On Extractability of the KZG Family of Polynomial Commitment Schemes

Kristýna Mašková


J. Belohorec

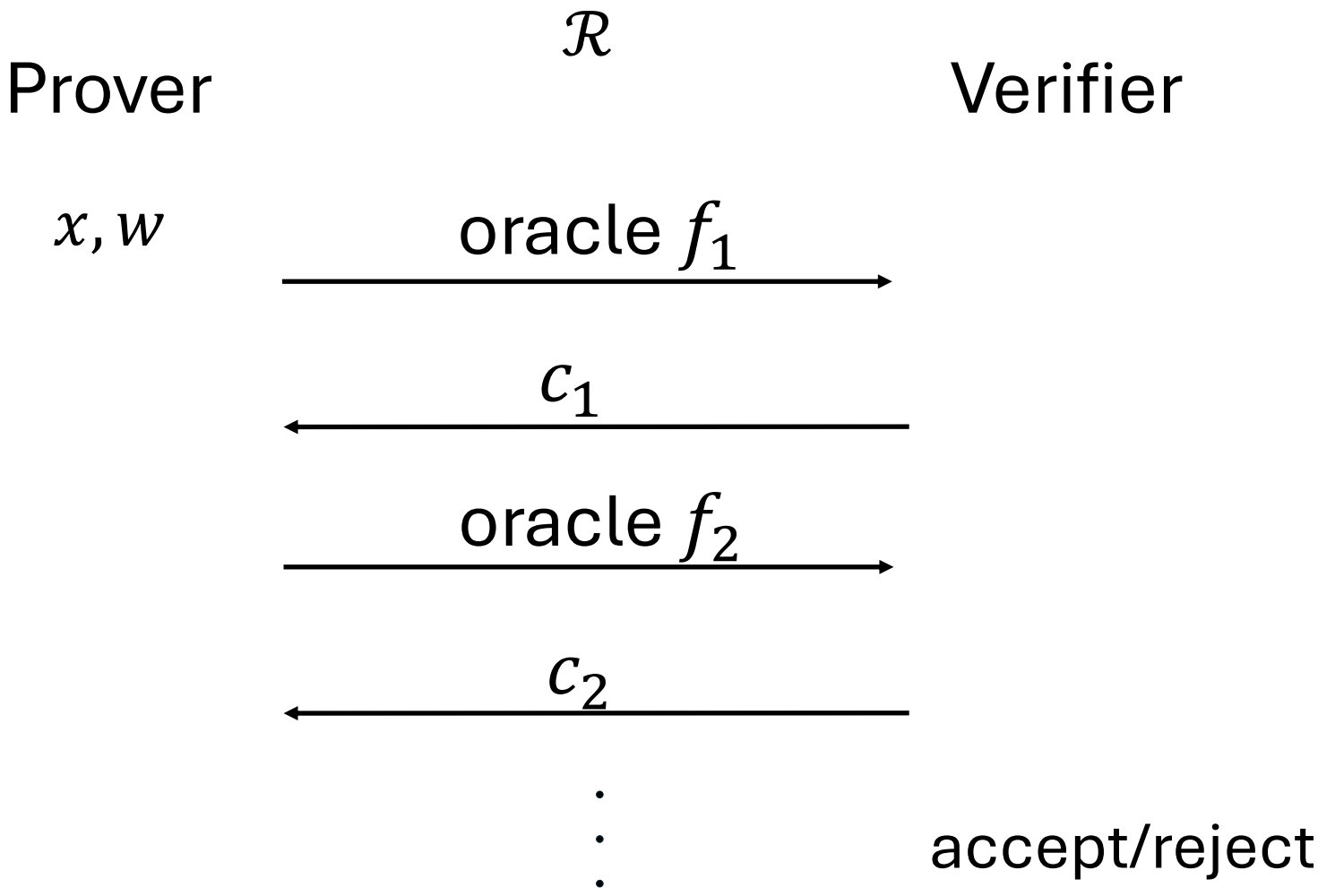

P. Dvořák


Ch. Hoffmann

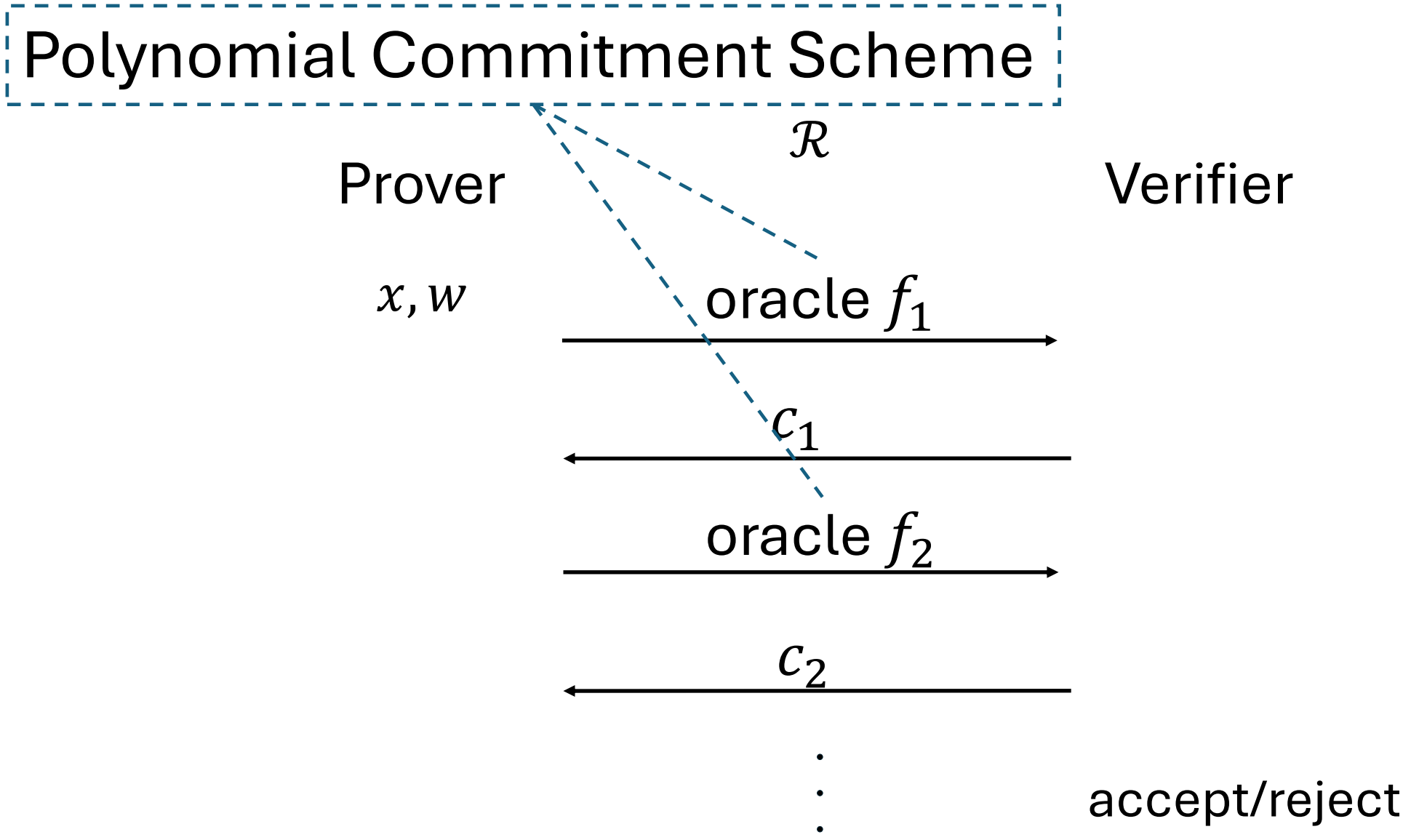

P. Hubáček


M. Pastyřík

Polynomial Interactive Oracle Proof → SNARK



