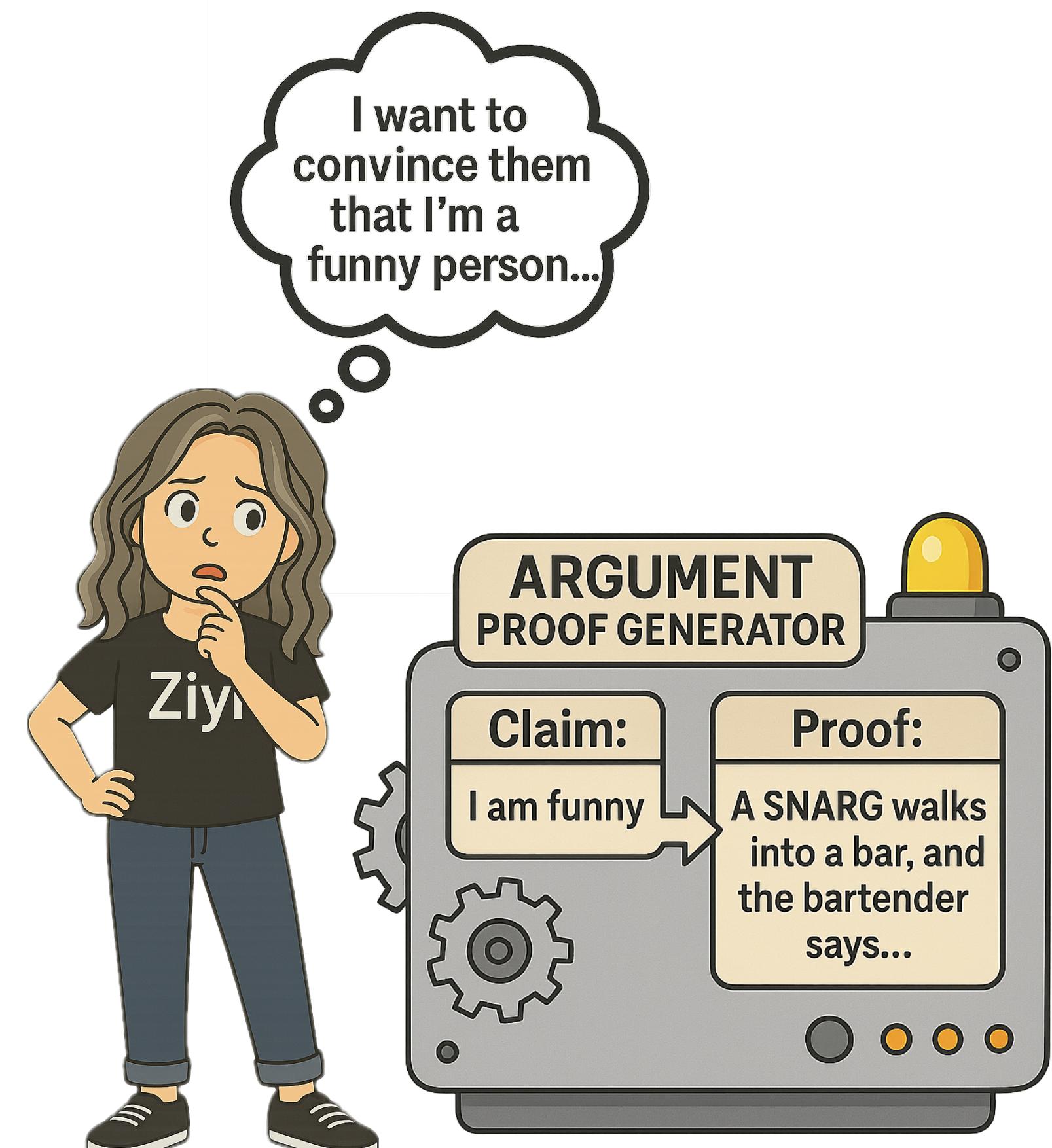


On the Security of Succinct Arguments from Probabilistic Proofs



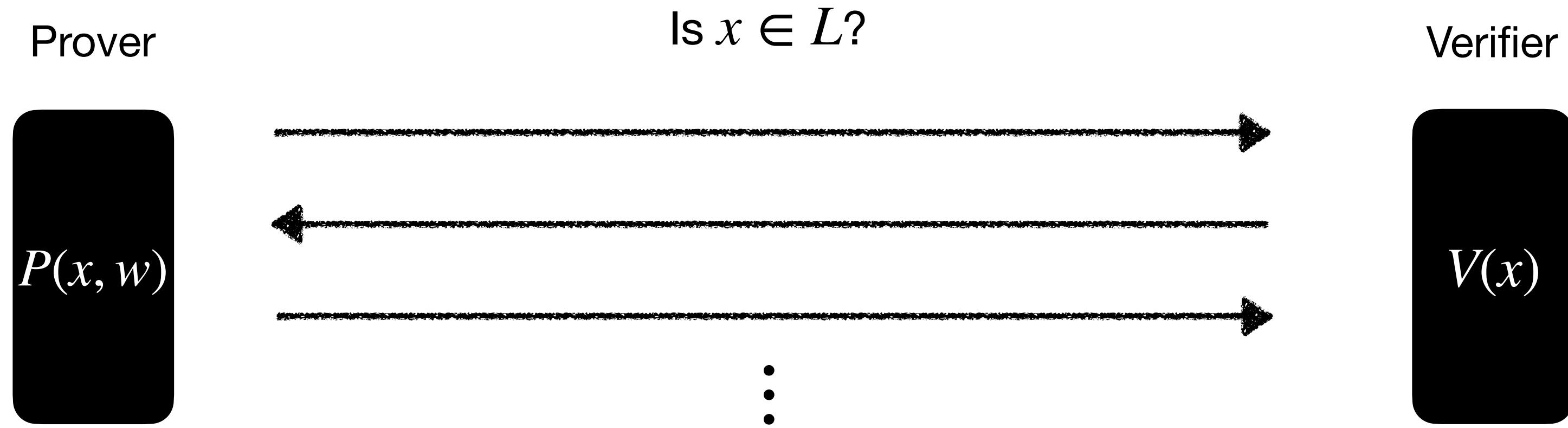
Ziyi Guan



EPFL

What are succinct arguments?

Interactive proofs



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

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

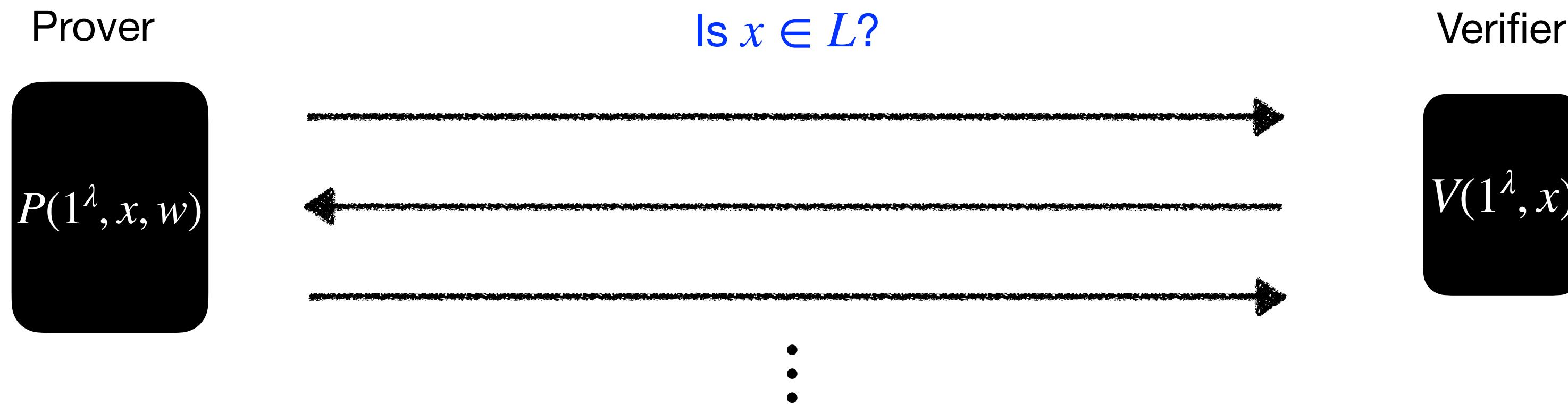
Target metric: COMMUNICATION COMPLEXITY

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

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

Interactive arguments

Interactive proofs with computational soundness



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

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

Today's protagonist:
Succinct Interactive Arguments

$\text{cc} \ll |w|$

Why study **succinct** interactive arguments?

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

They exist based on simple crypto assumptions...

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

zero-knowledge with
non-black-box simulation

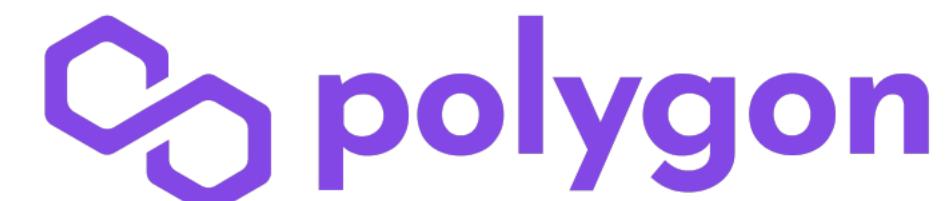
malicious MPC

...

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



Irrreducible

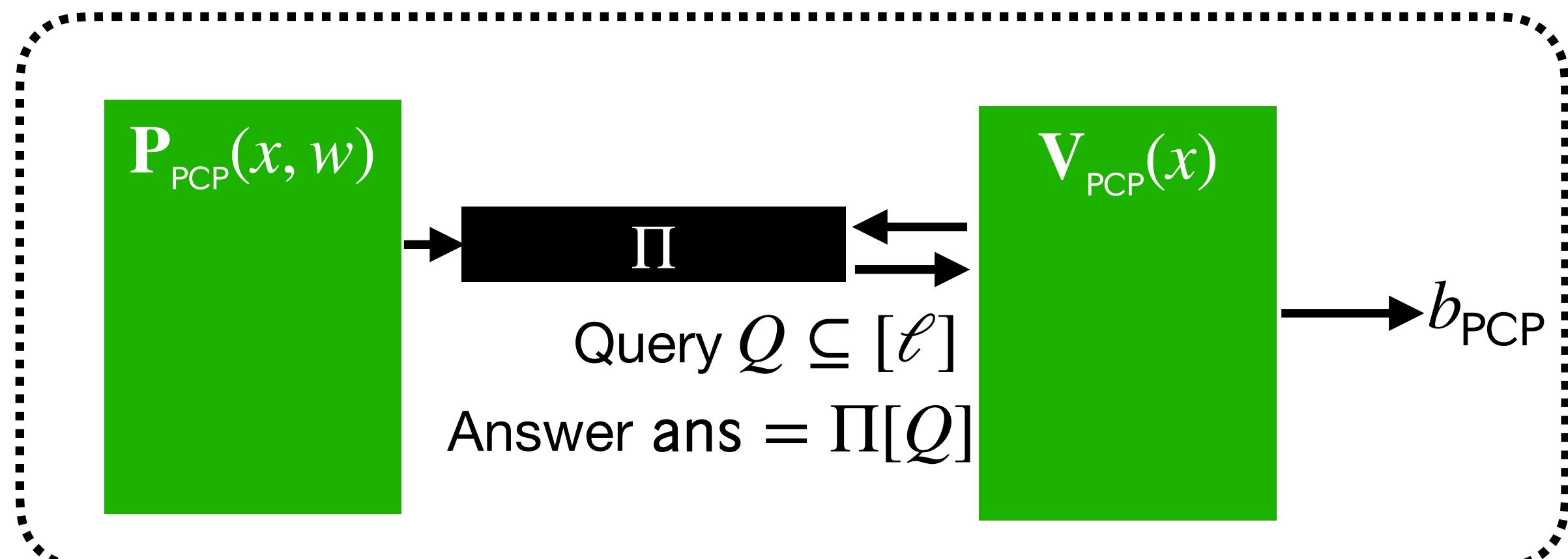


...

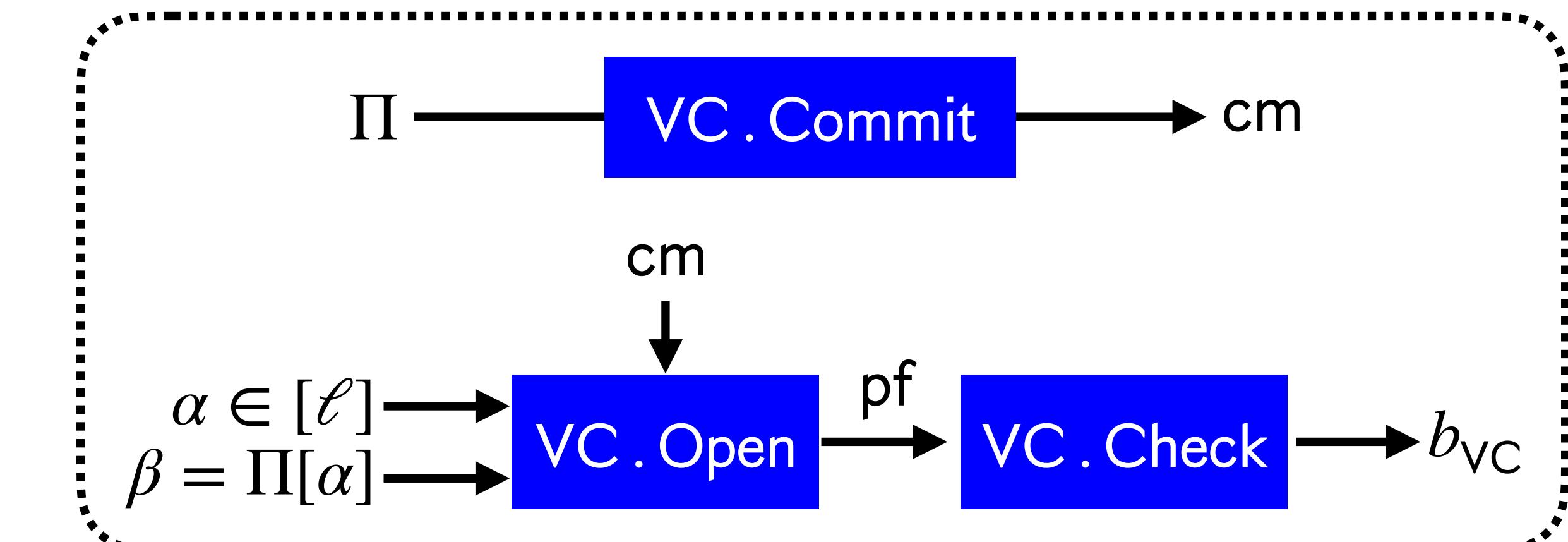
Kilian's protocol: The first and simplest succinct argument

How to construct succinct arguments?

