical contribution: We build on [CMSZ21] and more…

Theorem. $\forall\, \epsilon > 0$,

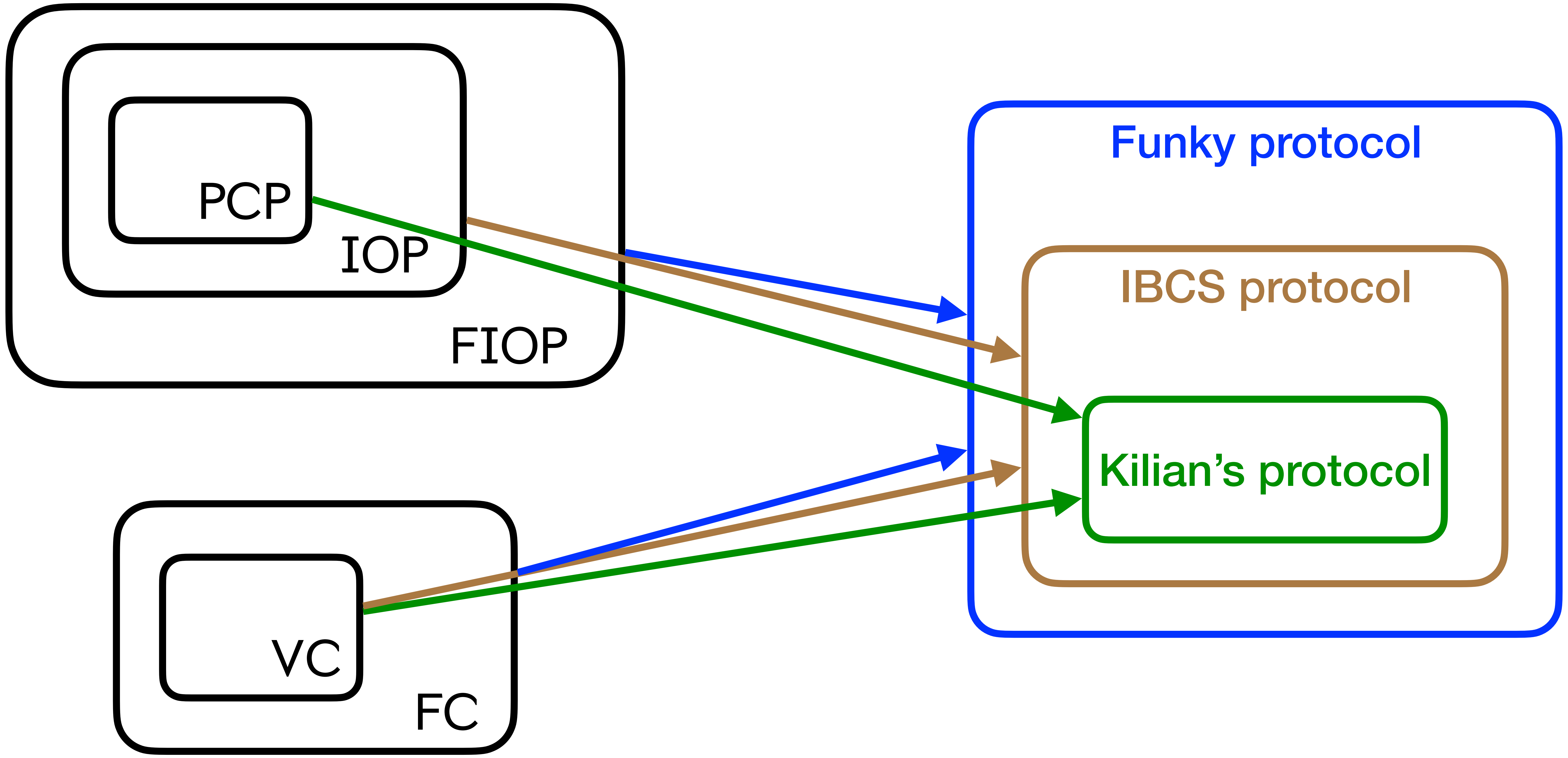
$$\epsilon^{\mathrm{PQ}}_{\mathrm{ARG}}(t_{\mathrm{ARG}}) \leq \epsilon_{\mathrm{IOP}} + \mathsf{k} \cdot l \cdot \epsilon_{\mathrm{VCCollapse}}(t_{\mathrm{VC}}) + \epsilon, \text{ where } t_{\mathrm{VC}} = \mathrm{poly}\left(t_{\mathrm{ARG}} \cdot l/\epsilon\right).$$

Extra l factor: cost of quantum rewinding

IBCS soundness: $\epsilon_{\mathrm{ARG}}(t_{\mathrm{ARG}}) \leq \epsilon_{\mathrm{IOP}} + \mathsf{k} \cdot \epsilon_{\mathrm{VC}}(t_{\mathrm{VC}}) + \epsilon$, where $t_{\mathrm{VC}} = O\left(t_{\mathrm{ARG}} \cdot l/\epsilon\right)$.