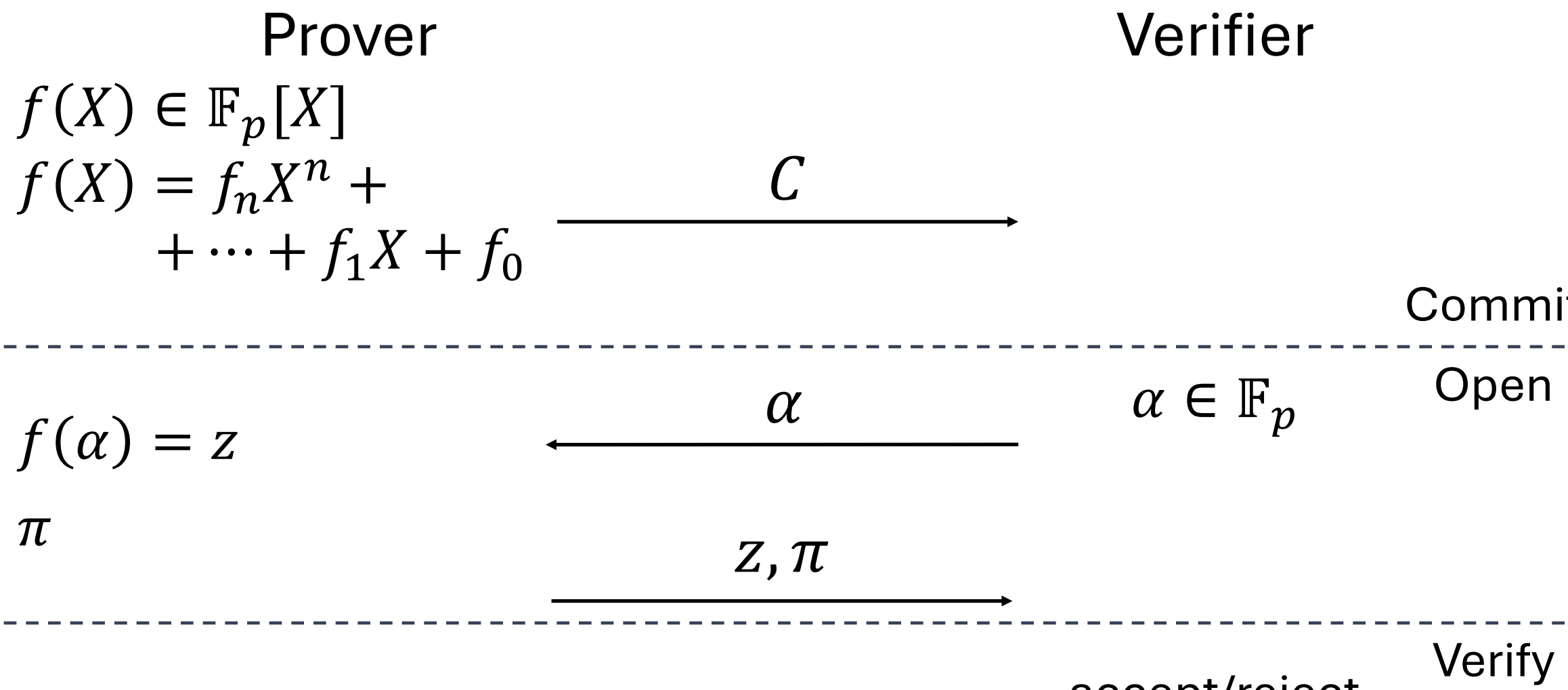
Polynomial Interactive Oracle Proof → SNARK



Related Work

	Scheme	Proof in	Security	Assumption / Model
Plonk, Halo 2 etc.	Univariate KZG [KZG10]	[KZG10]	Evaluation Binding	SDH
		[CFF+20]	Extractability	AGM
		[LPS23]	Extractability	AGMOS (FPR + TOFR)
		[LPS24]	Extractability	ARSDH
Sumchek based SNARKS	Multivariate KZG [PST13]	[PST13]	Evaluation Binding* *on average	SBDH
		[ZGK17]	Extractability* *modified scheme	Power Knowledge of Exponent (non-falsifiable)
		Our work	Extractability	ARSDH(n)

Polynomial Commitments [KZG10]



Evaluation Binding

Prover

???