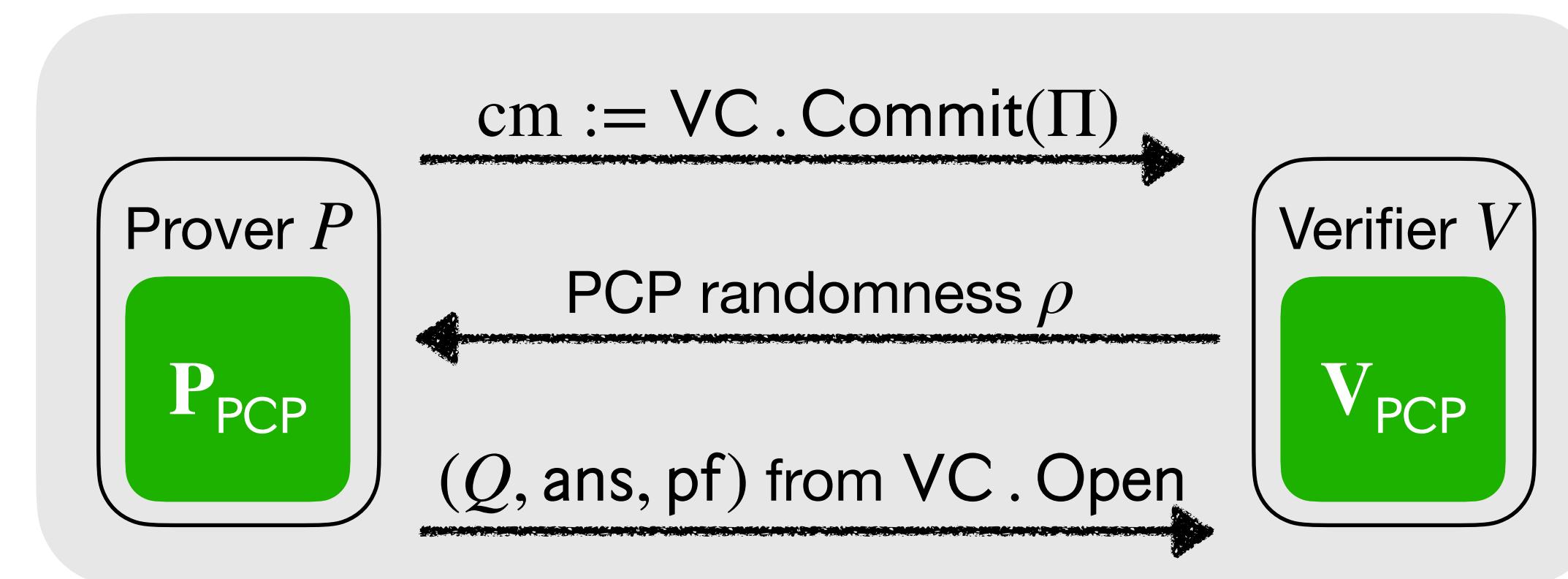
Building block #1: probabilistically checkable proof (PCP)



Building block #2: vector commitment scheme (VC)



Kilian's protocol



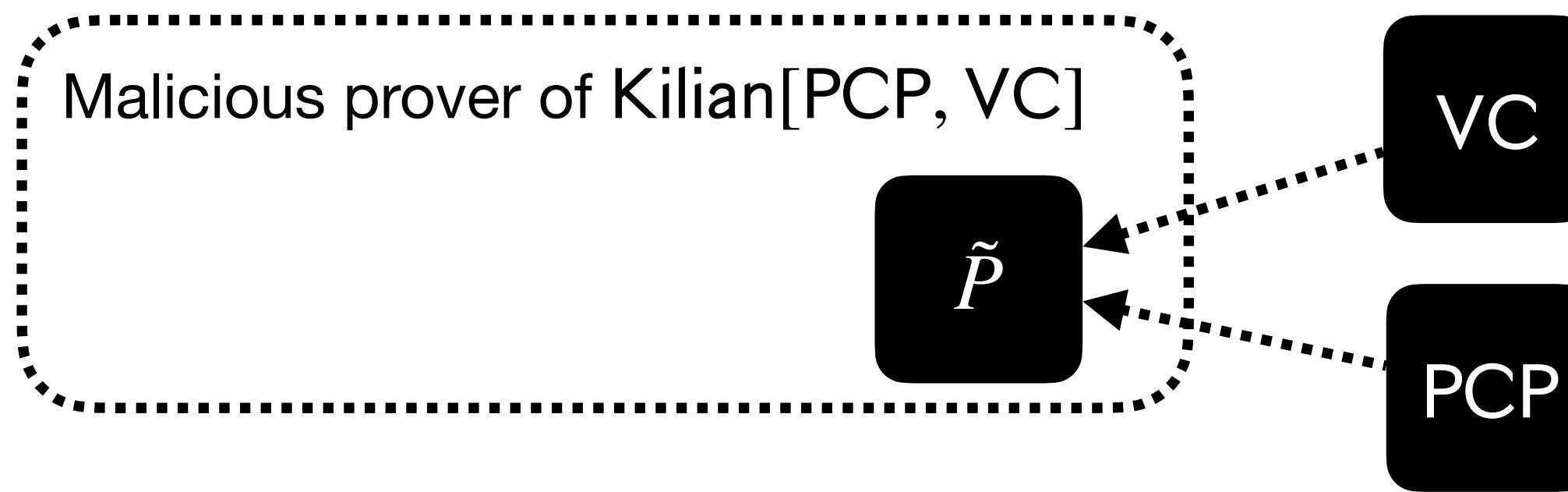
T -step computation:

- Prover time: $\text{poly}(T)$
- Verifier time: $\text{polylog}(T)$
- (CC: $\text{polylog}(T)$)

Simple (and only known) security analysis

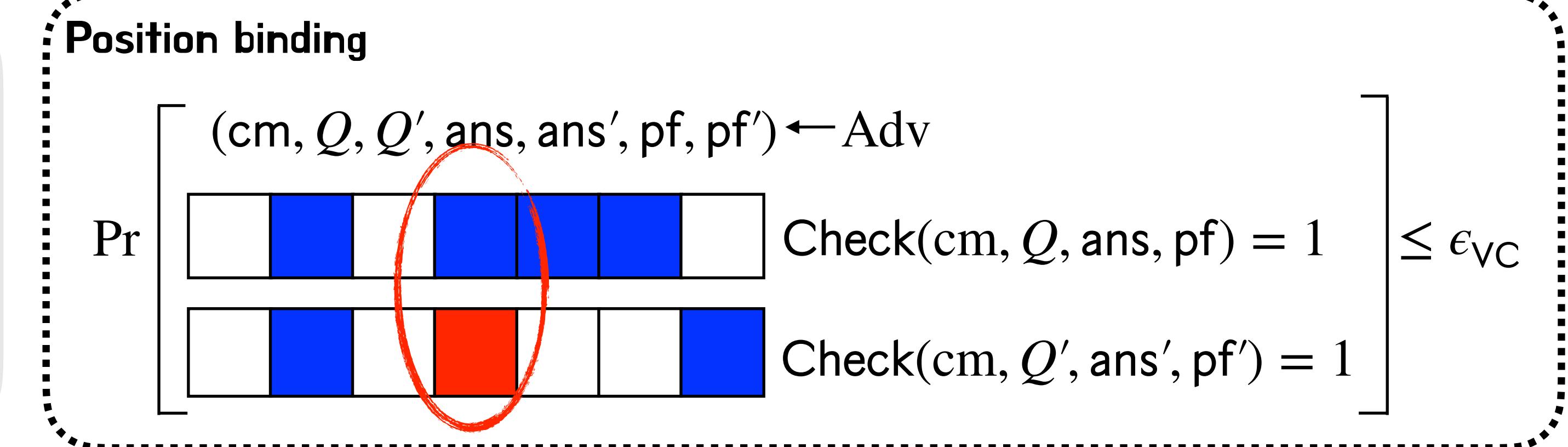
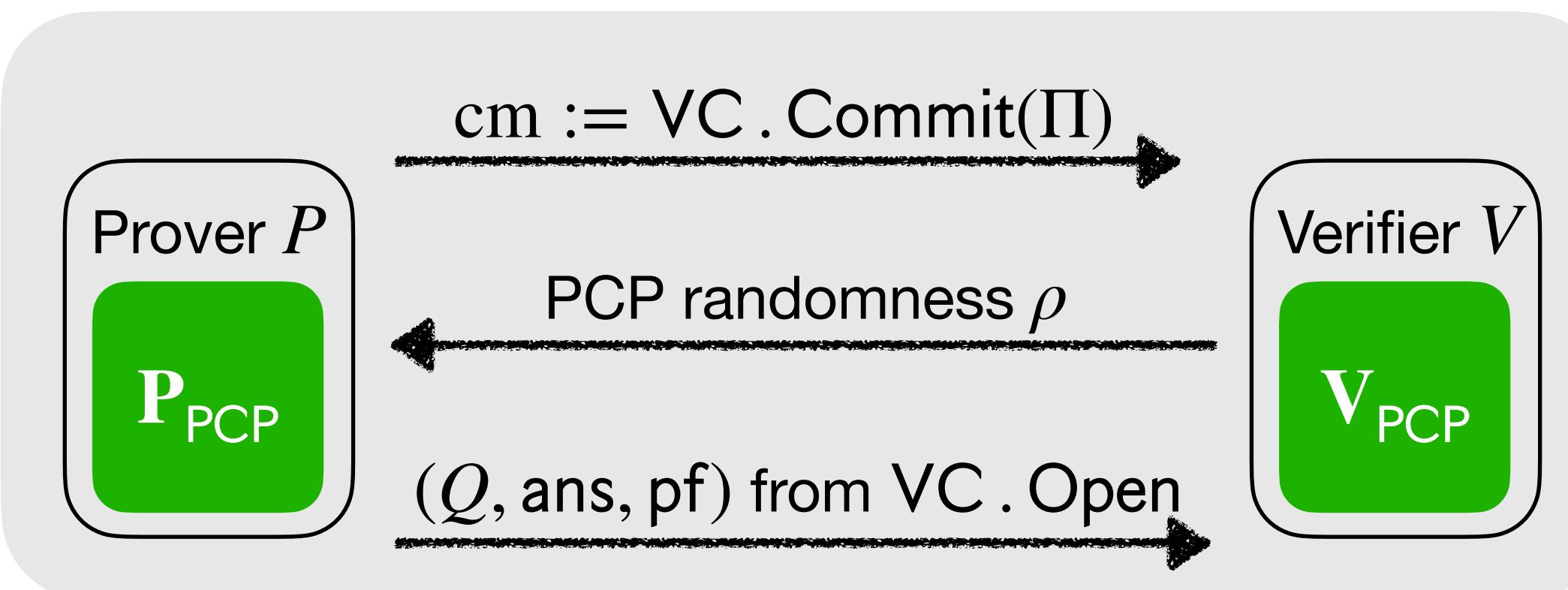
Goal: relate the soundness error of Kilian[PCP, VC]

to the soundness error of PCP and the position binding error of VC.



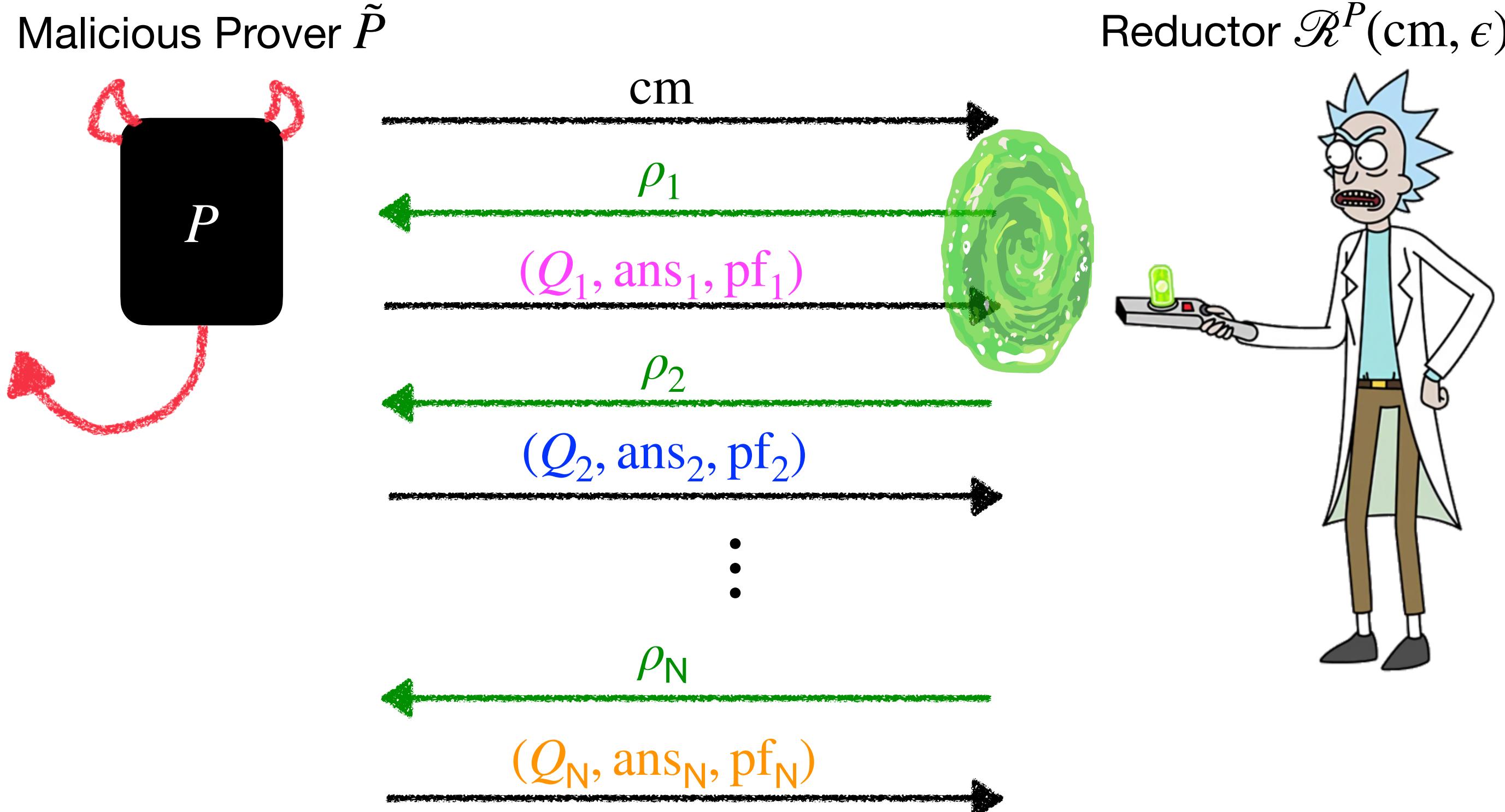
Rewind \tilde{P} to get a malicious PCP string $\tilde{\Pi}$
⇒ (PCP soundness) upper bound the success probability of $\tilde{\Pi}$
⇒ (Position binding) $\tilde{\Pi}$ cannot be too different from \tilde{P}

Kilian's protocol



Security from rewinding

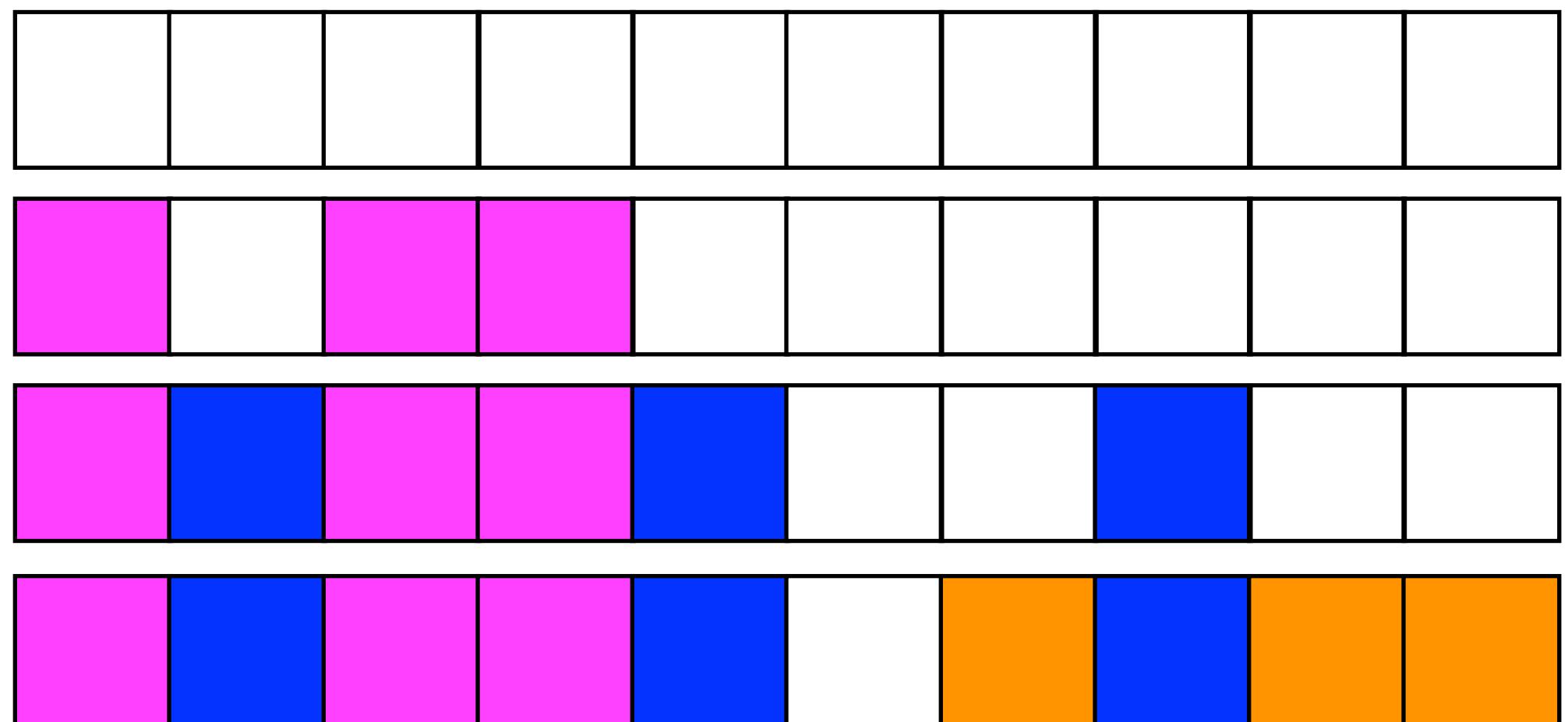
How to rewind?