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

Funky protocol:
Construction from all probabilistic proofs

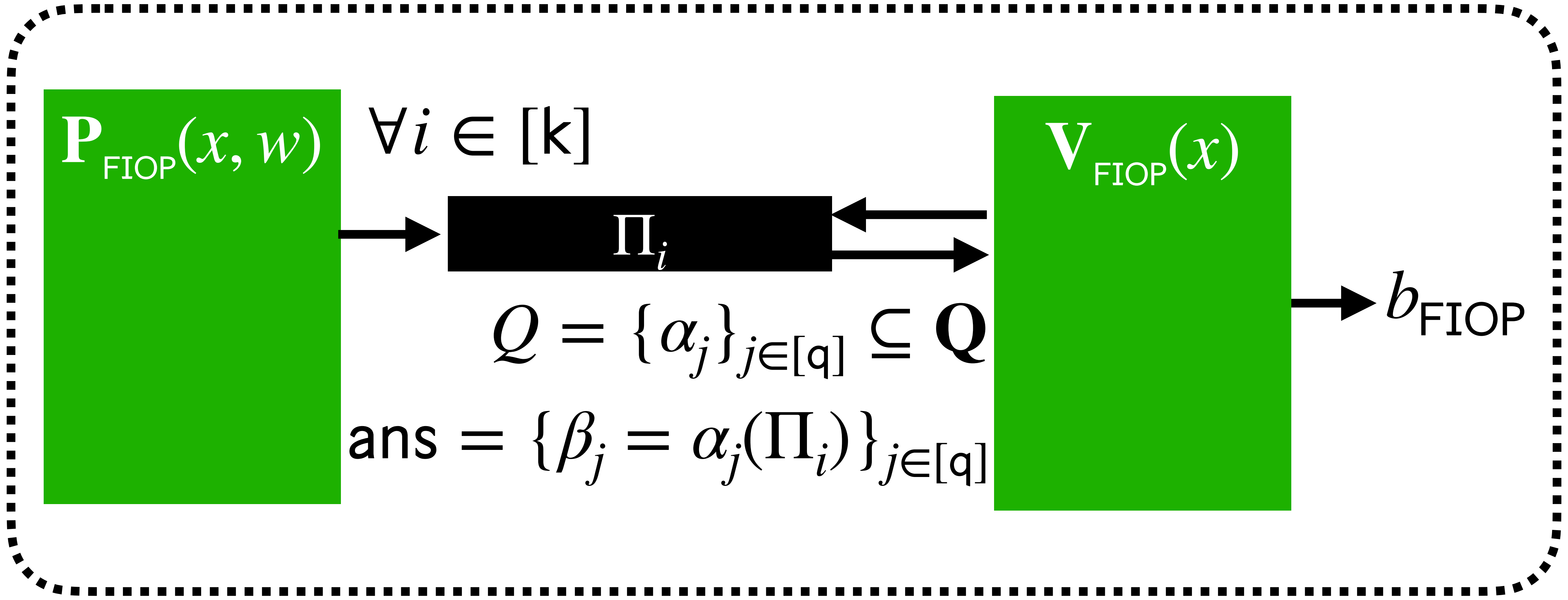


Building blocks

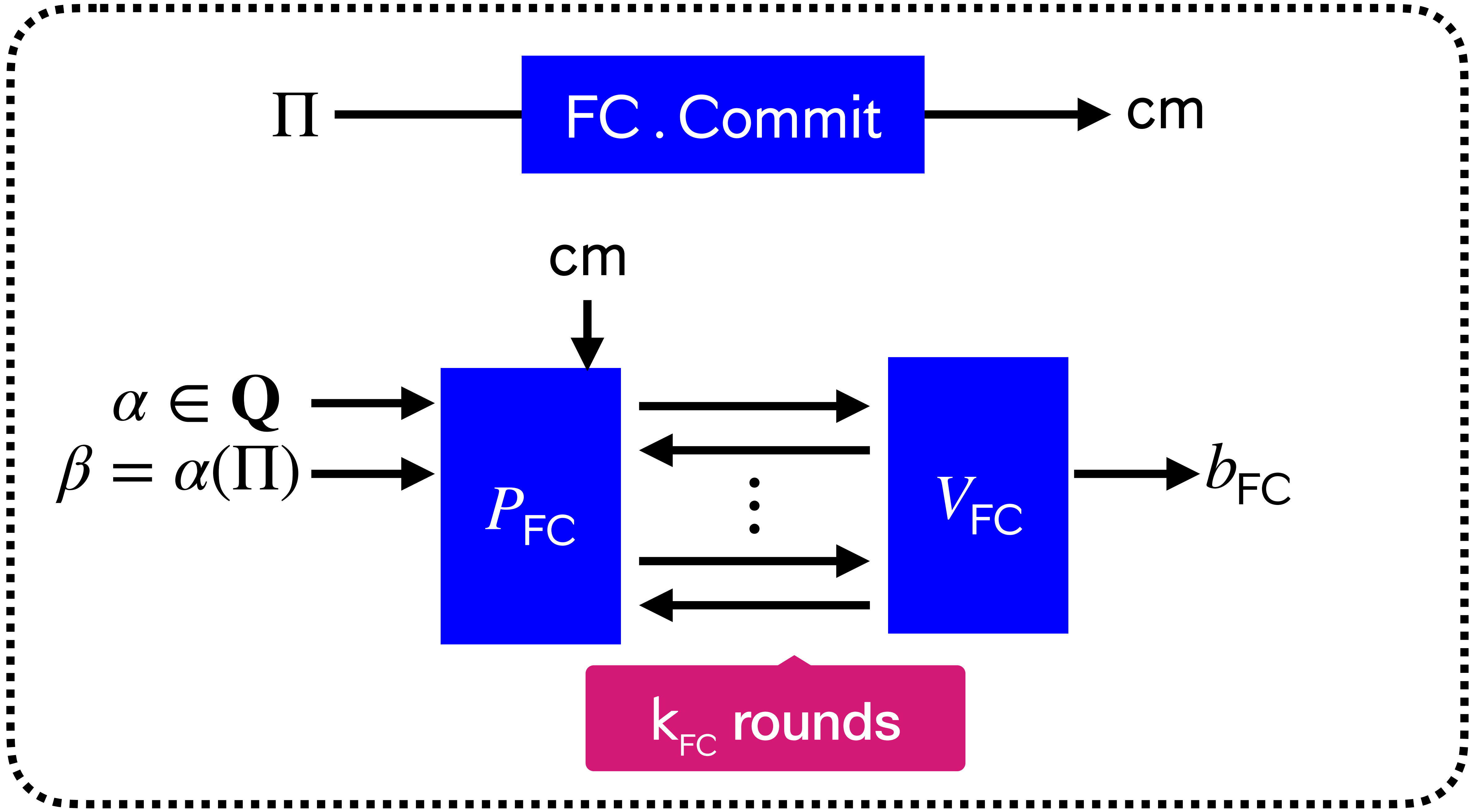
Building block #1: query class $\mathbf{Q}$

- $\mathbf{Q} \subseteq \{\alpha\colon \Sigma^{\ell} \to \mathbb{D}\}$

Building block #2: functional interactive oracle proof (FIOP)

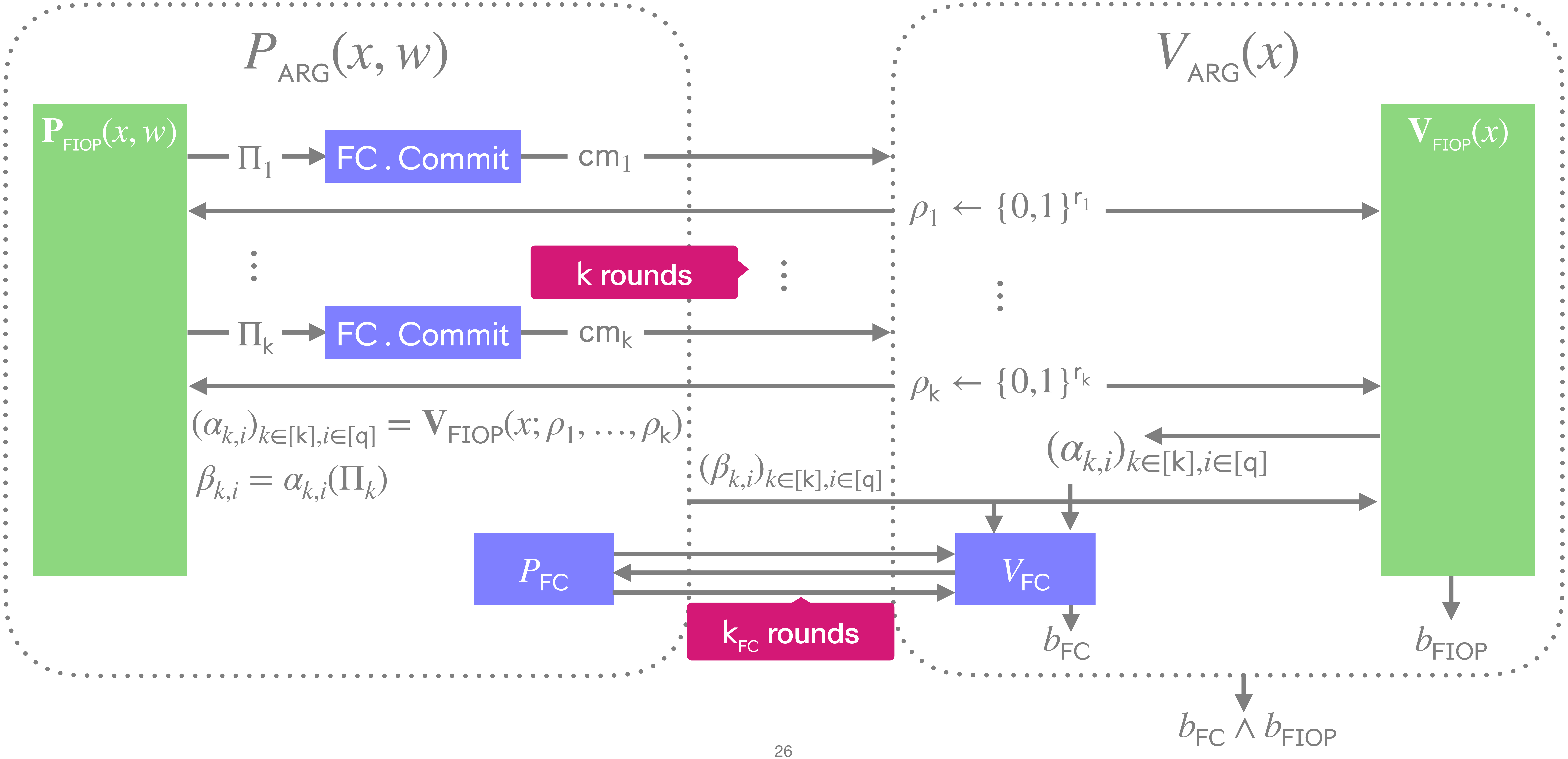


Building block #3: functional commitment scheme (FC)