Verifier

C

Commit

Open

$\alpha \in \mathbb{F}_p$

α

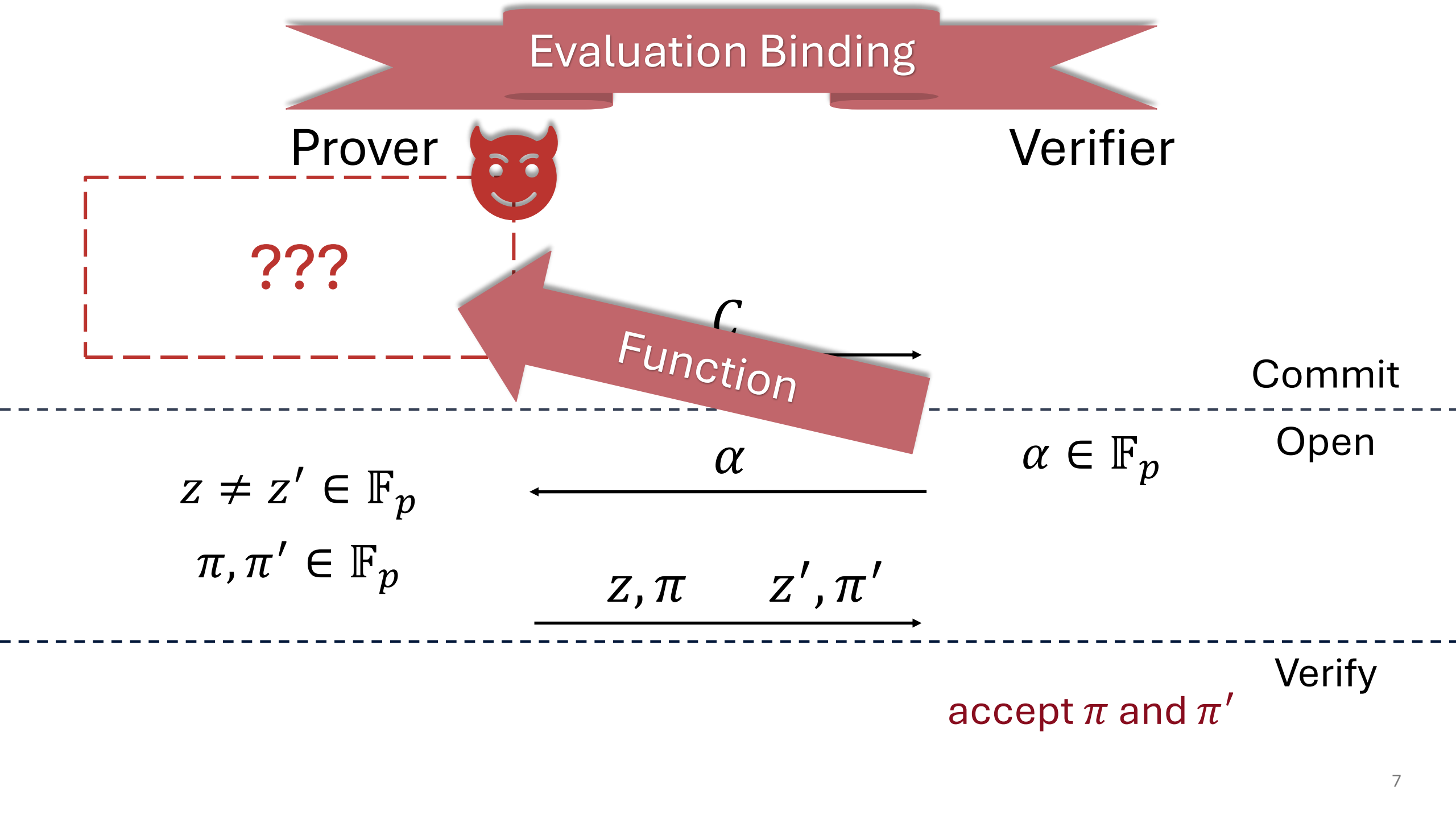
$z \neq z' \in \mathbb{F}_p$

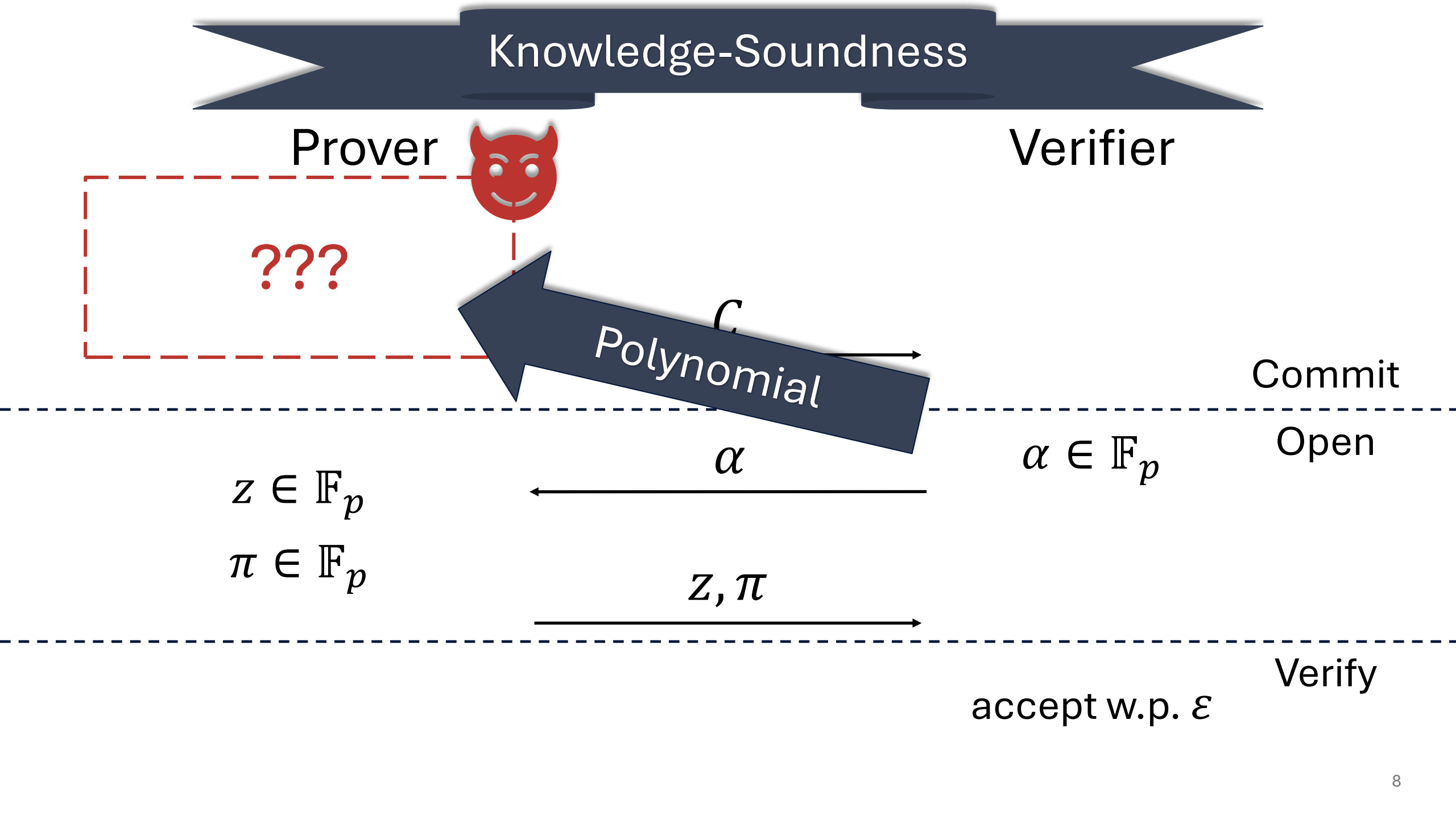