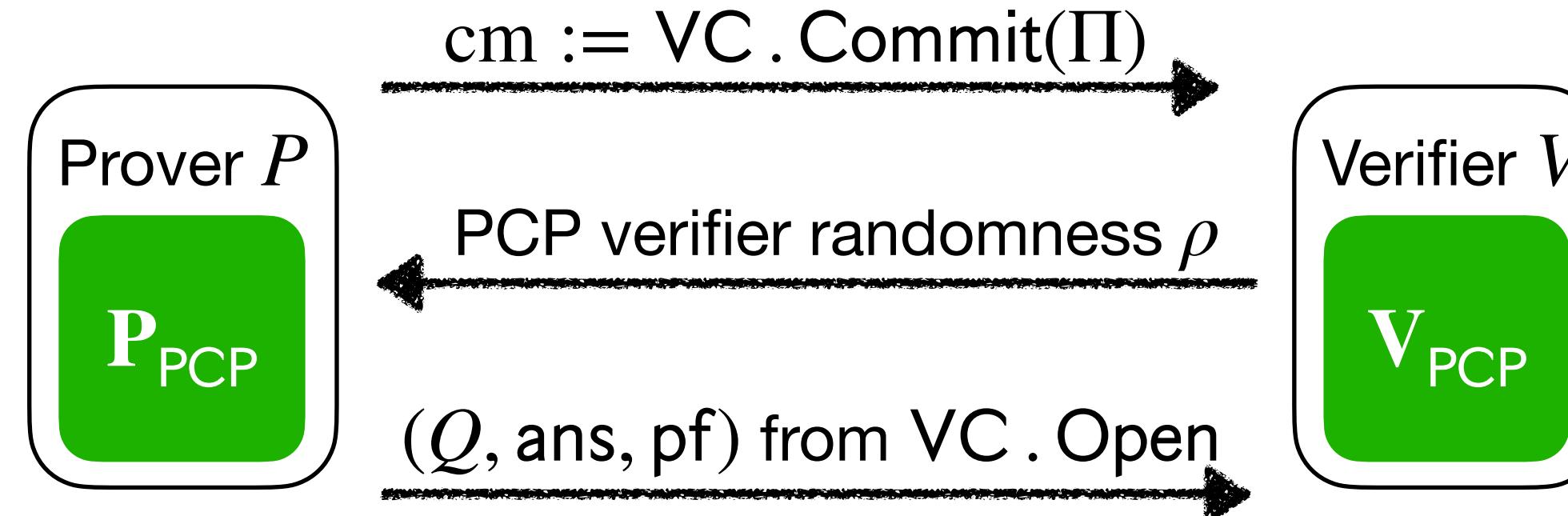
Subtle design choices:

- Strict time vs. expected time
- Sample with/without replacement
- Stopping conditions
- ...

Recover $\tilde{\Pi}$



What is the security of Kilian's protocol?



Previously:

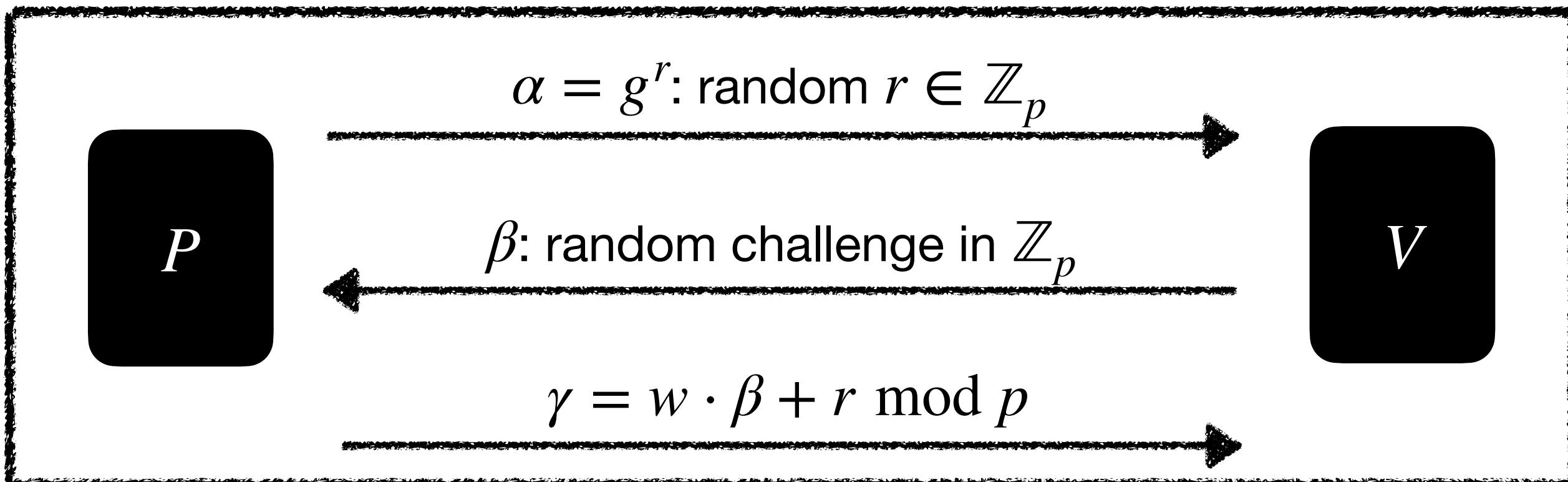
- [Kilian92] gives an **informal** analysis
- [BG08] $\epsilon_{\text{ARG}} \leq 8 \cdot \epsilon_{\text{PCP}} + \sqrt[3]{\epsilon_{\text{VC}}}$ and **assuming** PCP is **non-adaptive** & **reverse-samplable**
non-trivial restrictions
- [CMSZ21] Kilian is secure when ϵ_{PCP} **negligible** (in a paper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

We expect that $\epsilon_{\text{ARG}} \leq \epsilon_{\text{PCP}} + \epsilon_{\text{VC}} \dots$ right?



Surprise! A limitation:

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



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

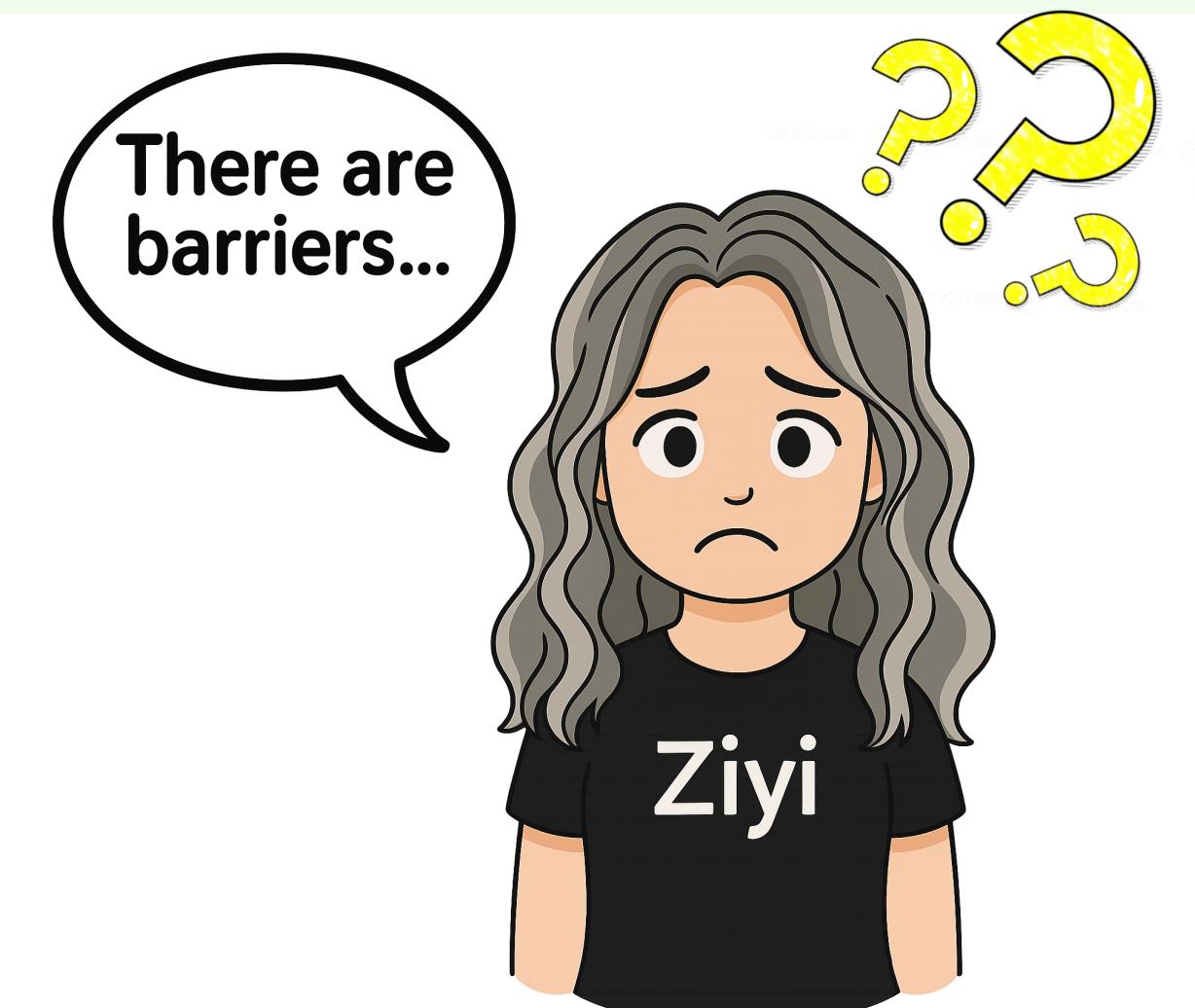
Suppose
 $\epsilon_{\text{ARG}} \leq \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}$



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

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

... so the folklore is beyond current rewinding techniques



Improved security for Kilian



Theorem. $\forall \epsilon > 0$,

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

λ : security parameter

Why $l \cdot 1/\epsilon$ overhead?

- l locations in Π
- \implies 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
- \implies Need $1/\epsilon$ times for each location as buffer

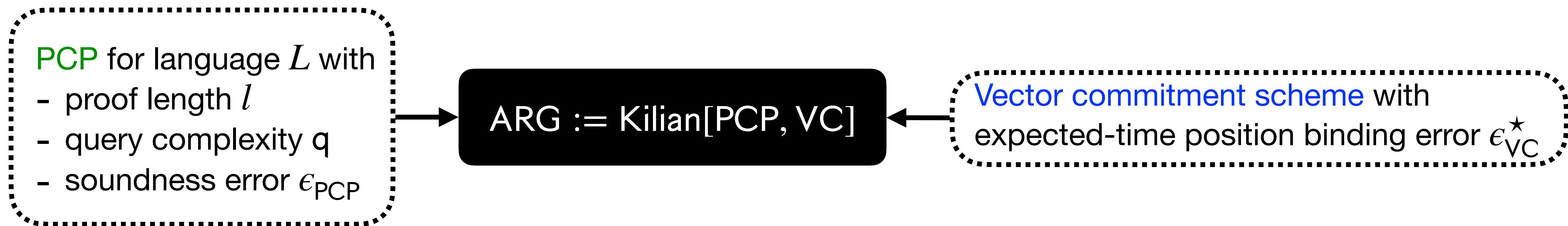
Suppose $\epsilon_{\text{VC}}(t) \leq O(t^2/2^\lambda)$ (e.g. an ideal Merkle tree)

By **Theorem**:

$$\epsilon_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{PCP}} + l^{2/3} \cdot O\left(\sqrt[3]{t_{\text{ARG}}^2/2^\lambda}\right)$$

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

Alternative route: expected-time regime



Theorem. $\forall \epsilon > 0$,

$$\epsilon_{\text{ARG}}^*(t_{\text{ARG}}^*) \leq \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}^*(t_{\text{VC}}^*) + \epsilon, \text{ where } t_{\text{VC}}^* = O(t_{\text{ARG}}^* \cdot \log(q/\epsilon)).$$



Set $\epsilon_{\text{VC}}^*(t^*) \leq O\left(\sqrt{(t^*)^2/2^\lambda}\right)$ (λ : security parameter
(e.g. an ideal Merkle tree))

Theorem
⇒

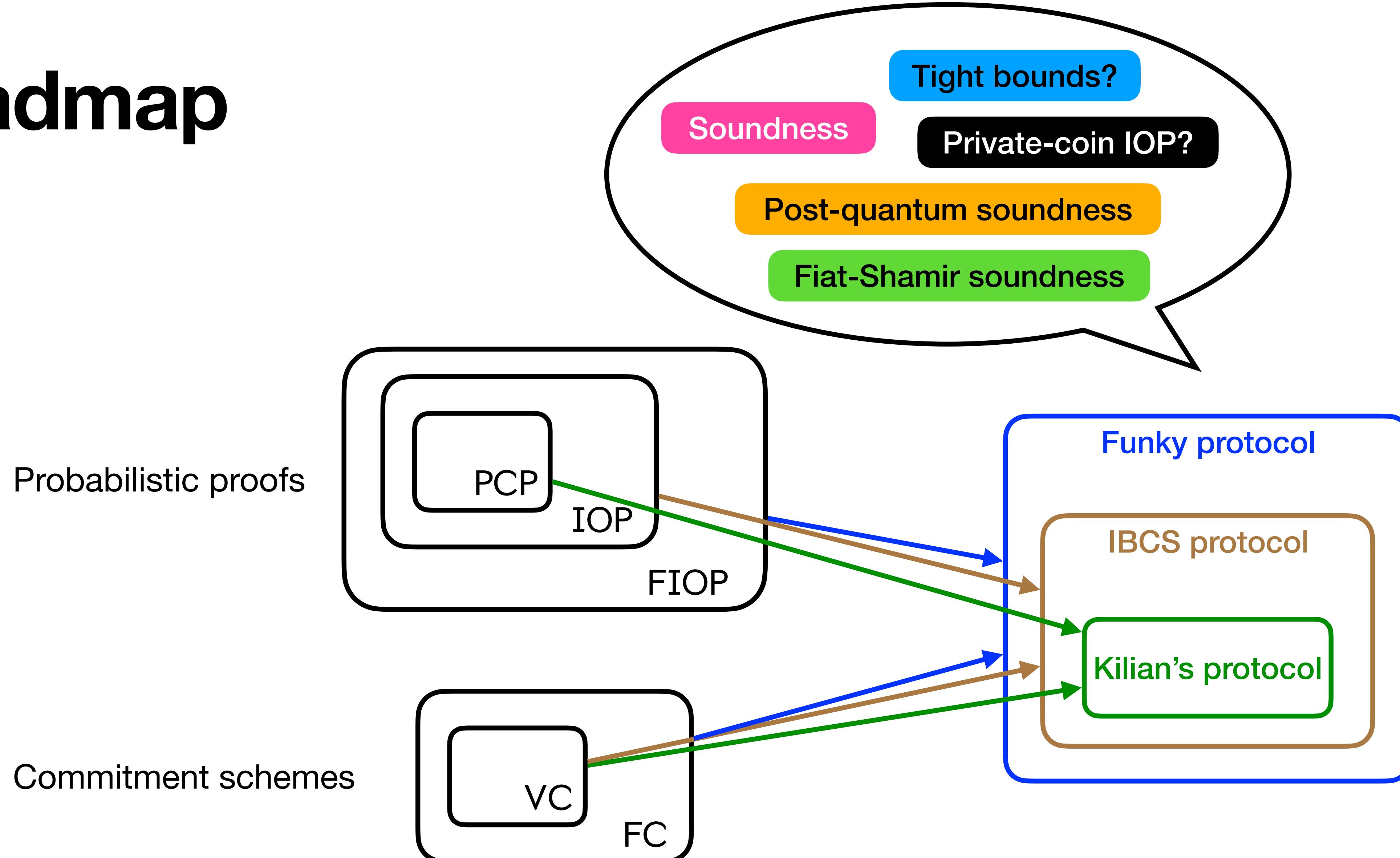
$$\epsilon_{\text{ARG}}^*(t_{\text{ARG}}^*) \leq \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}^*(t_{\text{ARG}}^* \cdot \log(q/\epsilon)) + \epsilon$$

$$\leq \epsilon_{\text{PCP}} + \text{polylog}\left(q \cdot \sqrt{(t_{\text{ARG}}^*)^2/2^\lambda}\right) \cdot O\left(\sqrt[2]{(t_{\text{ARG}}^*)^2/2^\lambda}\right)$$

small factor

We achieved $\epsilon_{\text{ARG}}^* \leq \epsilon_{\text{PCP}} + \epsilon_{\text{VC}}^*$!