[CGKY25]

Funky protocol



Special cases of the Funky protocol

	Proof string	Query class	Answer
PCP+VC [Kilian92] **IOP+VC** [BCS16,CDGS23]	$\Pi \in \Sigma^{\ell}$	point queries $\mathbf{Q}_{\text{point}}$	$\beta = \Pi[\alpha]$ for $\alpha \in [\ell]$
LPCP+LC [LM19]	$\Pi \in \mathbb{F}^{\ell}$	linear queries $\mathbf{Q}_{\text{lin}}$	$\beta = \sum_{i \in [\ell]} \Pi[i] \cdot \alpha[i]$ for $\alpha \in \mathbb{F}^{\ell}$
PIOP+PC [CHM+20,BFS20]	$\Pi \in \mathbb{F}[X]^{\leq \mathrm{D}}$	evaluation queries on polynomials $\mathbf{Q}_{\text{poly}}$	$\beta = \sum_{i \in [\ell]} \Pi[i] \cdot \alpha^{i-1}$ for $\alpha \in \mathbb{F}$
PIOP*+PC* [GWC19]	$\Pi \in (\mathbb{F}[X]^{\leq \mathrm{D}})^{m+n}$ $= (f_1, \ldots, f_m, g_1, \ldots, g_n)$	evaluation queries on structured polys $\mathbf{Q}_{\text{poly*}}$	$\beta = \sum_{k \in [n]} h_k(f_1(\alpha), \cdots, f_m(\alpha)) \cdot g_k(\alpha)$

Beyond Funky: Bulletproofs (and other sumcheck-based arguments), linear-only encodings [BCIOP13, GGPR13, Groth16], …

Special cases of the Funky protocol

	Proof string	Query class	Answer
PCP+VC IOP+VC			
LPCP+L			
PIOP+P			
PIOP*+P			$_k(\alpha)$

Funky protocol is everywhere

Succinct
RISC ZERO
Ligero
VALIDA
STARKWARE
Aztec
Matter Labs
polygon
NEXUS
Irreducible
…

Beyond Funky: Bulletproofs (and other sumcheck-based arguments), linear-only encodings [BCIOP13, GGPR13, Groth16], …

Which security property for FC?

Earlier in this talk IOP+VC
$\epsilon_{\mathsf{ARG}} \approx \epsilon_{\mathsf{IOP}} + \epsilon^{\mathsf{PB}}_{\mathsf{VC}}$

Vector Commitments position binding: $\Pr\left[\begin{array}{l} \beta_1 \neq \beta_2 \\ \wedge\ \forall i : \mathsf{FC.Check}(\mathsf{pp}, \mathsf{cm}, \alpha_i, \beta_i, \mathsf{pf}_i) = 1 \end{array} \middle| (\mathsf{cm}, \alpha, \beta_1, \mathsf{pf}_1, \beta_2, \mathsf{pf}_2) \leftarrow A(\mathsf{pp}) \right] \leq \epsilon$

[LM19] LPCP+LC
$\epsilon_{\mathsf{ARG}} \approx \epsilon_{\mathsf{LPCP}} + \epsilon^{\mathsf{FB}}_{\mathsf{LC}}$

Linear Commitments function binding: $\Pr\left[\begin{array}{l} \nexists \Pi : \forall i : \langle \alpha_i, \Pi \rangle = \beta_i \\ \wedge\ \forall i : \mathsf{FC.Check}(\mathsf{pp}, \mathsf{cm}, \alpha_i, \beta_i, \mathsf{pf}_i) = 1 \end{array} \middle| (\mathsf{cm}, (\alpha_i, \beta_i, \mathsf{pf}_i)_{i \in [n]}) \leftarrow A(\mathsf{pp}) \right] \leq \epsilon$

[CHMMVW20, BFS20] PIOP+PC
$\epsilon_{\mathsf{ARG}} \approx \epsilon_{\mathsf{PIOP}} + \kappa_{\mathsf{PC}}$

Too strong

Polynomial Commitments binding? strong correctness? interpolation binding? extractability?

[KZG10] [AJMMS23] [CHM+20, BFS20]

Functional Commitments function binding: $\Pr\left[\begin{array}{l} \nexists \Pi : \forall i : \alpha_i(\Pi) = \beta_i \\ \wedge\ \forall i : \mathsf{FC.Check}(\mathsf{pp}, \mathsf{cm}, \alpha_i, \beta_i, \mathsf{pf}_i) = 1 \end{array} \middle| (\mathsf{cm}, (\alpha_i, \beta_i, \mathsf{pf}_i)_{i \in [n]}) \leftarrow A(\mathsf{pp}) \right] \leq \epsilon$

Security of Funky protocol

Internal property of $\mathbf{Q}$
Independent of FIOP/FC

FIOP for language L with
- proof length l
- query complexity q
- round complexity k
- soundness error ϵ_{FIOP}

ARG := Funky[FIOP, FC]

Query class $\mathbf{Q}$ with tail error $\epsilon_{\mathbf{Q}}$

Functional commitment scheme with function binding error ϵ_{FC}

Theorem. $\forall\, \mathsf{N} \in \mathbb{N}$,

$$\epsilon_{\mathsf{ARG}}(t_{\mathsf{ARG}}) \leq \epsilon_{\mathsf{FIOP}} + \mathsf{k} \cdot \epsilon_{\mathsf{FC}}(t_{\mathsf{FC}}) + \mathsf{k} \cdot \epsilon_{\mathbf{Q}}(l, \mathsf{N}), \text{ where } t_{\mathsf{FC}} = O\left(t_{\mathsf{ARG}} \cdot \mathsf{N}\right).$$

TLDR:
- **A “tight” security notion for FC schemes**
- **Concrete and tight bounds using tail errors**

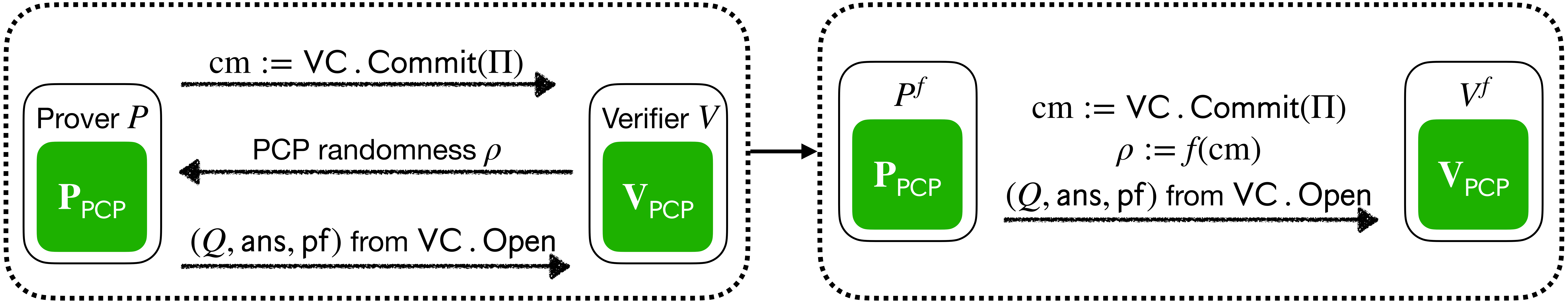
$\epsilon_{\mathbf{Q}_{\mathsf{point}}}(l, \mathsf{N}) = l/\mathsf{N} \implies$ **recovers the bounds for Kilian’s protocol and IBCS protocol**

Fiat-Shamir security:
From succinct arguments to SNARGs

Fiat-Shamir transformation

Random oracle: $\mathcal{O} = \{\mathcal{O}_\lambda\}_{\lambda \in \mathbb{N}}$
$\mathcal{O}_\lambda$: uniform distribution over $\{f: \{0,1\}^* \to \{0,1\}^\lambda\}$

Succinct interactive arguments → Succint non-interactive arguments



Central question: Is security preserved after the Fiat-Shamir transformation?