$\pi, \pi' \in \mathbb{F}_p$

$z, \pi \quad z', \pi'$

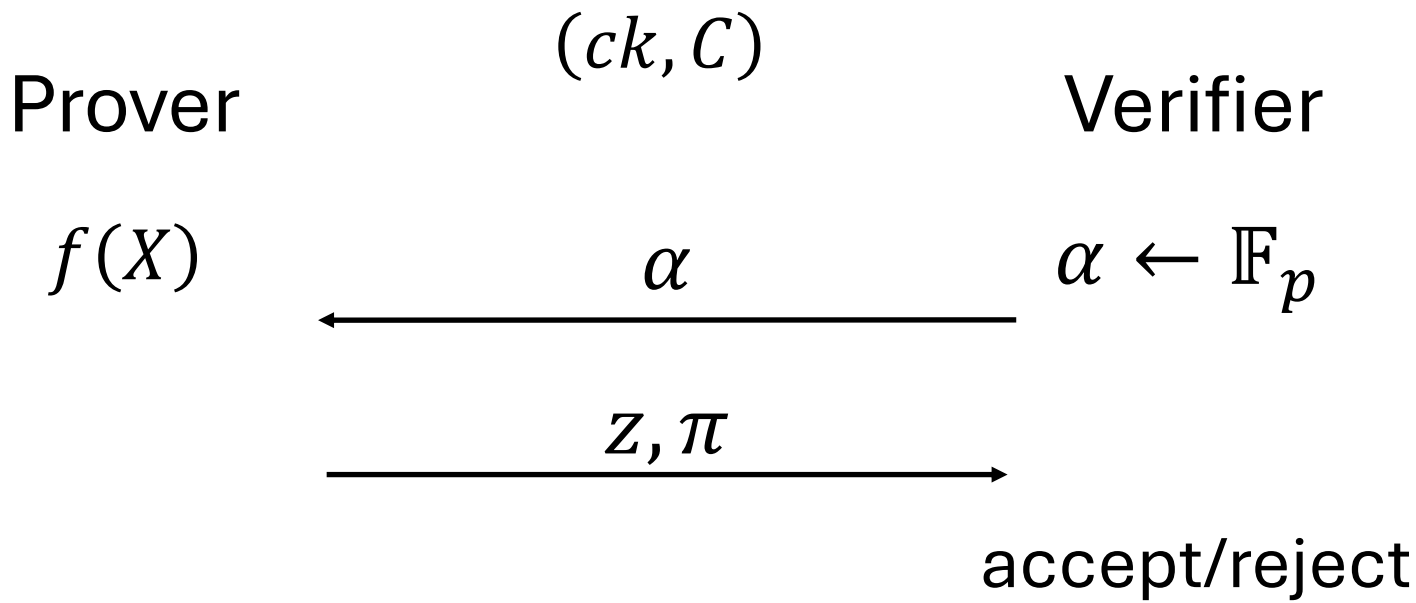
Verify

accept π and π'


Evaluation Binding
Prover
Verifier
???
Function
C
Commit
Open
$\alpha \in \mathbb{F}_p$
α
$z \neq z' \in \mathbb{F}_p$
$\pi, \pi' \in \mathbb{F}_p$
z, π
z', π'
Verify
accept π and π'