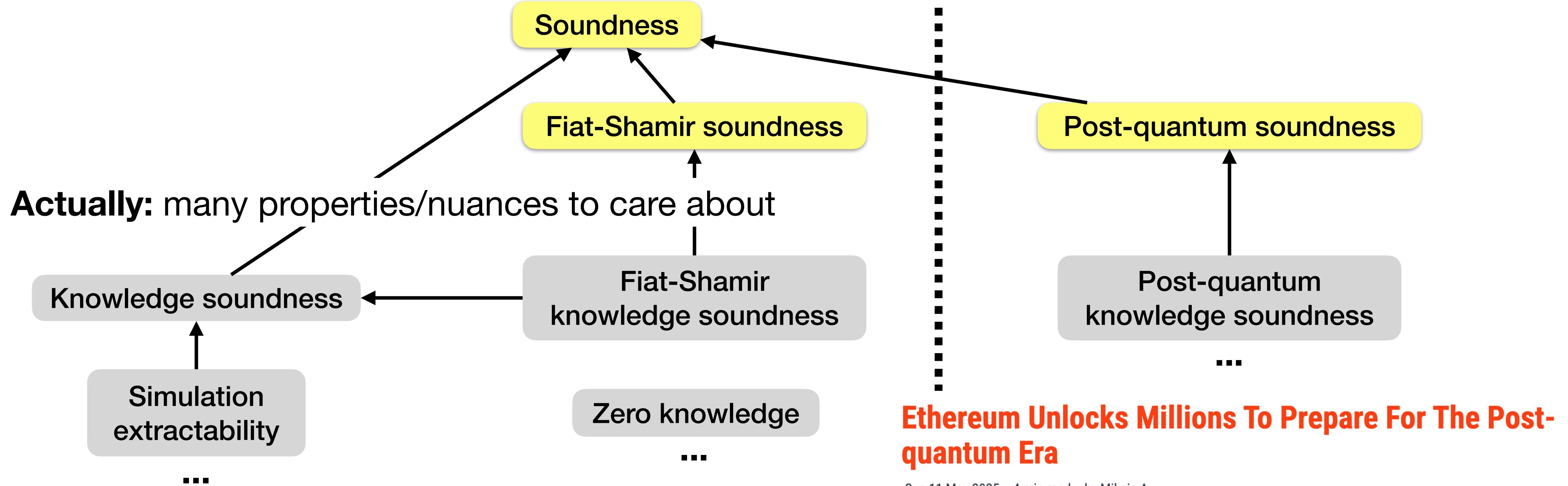
Roadmap



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

On security notions of arguments

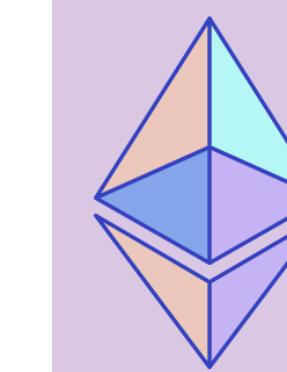
Today: focus on soundness only



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

Strict-time adversary
vs.
Expected-time adversary

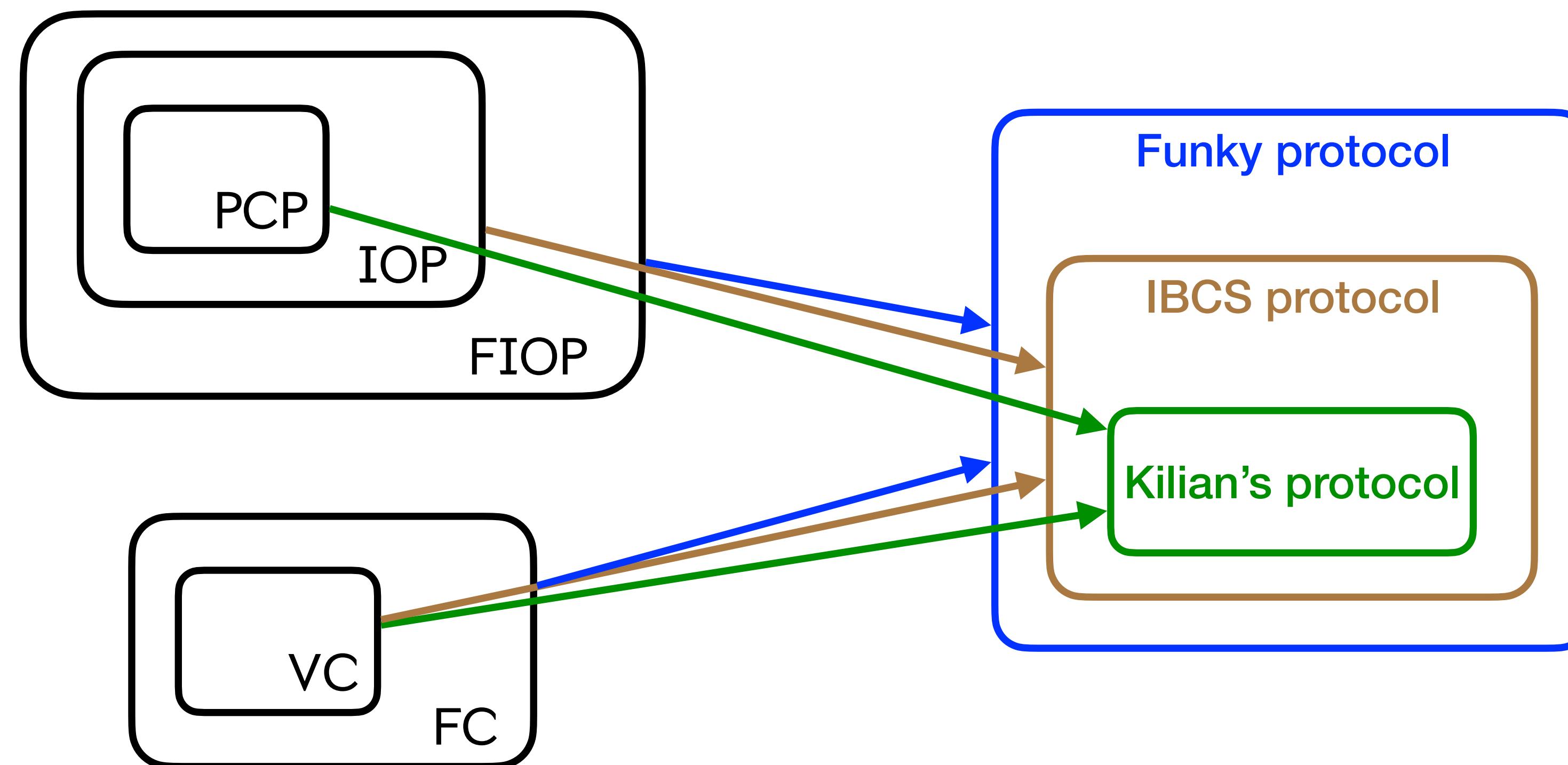
e.g., [BL02] zero-knowledge protocols do not have strict poly-time (black-box) extractor



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

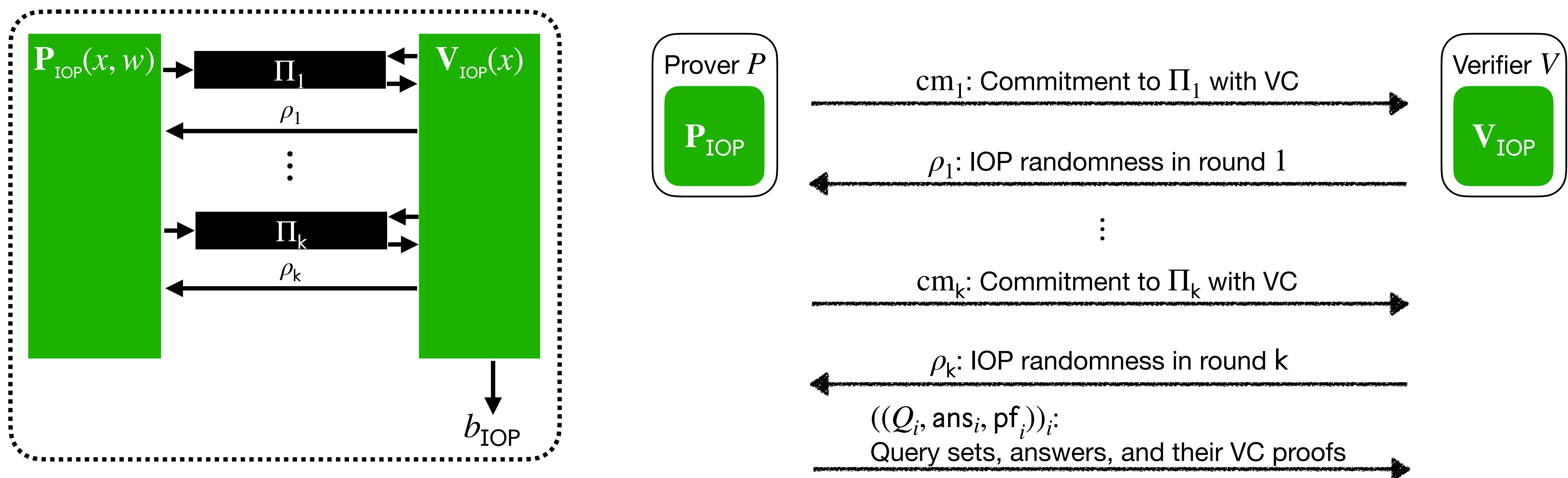


IBCS protocol

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 $\epsilon_{\text{ARG}} \leq \epsilon_{\text{IOP}} + \epsilon_{\text{VC}}$ is not possible... What can we get?

Theorem. $\forall \epsilon > 0$,

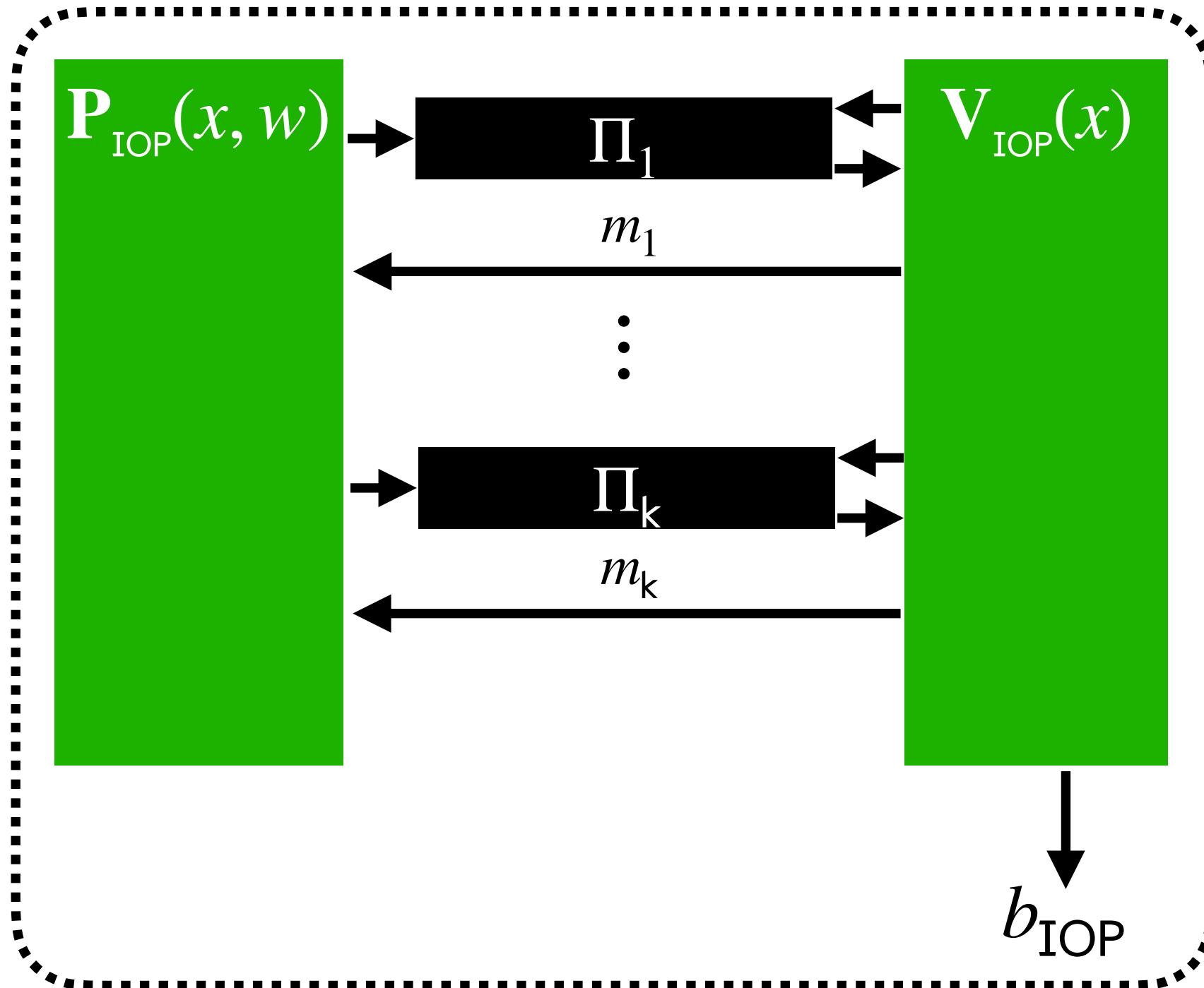
$$\epsilon_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{IOP}} + k \cdot \epsilon_{\text{VC}}(t_{\text{VC}}) + \epsilon, \text{ where } t_{\text{VC}} = O(t_{\text{ARG}} \cdot l/\epsilon).$$