In generical no [CY24]: $\epsilon_{\mathsf{NARG}}(x, t, m) \leq (m+1)^{\mathsf{k}} \cdot \epsilon_{\mathsf{ARG}}(x, t)$

RO queries

k might be superconstant!

Fiat-Shamir security

FIOP for language L with
- proof length l
- query complexity q
- round complexity k
- Fiat-Shamir soundness error $\epsilon_{\mathsf{FIOP}}^{\mathsf{FS}}$

ARG := Funky[FIOP, FC]

Query classes $\mathbf{Q}$ with tail error $\epsilon_{\mathbf{Q}}$

Functional commitment scheme with Fiat-Shamir function binding error $\epsilon_{\mathsf{FC}}^{\mathsf{FSFB}}$

Theorem. $\forall\, \mathsf{N} \in \mathbb{N}$,

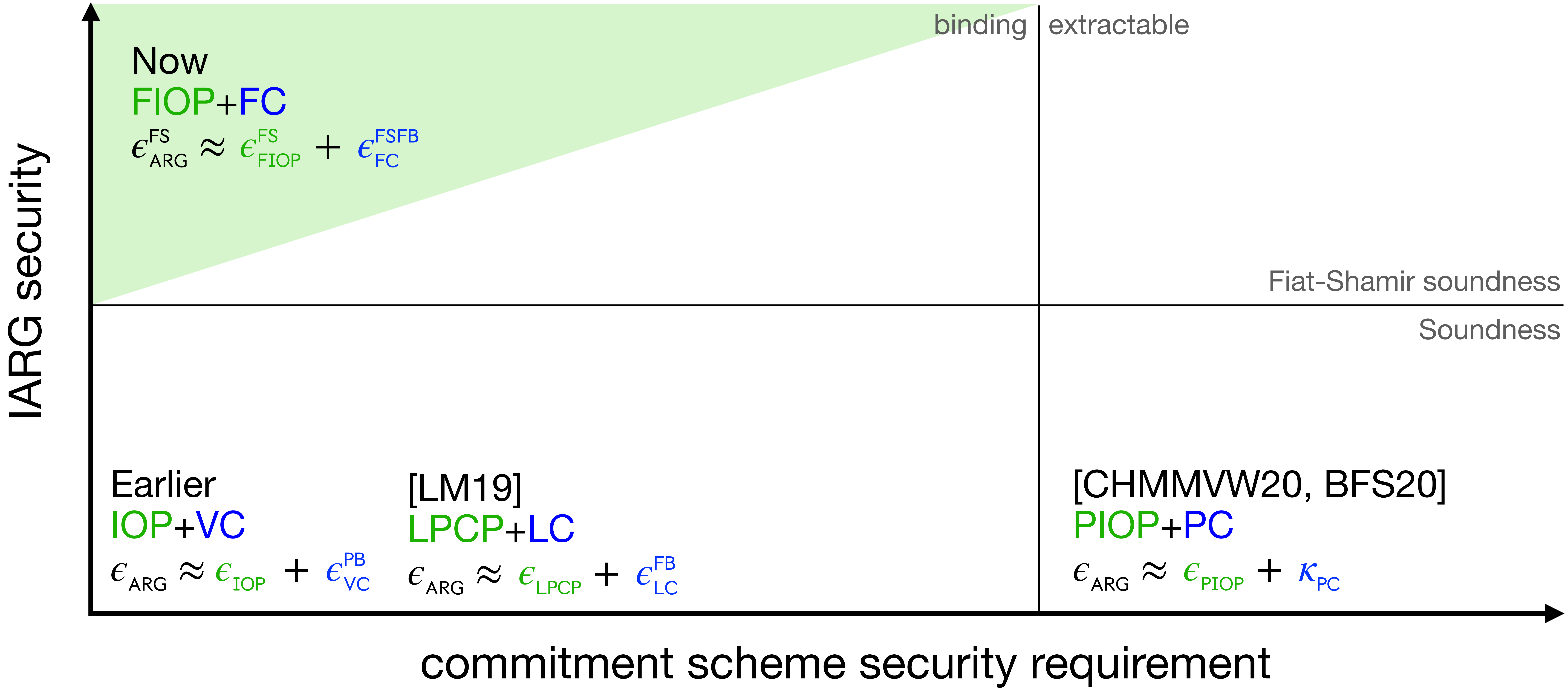
$$\epsilon_{\mathsf{NARG}}(t_{\mathsf{ARG}}, m_{\mathsf{ARG}}) \leq \epsilon_{\mathsf{FIOP}}^{\mathsf{FS}}(O(m_{\mathsf{ARG}})) + \mathsf{k} \cdot \epsilon_{\mathsf{FC}}^{\mathsf{FSFB}}(t_{\mathsf{FC}}, m_{\mathsf{FC}}) + \mathsf{k} \cdot \epsilon_{\mathbf{Q}}(l, \mathsf{N}), \text{ where } \begin{cases} t_{\mathsf{FC}} = O\left(t_{\mathsf{ARG}} \cdot \mathsf{N}\right) \\ m_{\mathsf{FC}} = O\left(m_{\mathsf{ARG}} \cdot \mathsf{k} \cdot \mathsf{N}\right) \end{cases}.$$

A theorem that generalizes everything we saw (except post-quantum)

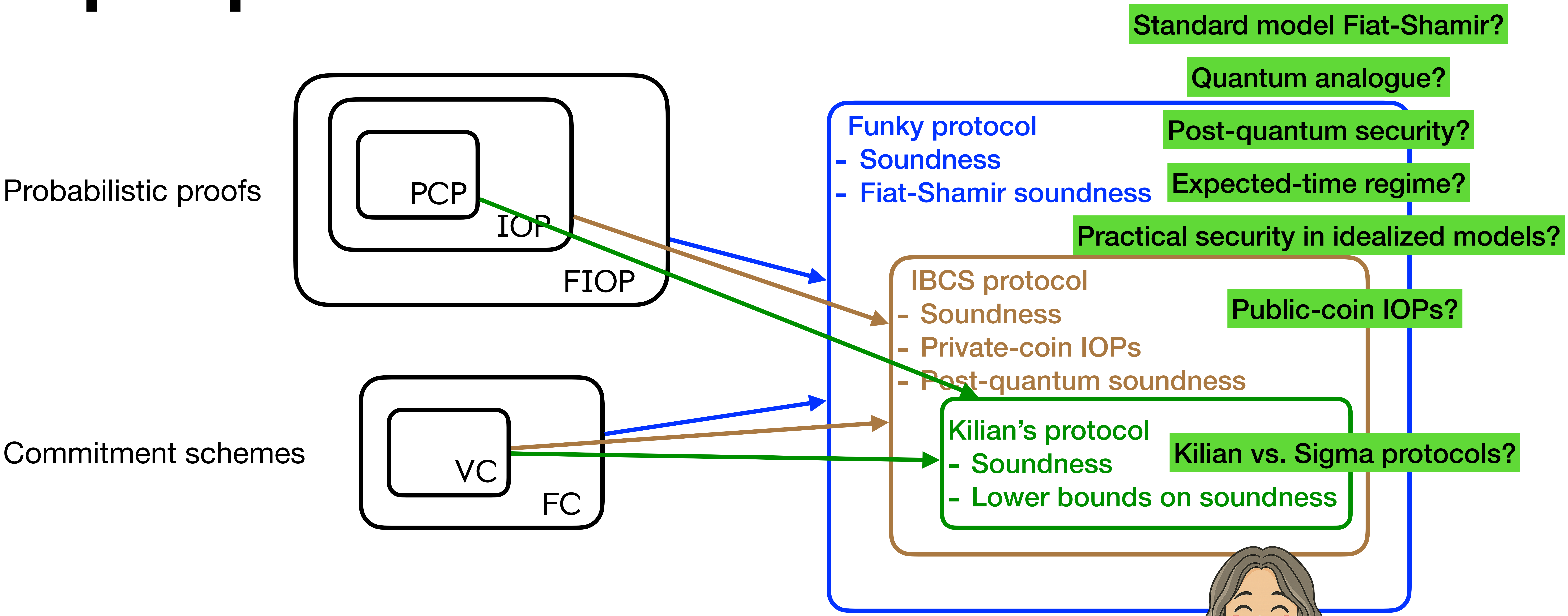
Corollary: security analysis of Plonk [GWC19] from falsifiable assumption (ARSDH)
(previously: from ARSDH+SplitRSDH)