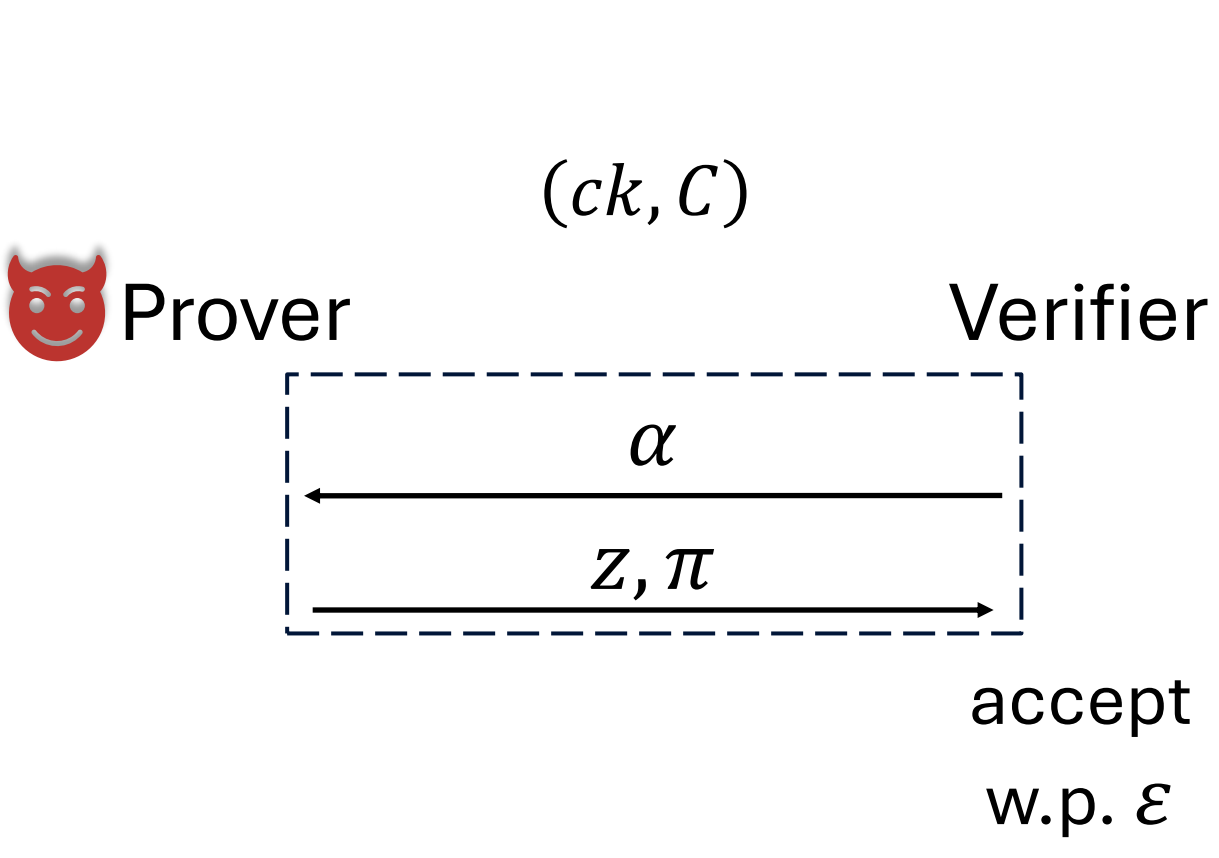

Knowledge-Soundness
Prover
Verifier
???
C
Polynomial
Commit
Open
α
$\alpha \in \mathbb{F}_p$
$z \in \mathbb{F}_p$
$\pi \in \mathbb{F}_p$
z, π
Verify
accept w.p. ε

Proof of Knowledge of a Polynomial (PoKoP)