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

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

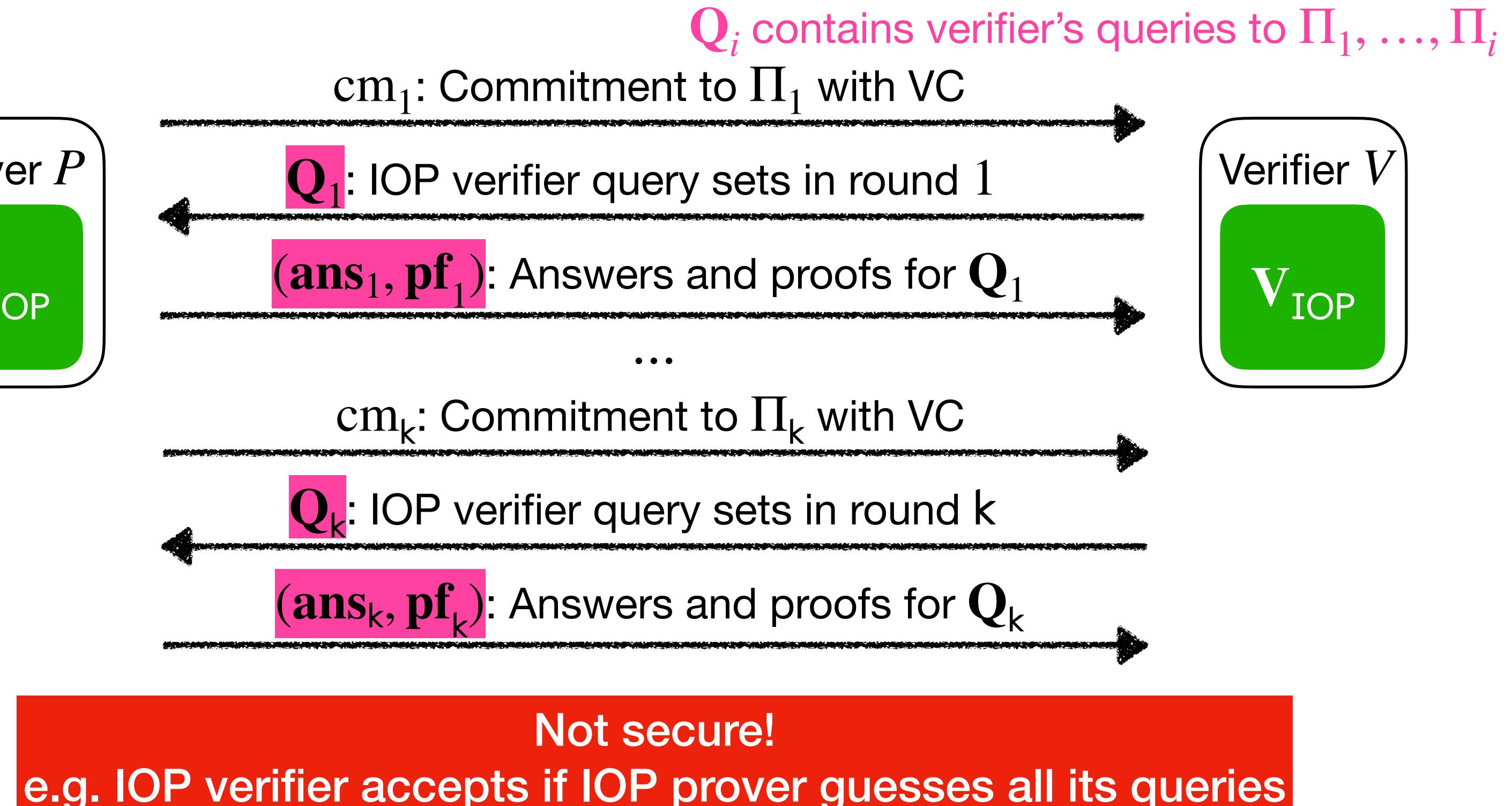
Why do we need public-coin IOPs?

Private-coin interactive oracle proof (IOP)



How about public-query IOPs?

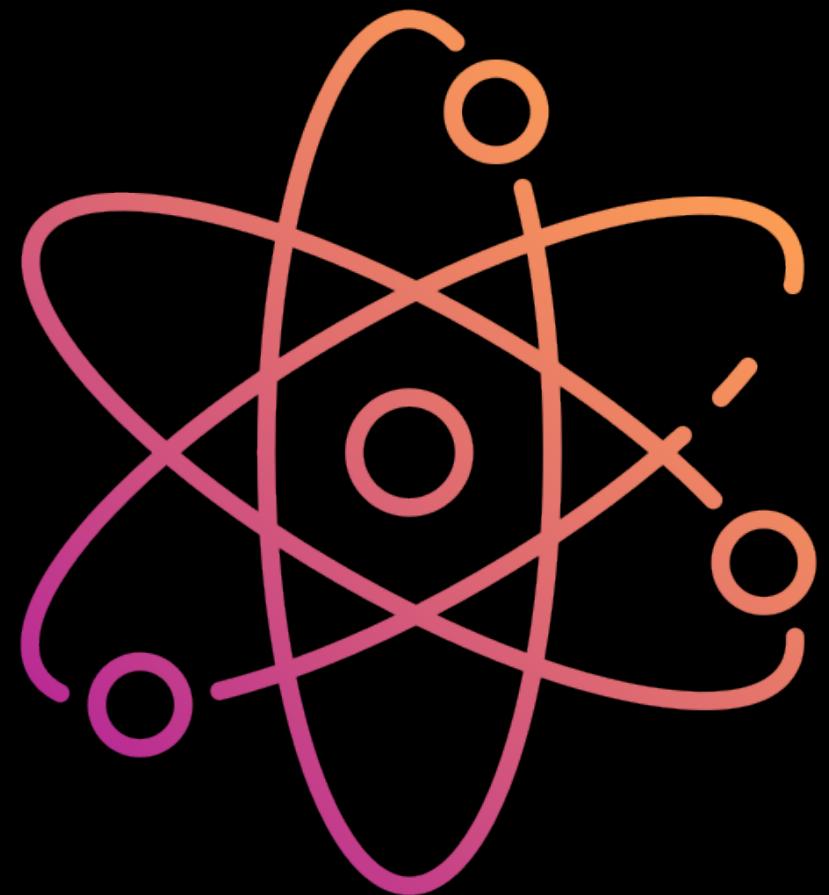
Queries can be learned by the prover (in "real-time")



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?)

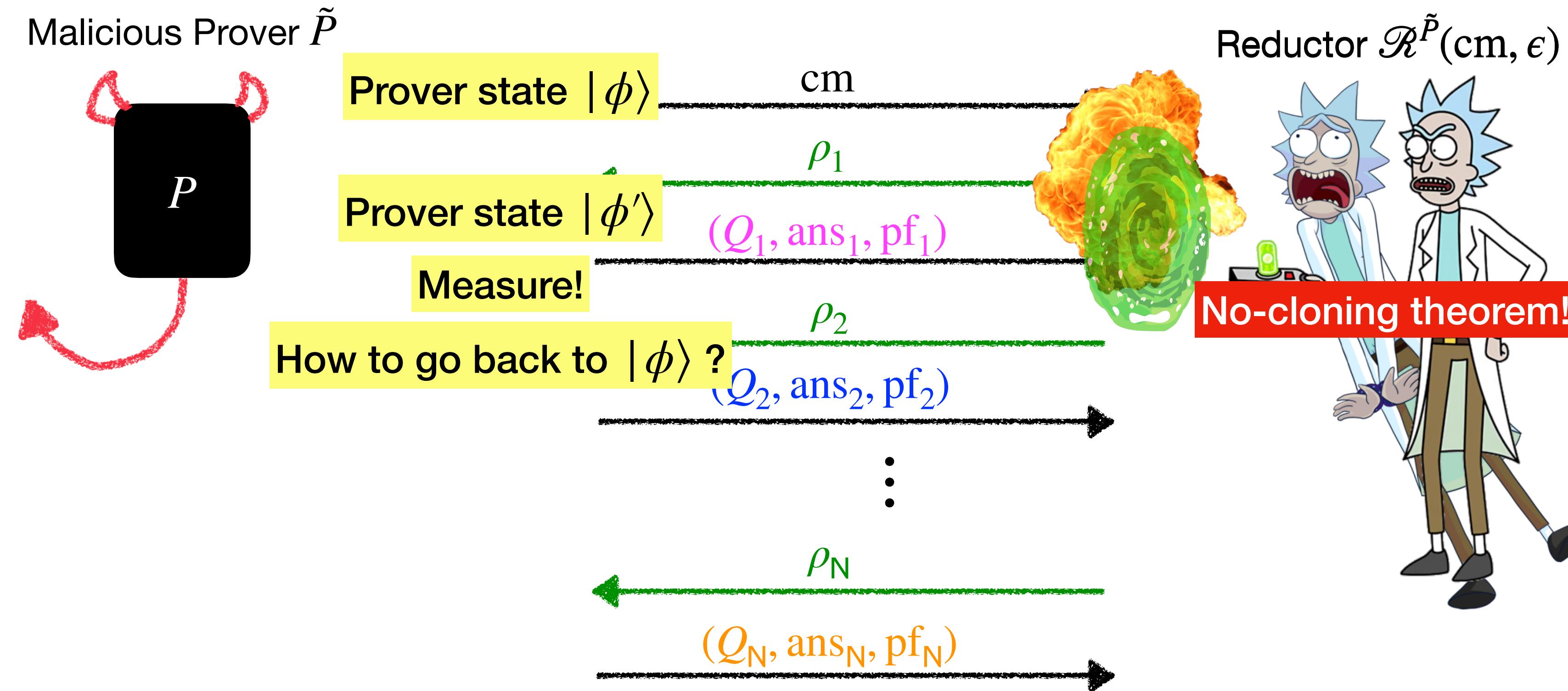


Interlude: **post-quantum** security

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

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

On quantum rewinding



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

Problem: Kilian's protocol needs many rewinds

Recent new tools for quantum rewinding [CMSZ21]:
“repair” the state instead of “rewind”

⇒ 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



Theorem. $\forall \epsilon > 0$,

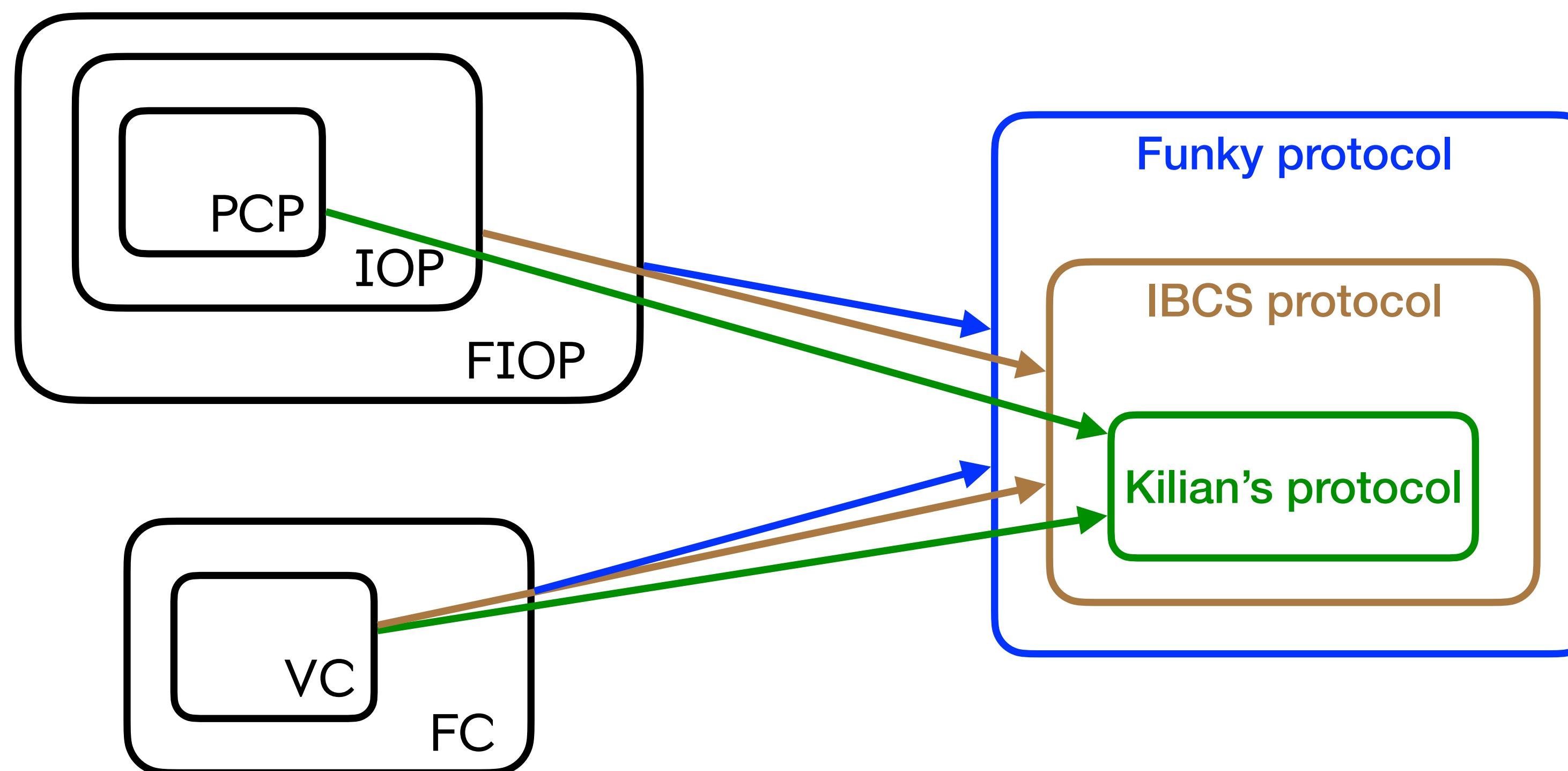
$$\epsilon_{\text{ARG}}^{\text{PQ}}(t_{\text{ARG}}) \leq \epsilon_{\text{IOP}} + k \cdot l \cdot \epsilon_{\text{VCCollapse}}(t_{\text{VC}}) + \epsilon, \text{ where } t_{\text{VC}} = \text{poly}(t_{\text{ARG}} \cdot l/\epsilon).$$