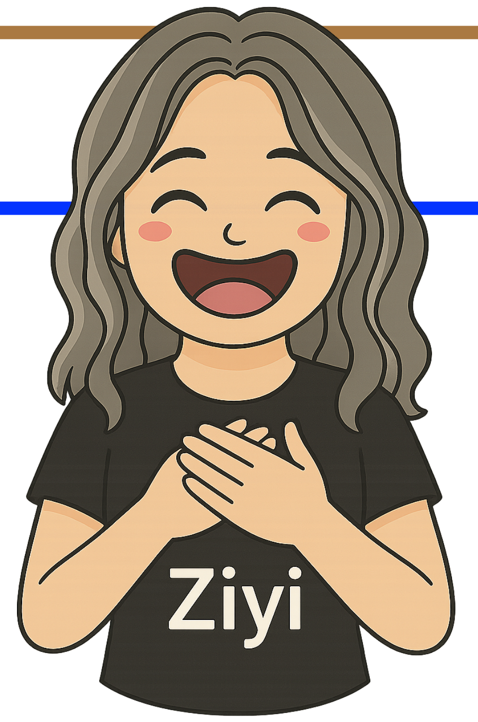
Aztec polygon ZKsync …

Overview: standard-model analyses



Open problems





Thank you!

References

[BG08]: Boaz Barak and Oded Goldreich. “Universal Arguments and their Applications”. CCC ’02.

[BL02]: Boaz Barak and Yehuda Lindell. “Strict polynomial-time in simulation and extraction”. STOC ‘02.

[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”. arXiv:2411.05360.

[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.

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

[CY24]: Alessandro Chiesa and Eylon Yogev. Building Cryptographic Proofs from Hash Functions. 2024. URL: https://github.com/hash-based-snargs-book.

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

[GWC19]: Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over Lagrangebases for Oecumenical Noninteractive arguments of Knowledge. ePrint Report 2019/953.

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

[LMS22]: Russell W. F. Lai, Giulio Malavolta, and Nicholas Spooner. “Quantum Rewinding for Many-Round Protocols”. TCC ’22.

[PS00]: David Pointcheval and Jacques Stern. “Security Arguments for Digital Signatures and Blind Signatures”. Journal of Cryptology 13 (2000), 361–396.

[Unr12]: Dominique Unruh. “Quantum proofs of knowledge”. EUROCRYPT ’12.

[Unr16b]: Dominique Unruh. “Computationally binding quantum commitments”. EUROCRYPT ’16.

[Wat06]: John Watrous. “Zero-knowledge against quantum attacks”. STOC ’06.

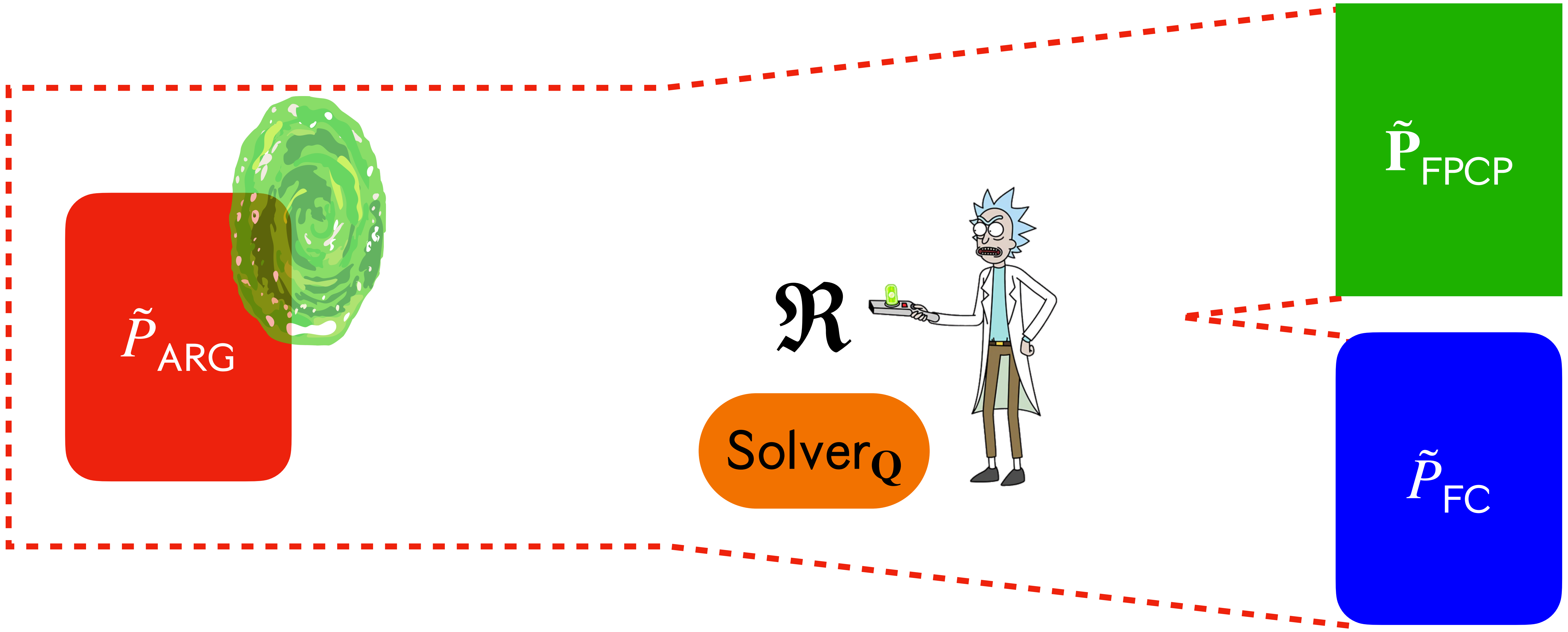
Security of Funky from FPCP and non-interactive FC

Security reduction for Funky[FPCP, FC]

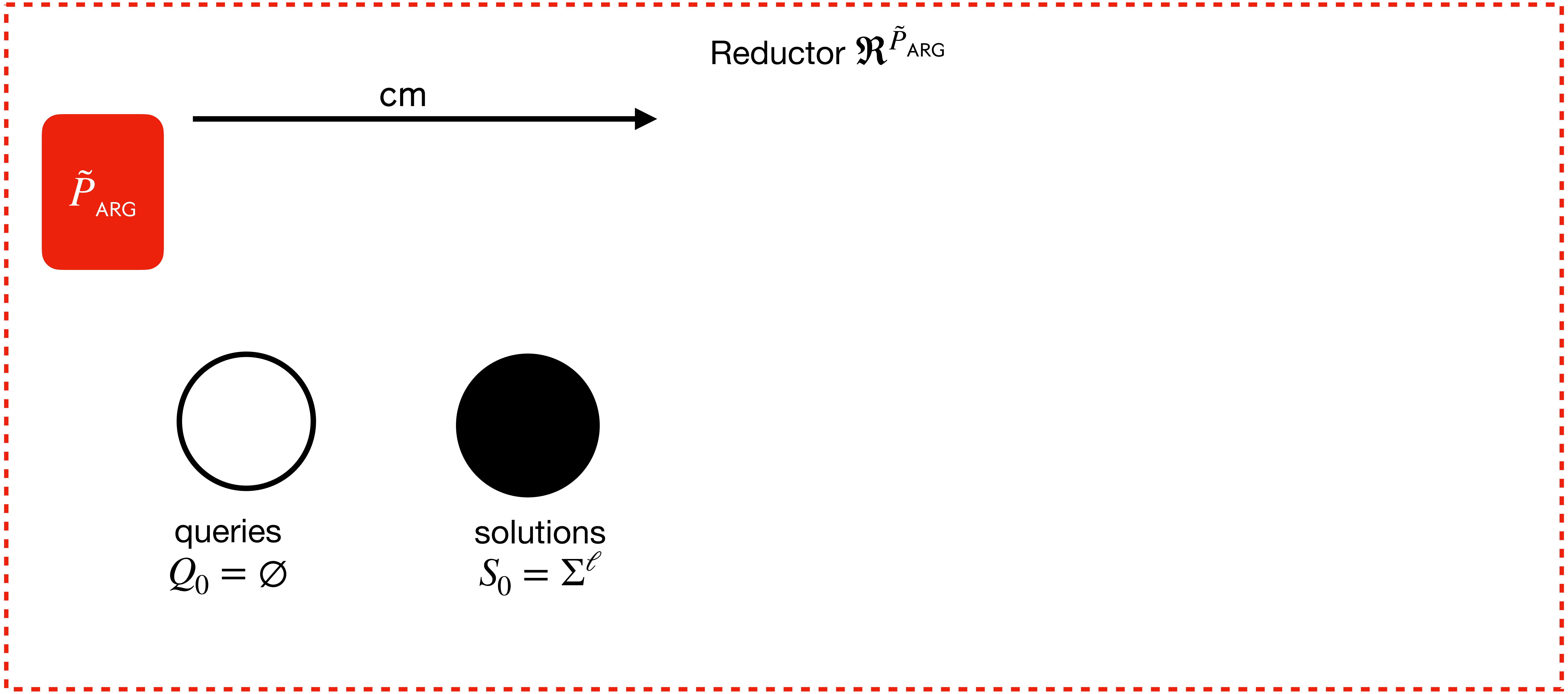
Goal:

(for FPCPs and non-interactive FCs)

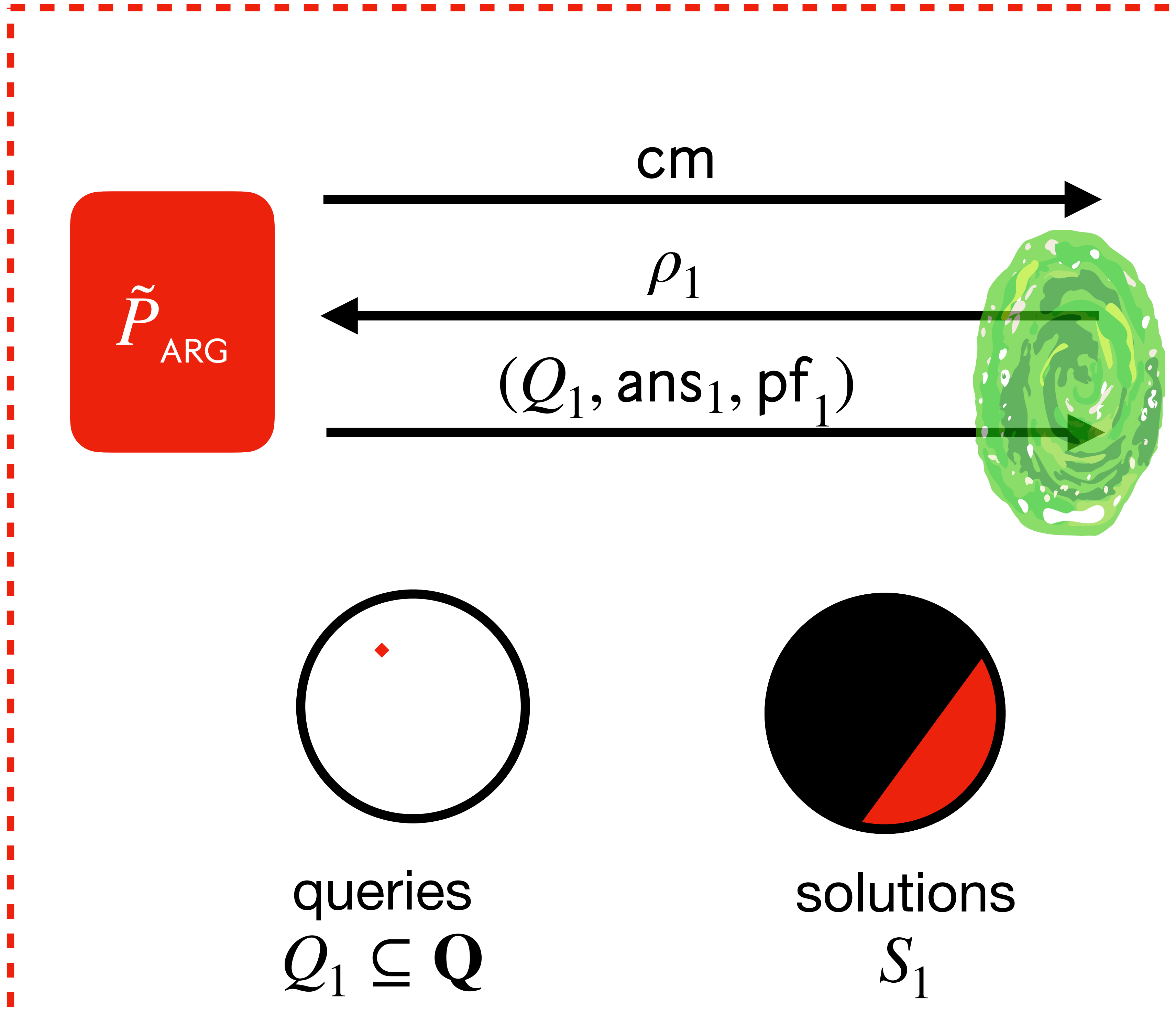
$$\epsilon_{\mathsf{ARG}}(t_{\mathsf{ARG}}) \leq \epsilon_{\mathsf{FIOP}} + \mathsf{k} \cdot \epsilon_{\mathsf{FC}}(t_{\mathsf{FC}}) + \mathsf{k} \cdot \epsilon_{\mathbf{Q}}(l, \mathsf{N}), \text{ where } t_{\mathsf{FC}} = O\left(t_{\mathsf{ARG}} \cdot \mathsf{N}\right)$$



Security reduction for Funky[FPCP, FC]