Extra l factor: cost of quantum rewinding

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

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

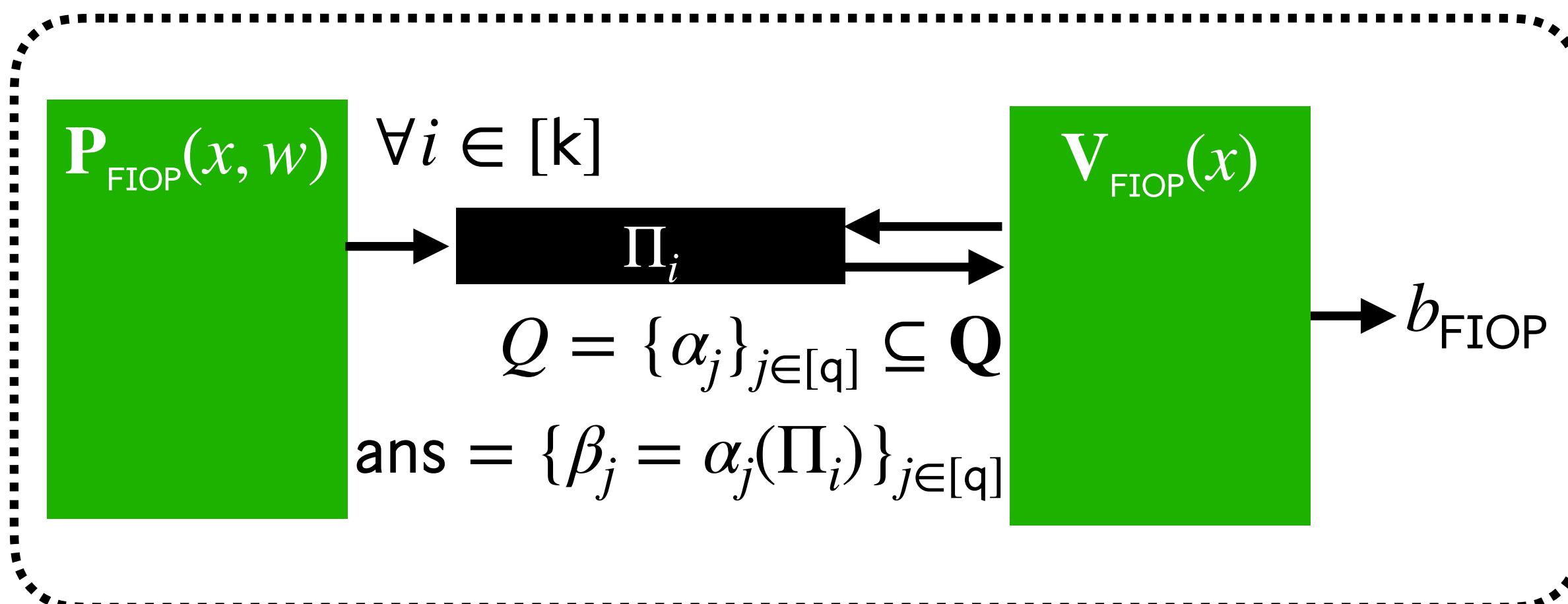


Building blocks

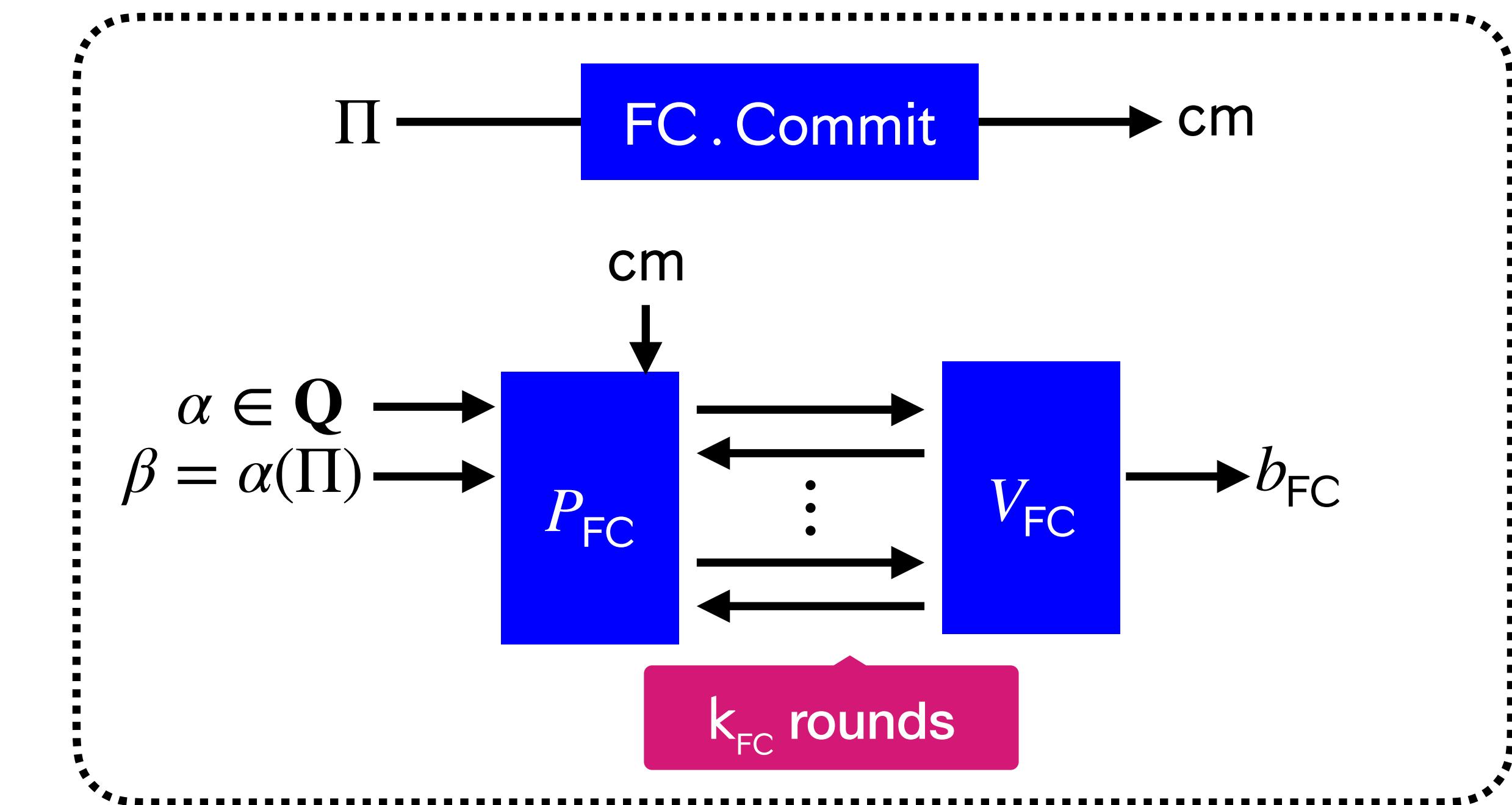
Building block #1: query class \mathbf{Q}

$$\text{- } \mathbf{Q} \subseteq \{\alpha: \Sigma^\ell \rightarrow \mathbb{D}\}$$

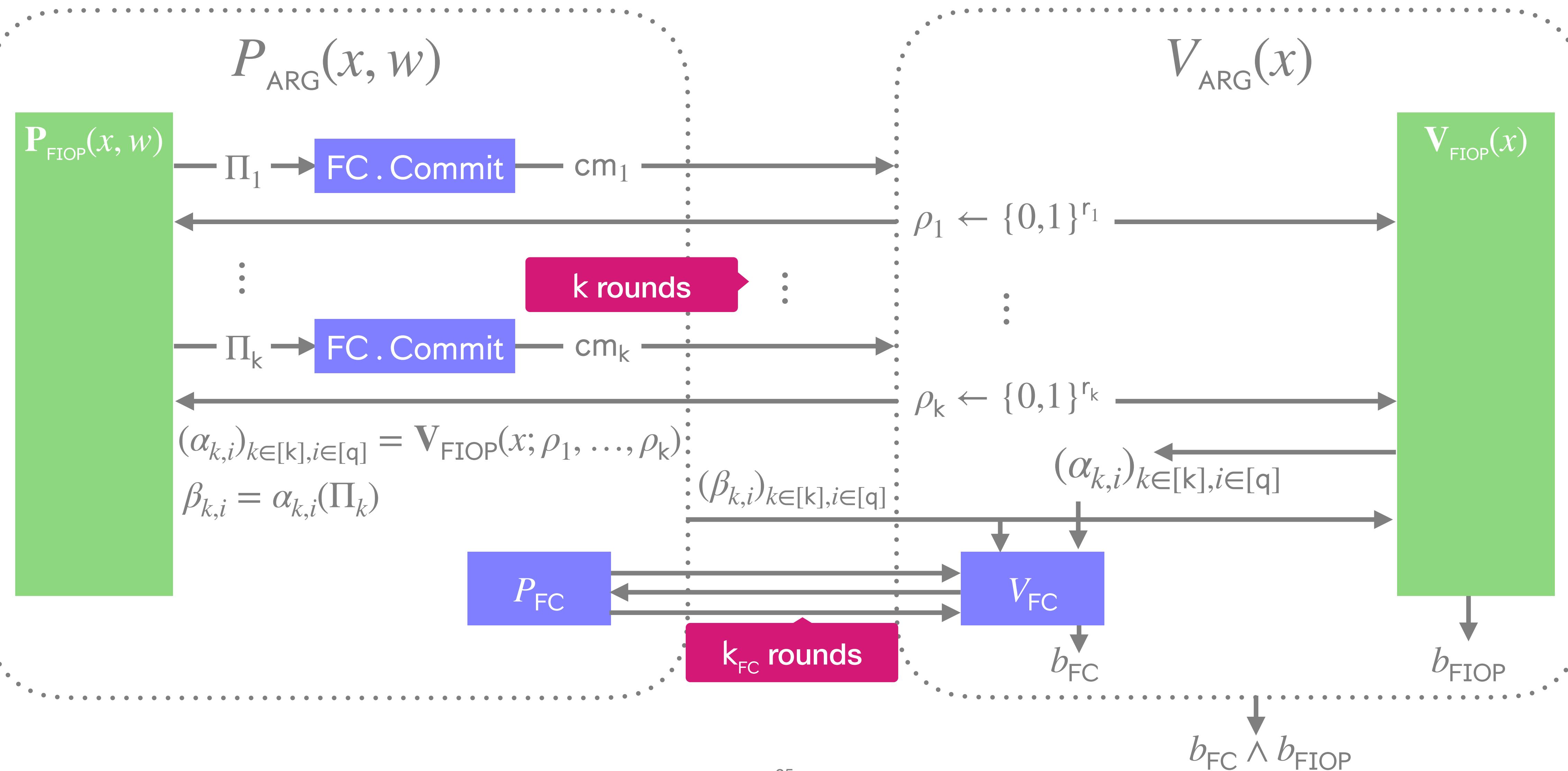
Building block #2: functional interactive oracle proof (FIOP)



Building block #3: functional commitment scheme (FC)



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 $\mathbf{Q}_{\text{point}}$	$\beta = \Pi[\alpha] \text{ for } \alpha \in [\ell]$
LPCP+LC [LM19]	$\Pi \in \mathbb{F}^\ell$	linear queries \mathbf{Q}_{lin}	$\beta = \sum_{i \in [\ell]} \Pi[i] \cdot \alpha[i] \text{ for } \alpha \in \mathbb{F}^\ell$
PIOP+PC [CHM+20,BFS20]	$\Pi \in \mathbb{F}[X]^{\leq D}$	evaluation queries on polynomials \mathbf{Q}_{poly}	$\beta = \sum_{i \in [\ell]} \Pi[i] \cdot \alpha^{i-1} \text{ for } \alpha \in \mathbb{F}$
PIOP*+PC* [GWC19]	$\Pi \in (\mathbb{F}[X]^{\leq D})^{m+n} = (f_1, \dots, f_m, g_1, \dots, g_n)$	evaluation queries on structured polys $\mathbf{Q}_{\text{poly}*}$	$\beta = \sum_{k \in [n]} h_k(f_1(\alpha), \dots, f_m(\alpha)) \cdot g_k(\alpha)$

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
Funky protocol is everywhere		
 Succinct	 RISC ZERO	 Ligero
 STARKWARE	 Aztec	 VALIDA
 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

$$\epsilon_{\text{ARG}} \approx \epsilon_{\text{IOP}} + \epsilon_{\text{VC}}^{\text{PB}}$$

Vector Commitments

position binding:

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

[LM19] LPCP+LC

$$\epsilon_{\text{ARG}} \approx \epsilon_{\text{LPCP}} + \epsilon_{\text{LC}}^{\text{FB}}$$

Linear Commitments

function binding:

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

[CHMMW20, BFS20] PIOP+PC

$$\epsilon_{\text{ARG}} \approx \epsilon_{\text{PIOP}} + \kappa_{\text{PC}}$$

Polynomial Commitments

binding? strong correctness? interpolation binding? extractability?

[KZG10]

Too strong

[AJMMS23]

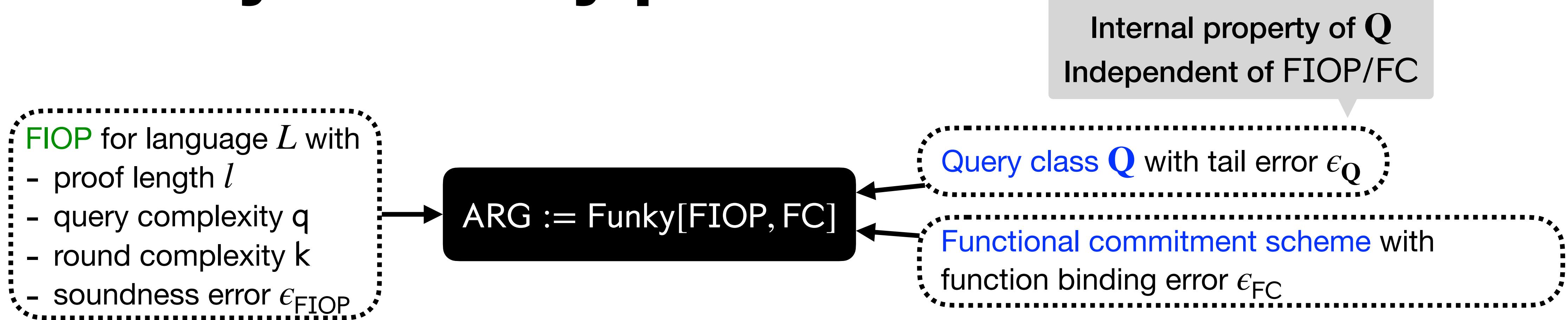
[CHM+20, BFS20]

Functional Commitments

function binding:

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

Security of Funky protocol



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

$$\epsilon_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{FIOP}} + k \cdot \epsilon_{\text{FC}}(t_{\text{FC}}) + k \cdot \epsilon_Q(l, N), \text{ where } t_{\text{FC}} = O(t_{\text{ARG}} \cdot N).$$

TLDR:

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

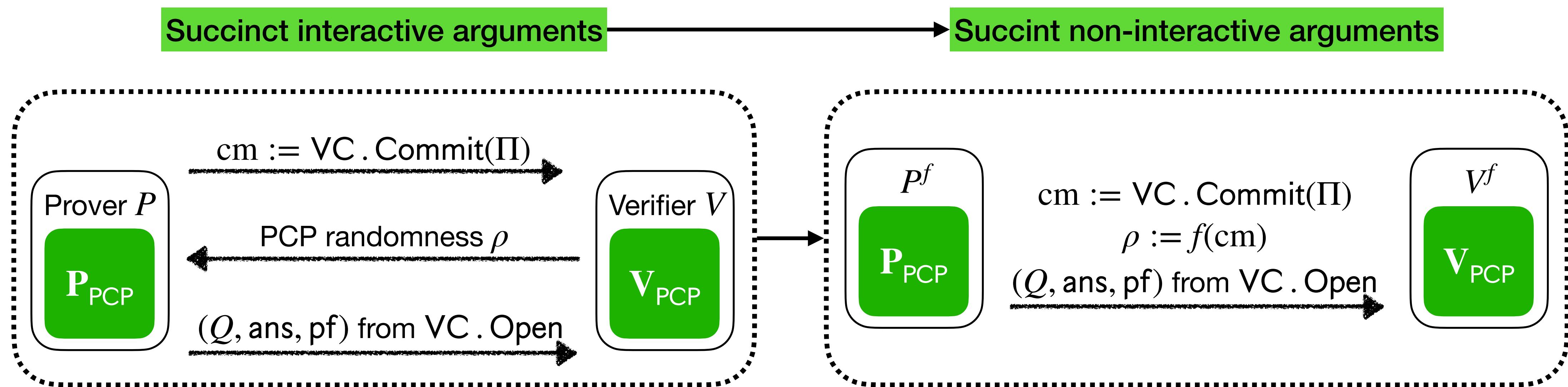
$\epsilon_{Q_{\text{point}}}(l, N) = l/N \implies$ recovers the bounds for Kilian’s protocol and IBCS protocol

Fiat-Shamir security: From succinct arguments to SNARGs

Fiat-Shamir transformation

Random oracle: $\mathcal{O} = \{\mathcal{O}_\lambda\}_{\lambda \in \mathbb{N}}$

\mathcal{O}_λ : uniform distribution over $\{f: \{0,1\}^* \rightarrow \{0,1\}^\lambda\}$



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

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

RO queries

k might be superconstant!