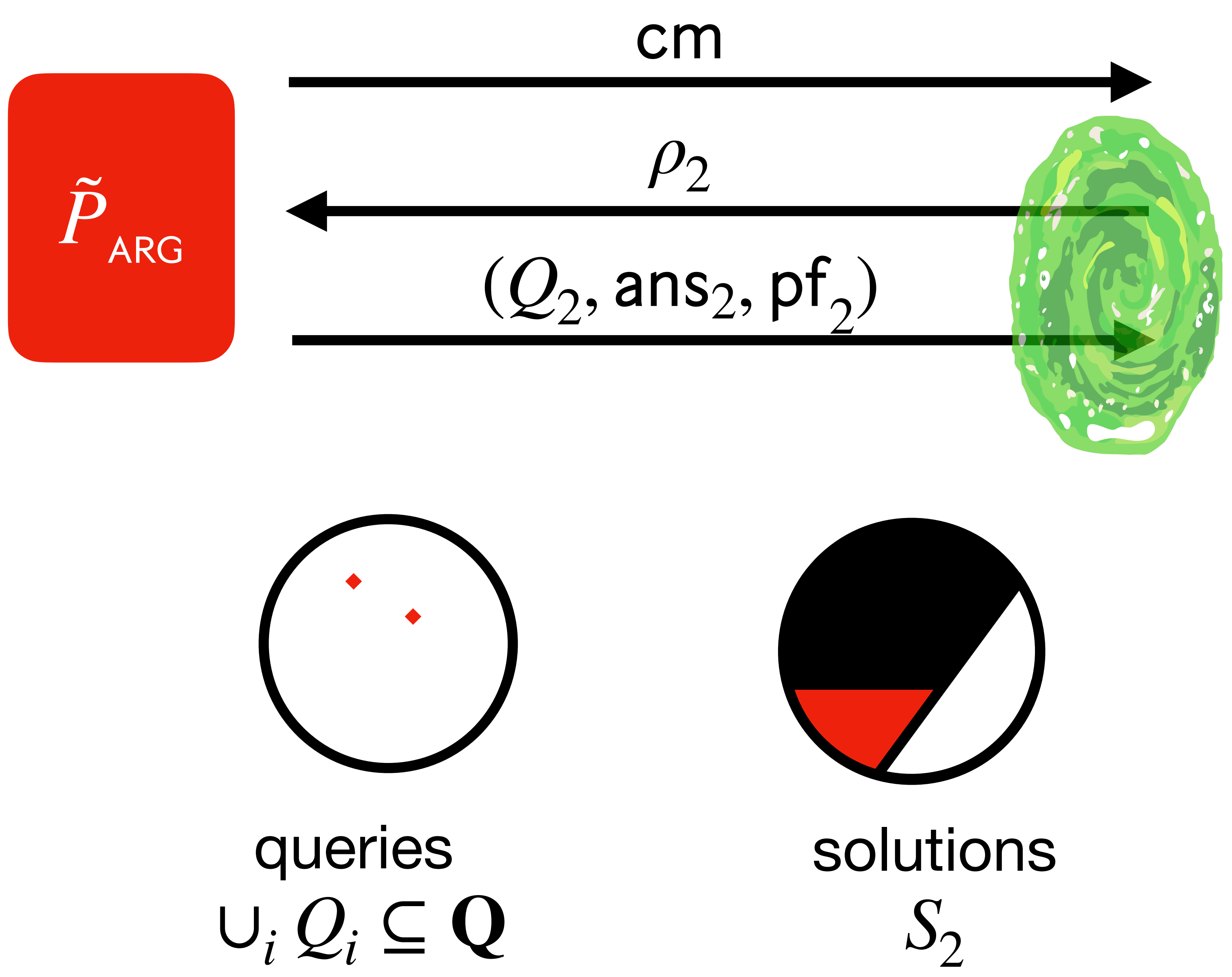
Security reduction for Funky[FPCP, FC]



$$S_1 = \{\tilde{\Pi} \mid \forall \alpha_{1,j} \in Q_1, \alpha_{1,j}(\tilde{\Pi}) = \beta_{1,j}\}$$

Security reduction for Funky[FPCP, FC]

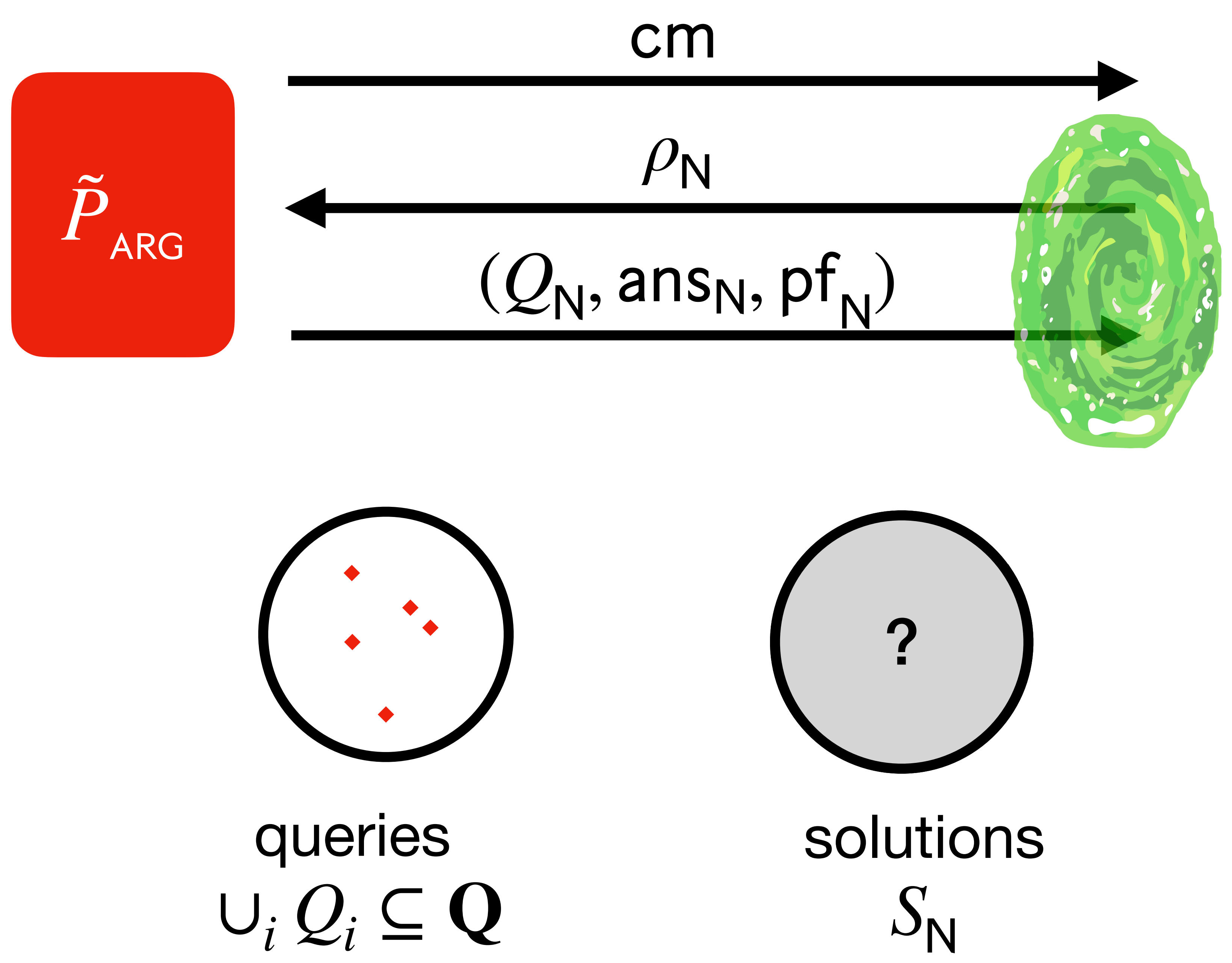
Reductor $\mathfrak{R}^{\tilde{P}_{\mathrm{ARG}}}$



$$S_2 = \{\tilde{\Pi} \mid \forall \alpha_{2,j} \in Q_2, \alpha_{2,j}(\tilde{\Pi}) = \beta_{2,j}\} \cap S_1$$