Fiat-Shamir security



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

$$\epsilon_{\text{NARG}}(t_{\text{ARG}}, m_{\text{ARG}}) \leq \epsilon_{\text{FIOB}}^{\text{FS}}(O(m_{\text{ARG}})) + k \cdot \epsilon_{\text{FC}}^{\text{FSFB}}(t_{\text{FC}}, m_{\text{FC}}) + k \cdot \epsilon_Q(l, N), \text{ where } \begin{cases} t_{\text{FC}} = O(t_{\text{ARG}} \cdot N) \\ m_{\text{FC}} = O(m_{\text{ARG}} \cdot k \cdot N) \end{cases}.$$

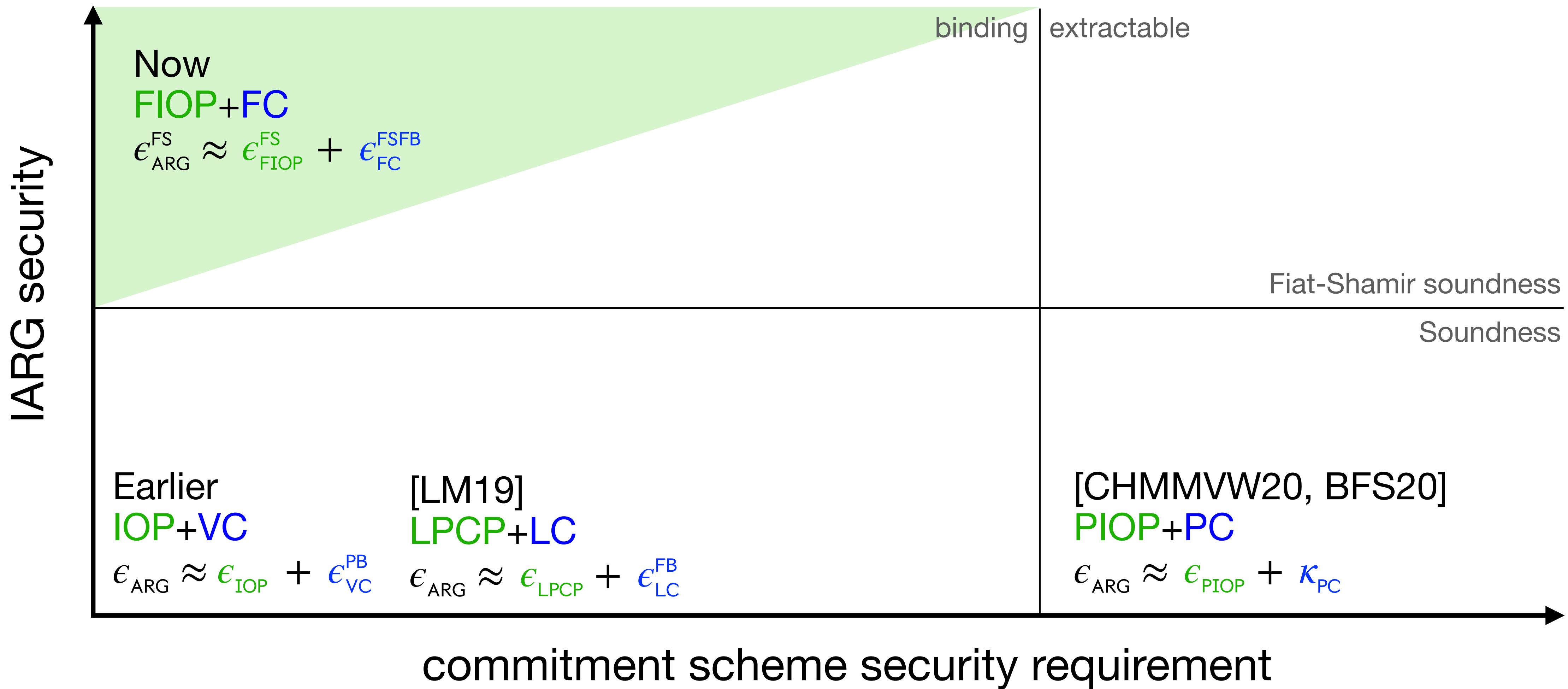
A theorem that generalizes everything we saw (except post-quantum)

Corollary: security analysis of Plonk [GWC19] from falsifiable assumption



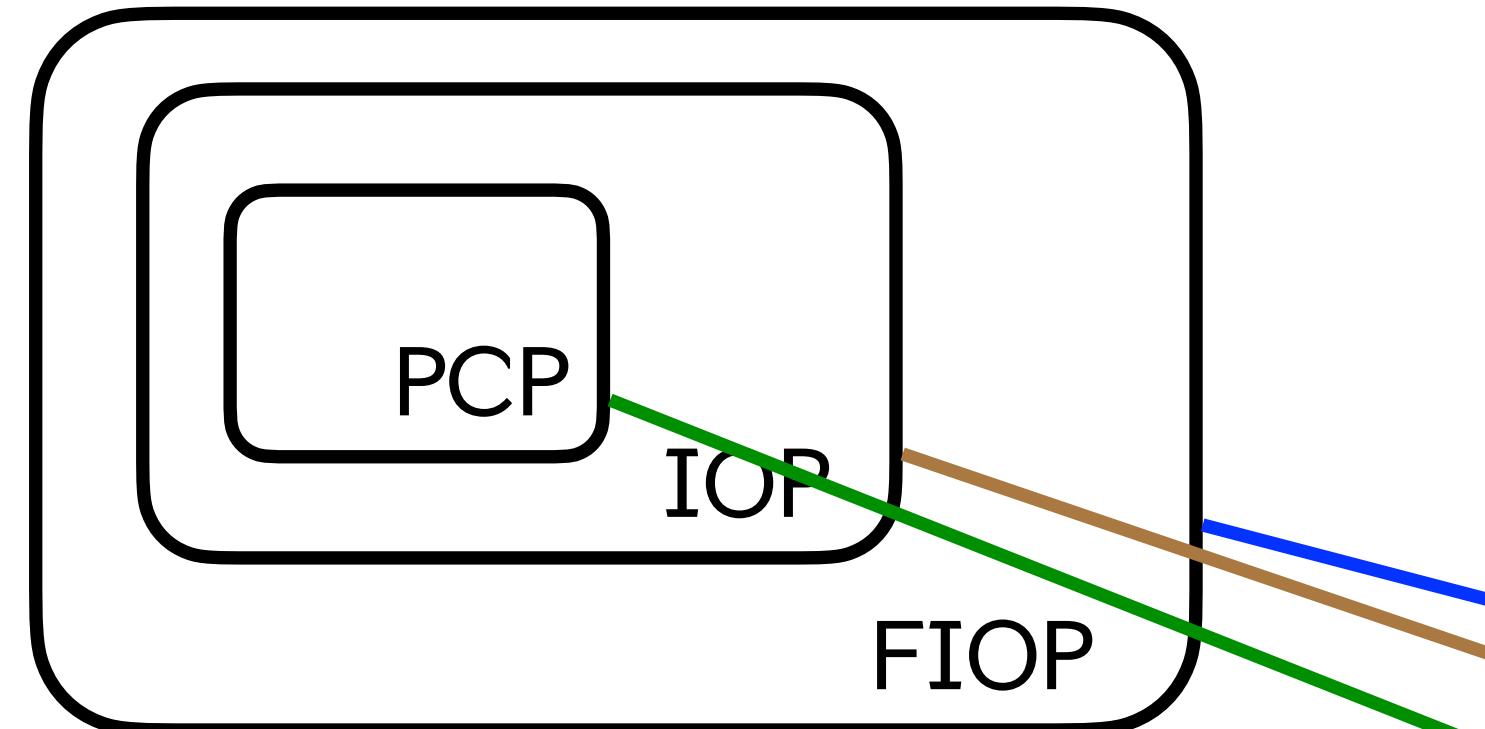
...

Overview: standard-model analyses

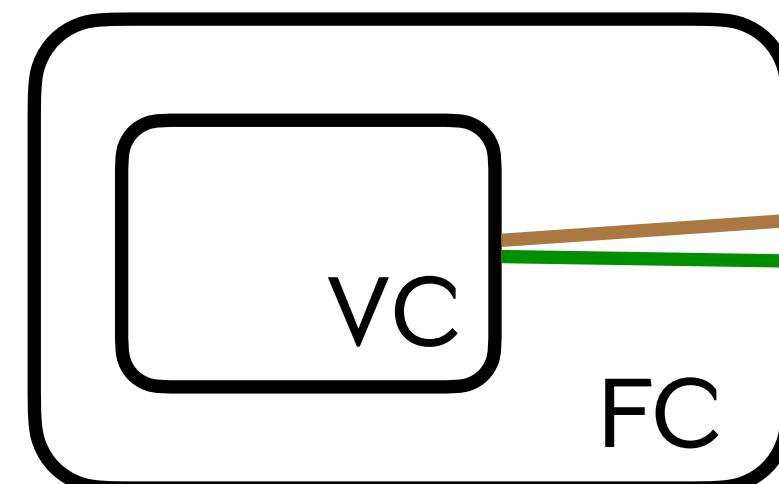


Open problems

Probabilistic proofs



Commitment schemes



Funky protocol

- Soundness
- Fiat-Shamir soundness

Standard model Fiat-Shamir?

Quantum analogue?

Post-quantum security?

Expected-time regime?

Practical security in idealized models?

IBCS protocol

- Soundness
- Private-coin IOPs
- Post-quantum soundness

Public-coin IOPs?

Kilian's protocol

- Soundness
- Lower bounds on soundness

Kilian vs. Sigma protocols?



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.
- [CDGS23]: Alessandro Chiesa, Marcel Dall’Agnol, [Ziyi Guan](#), and Nicholas Spooner. On the Security of Succinct Interactive Arguments from Vector Commitments. ePrint Report 2023/1737.
- [CDGSY24]: 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.
- [CDDGS24]: Alessandro Chiesa, Marcel Dall’Agnol, Zijing Di, [Ziyi Guan](#), and Nicholas Spooner. “Quantum Rewinding for IOP-Based Succinct Arguments”. arXiv:2411.05360.
- [CGKY25]: 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.

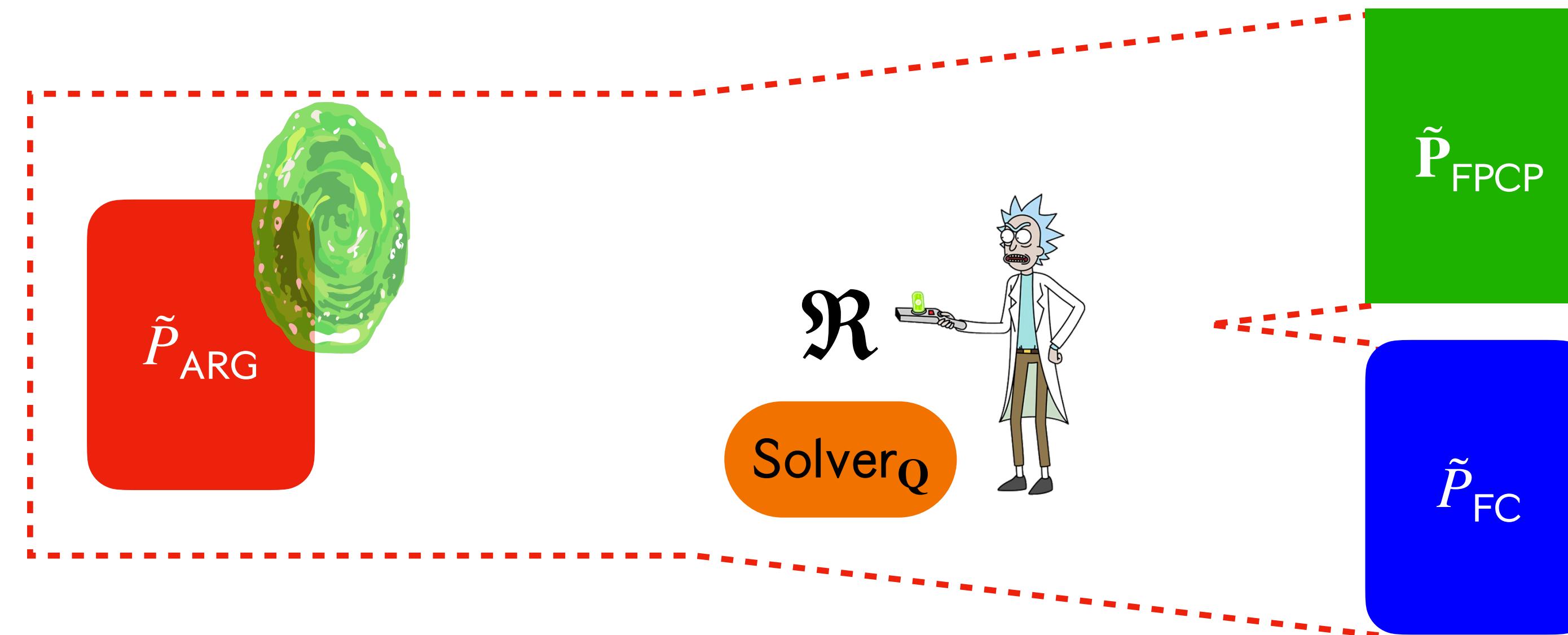
Security of Funky from FPCP and non-interactive FC

Security reduction for Funky[FPCP, FC]

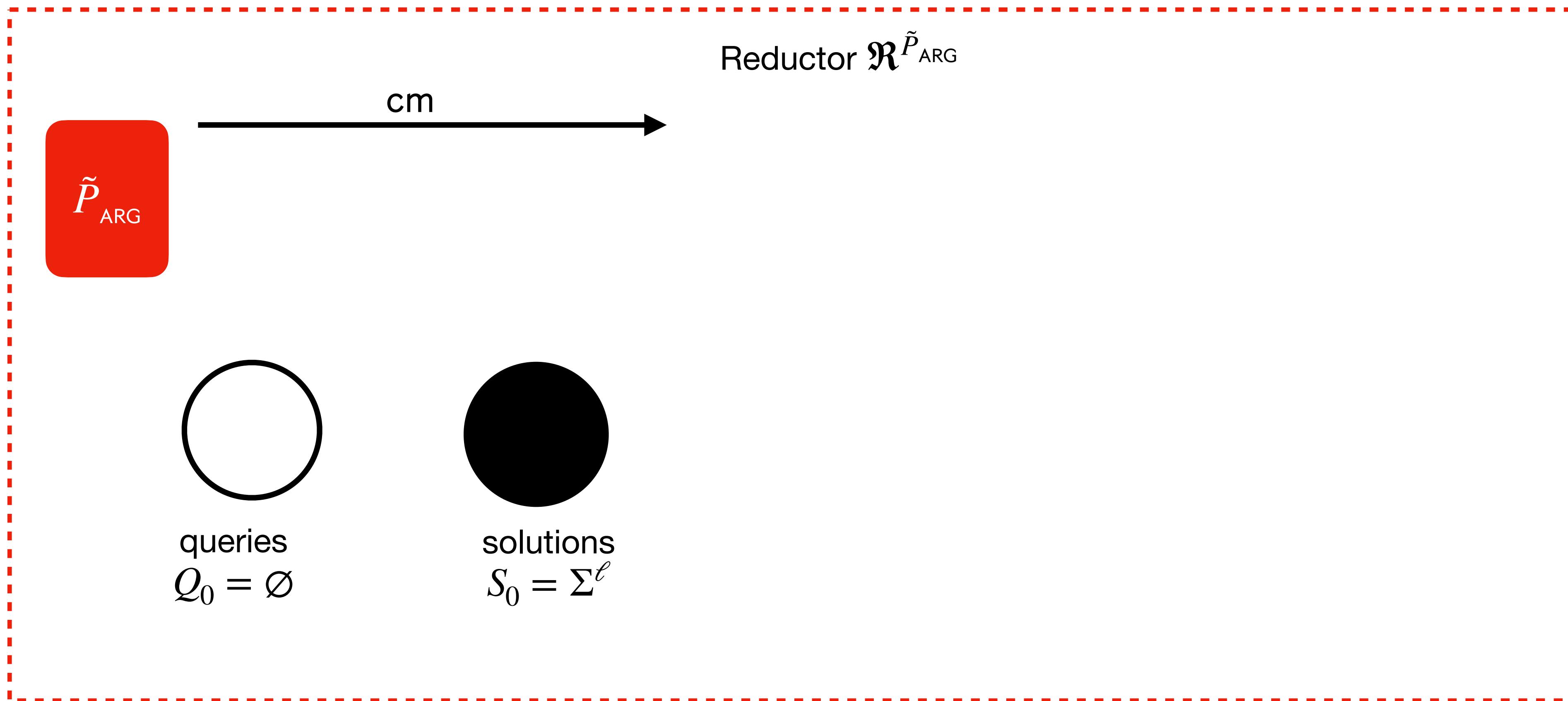
Goal:

(for FPCPs and non-interactive FCs)

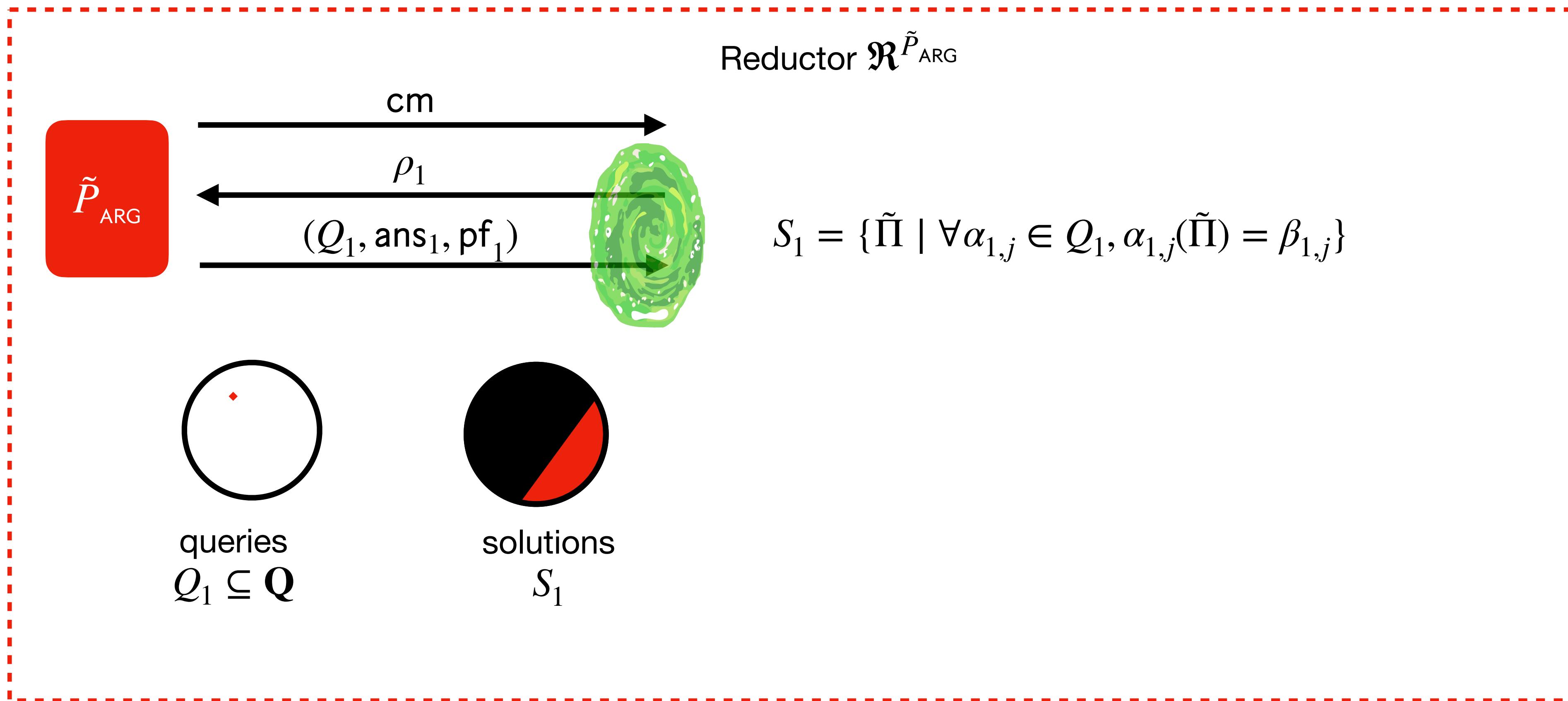
$$\epsilon_{\text{ARG}}(t_{\text{ARG}}) \leq \epsilon_{\text{FIOP}} + k \cdot \epsilon_{\text{FC}}(t_{\text{FC}}) + k \cdot \epsilon_Q(l, N), \text{ where } t_{\text{FC}} = O(t_{\text{ARG}} \cdot N)$$



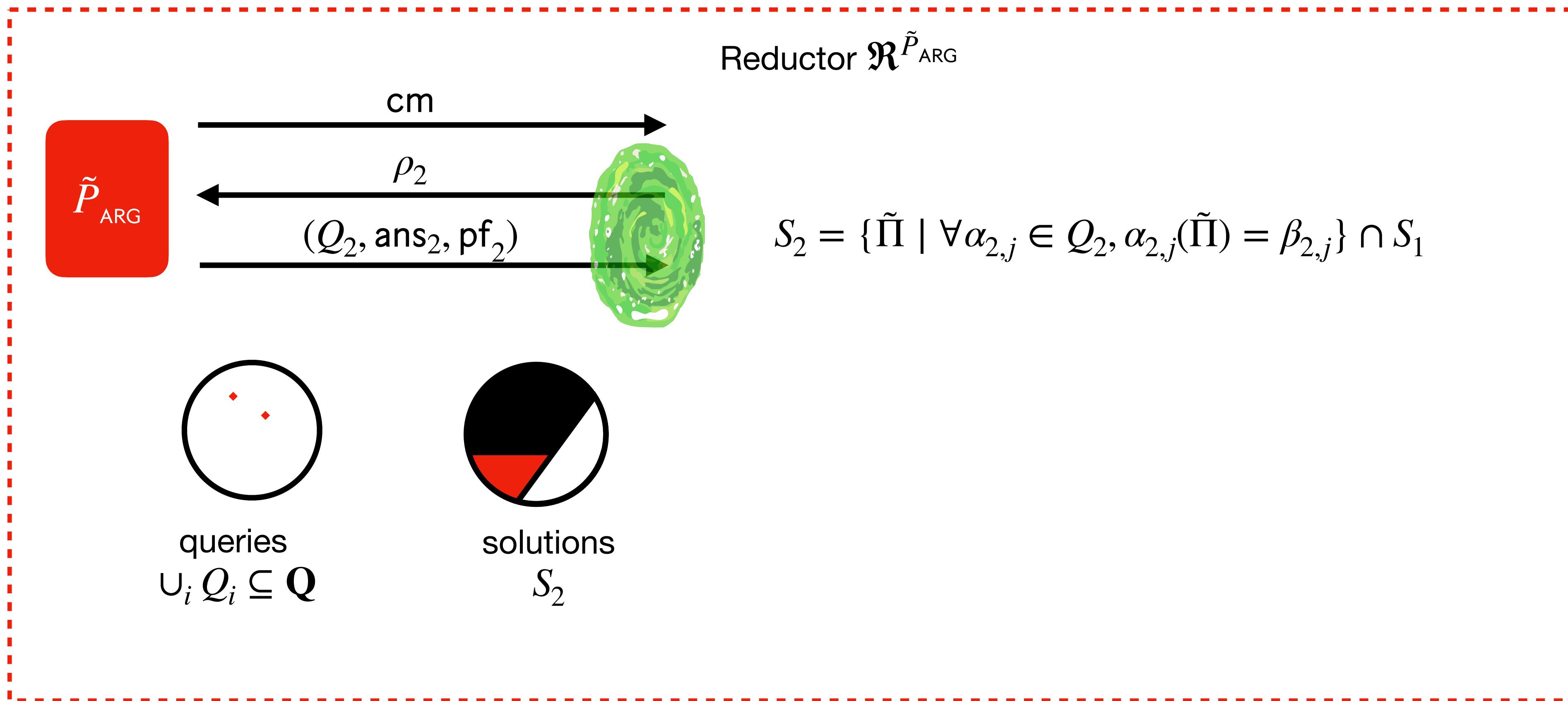
Security reduction for Funky[FPCP, FC]



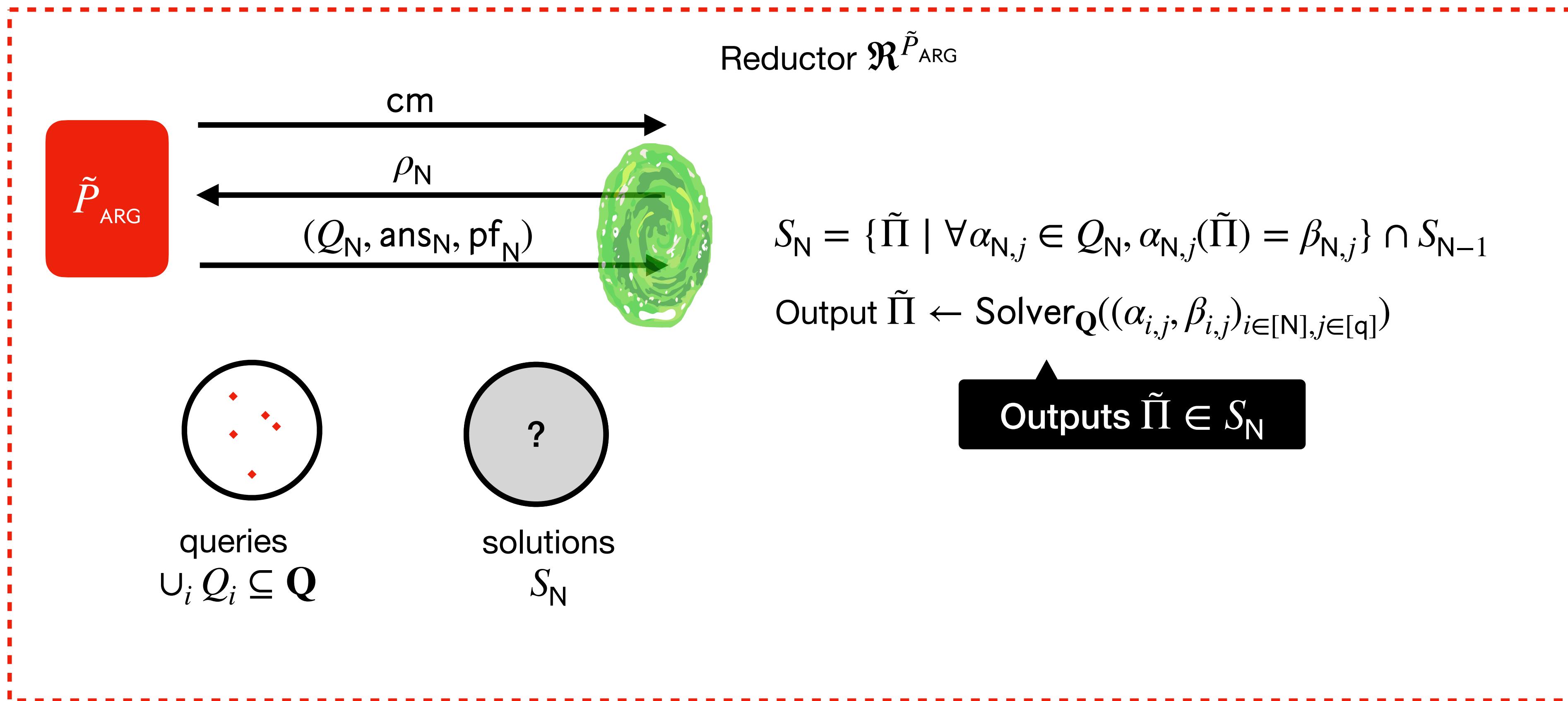
Security reduction for Funky[FPCP, FC]



Security reduction for Funky[FPCP, FC]



Security reduction for Funky[FPCP, FC]



Security reduction for Funky[FPCP, FC]

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

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

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

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

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

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

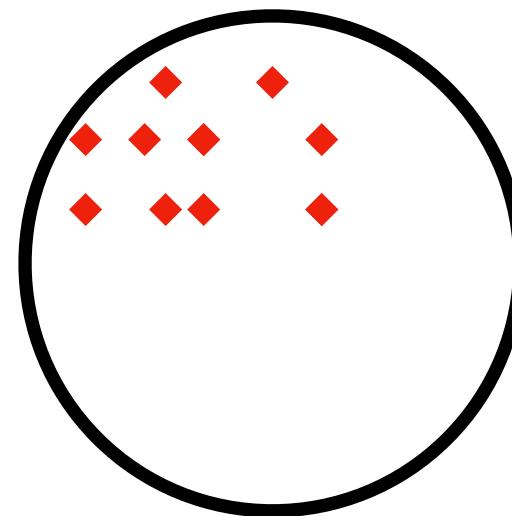
- Either (Q, ans) is inconsistent with $\tilde{\Pi}$; or
- (Q, ans) contains “new queries”

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

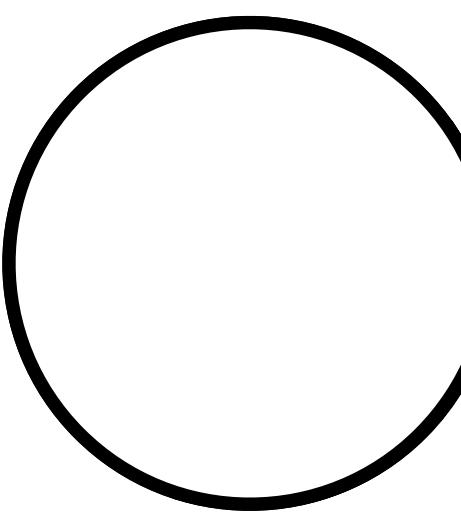
$S_{N+1} \neq \emptyset \wedge S_{N+1} \neq S_N$
 \rightarrow tail error of the query class Q

Security reduction lemma

queries $\cup_i Q_i$



solutions S_i



Case 1:

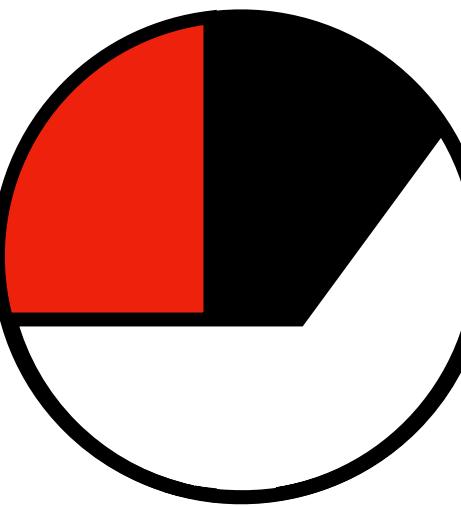
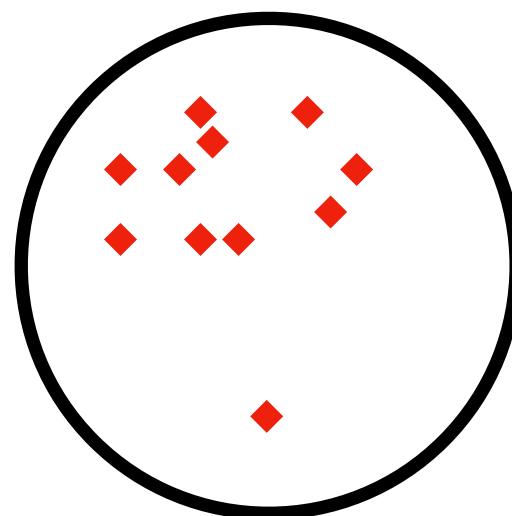
$$\Pr \left[\begin{array}{l} \exists \tilde{\Pi} : \forall \alpha \in \cup_i Q_i : \alpha(\tilde{\Pi}) = \text{ans}[\alpha] \\ \text{Yet all FC checks pass} \end{array} \right] \leq \epsilon_{\text{FC}}(t_{\text{FC}})$$

Function binding

$S_{N+1} = \emptyset$ (no solution)

\rightarrow FC verifier accepts all FC proofs

Case 2:



$i = N + 1$

$S_{N+1} \neq \emptyset \wedge S_{N+1} \neq S_N$

\rightarrow tail error of the query class Q

Internal property of Q
Independent of FIO/P/FC

$$\Pr [S_{N+1} \neq \emptyset \wedge S_{N+1} \neq S_N] \leq \epsilon_Q(\ell, N)$$

Tail error

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