Security reduction for Funky[FPCP, FC]

Reductor $\mathfrak{R}^{\tilde{P}_{\mathsf{ARG}}}$



$S_{\mathsf{N}} = \{\tilde{\Pi} \mid \forall \alpha_{\mathsf{N},j} \in Q_{\mathsf{N}}, \alpha_{\mathsf{N},j}(\tilde{\Pi}) = \beta_{\mathsf{N},j}\} \cap S_{\mathsf{N}-1}$

Output $\tilde{\Pi} \leftarrow \mathsf{Solver}_{\mathbf{Q}}((\alpha_{i,j}, \beta_{i,j})_{i\in[\mathsf{N}], j\in[\mathsf{q}]})$

Outputs $\tilde{\Pi} \in S_{\mathsf{N}}$

Security reduction for Funky[FPCP, FC]

Produced by the reductor $\mathfrak{R}^{\tilde{P}_{\text{ARG}}}$

$$\Pr\left[\langle \tilde{P}, V(x)\rangle = 1\right] \leq \Pr\begin{bmatrix}\text{Sample } \rho \\ \text{FPCP verifier accepts: } \mathbf{V}^{\tilde{\Pi}}(x;\rho) = 1 \\ \text{ARG verifier accepts: } V(x;\rho;Q,\text{ans},\text{pf})\rangle = 1\end{bmatrix}$$

FPCP soundness
$\leq \epsilon_{\text{FPCP}}(x)$

Produced by a t_{ARG}-time adversary $\tilde{P}_{\text{ARG}}$ given ρ

$$+ \Pr\begin{bmatrix}\text{Sample } \rho \\ \text{FPCP verifier rejects: } \mathbf{V}^{\tilde{\Pi}}(x;\rho) \neq 1 \\ \text{ARG verifier accepts: } V(x;\rho;Q,\text{ans},\text{pf})\rangle = 1\end{bmatrix}$$

Security reduction lemma
$\leq \epsilon_{\text{FC}}(t_{\text{FC}}) + \epsilon_{\mathbf{Q}}(\ell, \text{N})$

- Either (Q, ans) is inconsistent with $\tilde{\Pi}$; or
- (Q, ans) contains "new queries"

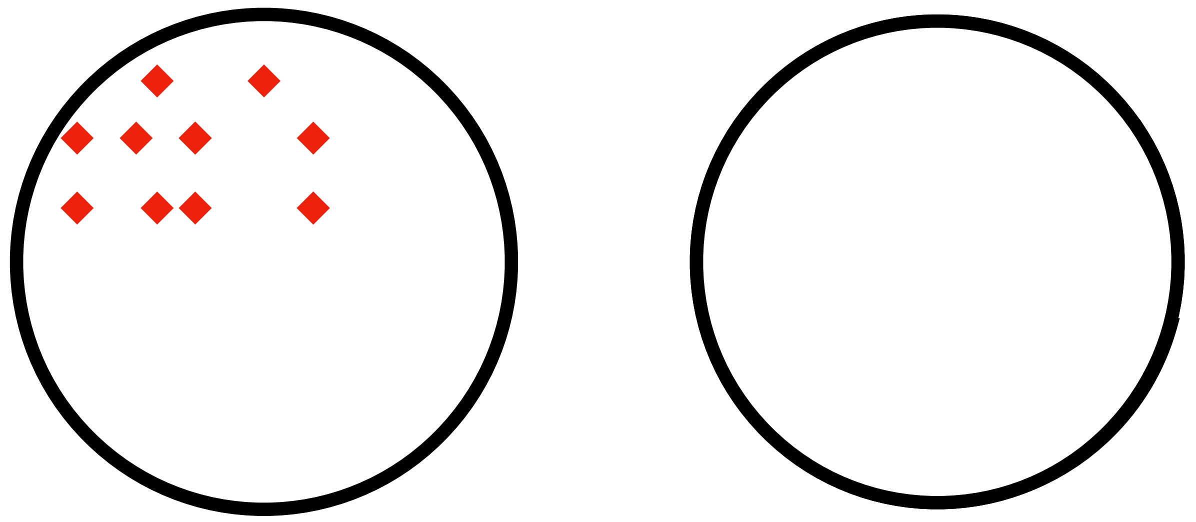
$S_{\text{N+1}} = \emptyset$ (no solution)
→ FC verifier accepts all FC proofs

$S_{\text{N+1}} \neq \emptyset \wedge S_{\text{N+1}} \neq S_{\text{N}}$
→ *tail error* of the query class $\mathbf{Q}$

Security reduction lemma

queries $\cup_i Q_i$ solutions S_i

Case 1:

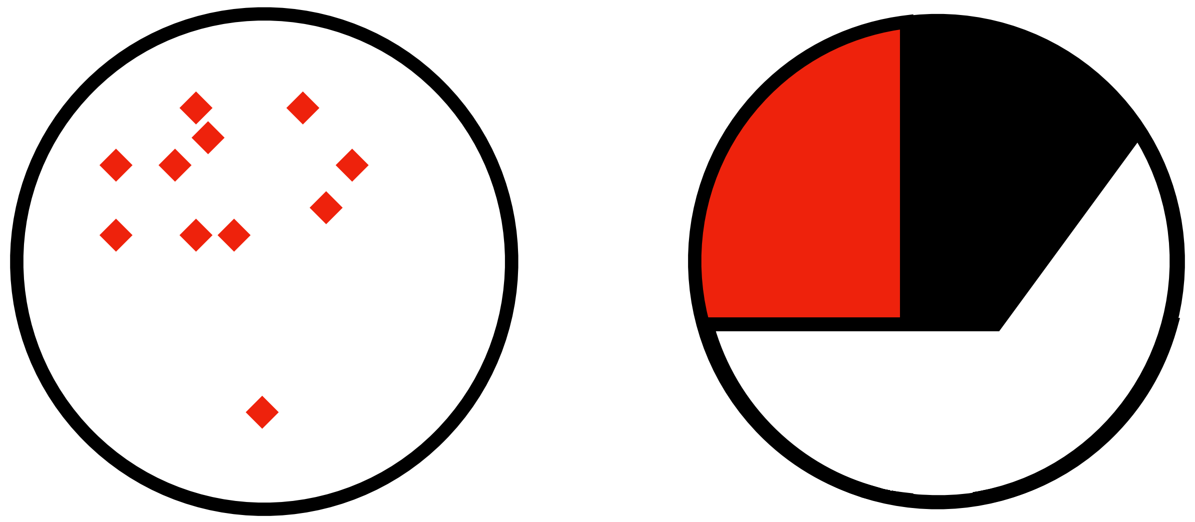


$$\Pr\left[\begin{array}{l}\nexists \tilde{\Pi} : \forall \alpha \in \cup_i Q_i : \alpha(\tilde{\Pi}) = \mathsf{ans}[\alpha] \\ \text{Yet all FC checks pass}\end{array}\right] \leq \epsilon_{\mathsf{FC}}(t_{\mathsf{FC}})$$

Function binding

$S_{N+1} = \varnothing$ (no solution)
→ FC verifier accepts all FC proofs

Case 2:



$i = N + 1$

Internal property of $\mathbf{Q}$
Independent of FIOP/FC

$$\Pr\left[S_{N+1} \neq \varnothing \land S_{N+1} \neq S_N\right] \leq \epsilon_{\mathbf{Q}}(\ell, N)$$

Tail error

$S_{N+1} \neq \varnothing \land S_{N+1} \neq S_N$
→ *tail error* of the query class $\mathbf{Q}$

Tail error well-behaved for reasonable query classes:
For large N, unlikely that the $(N+1)$-th rewind gives new info