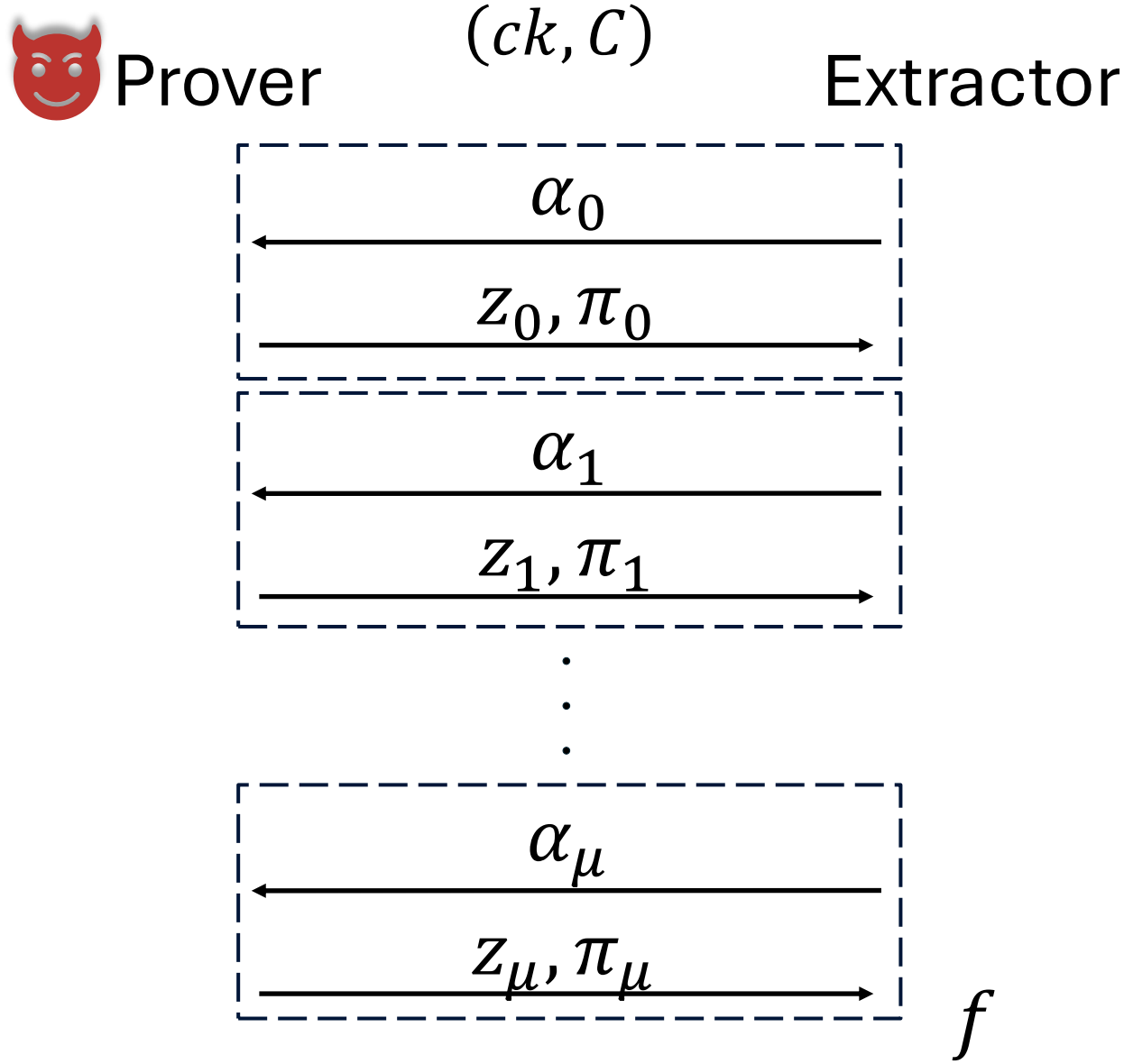


- New notion
- Sufficient for PIOP → SNARK compilers
- Useful for rewinding

Knowledge-Soundness

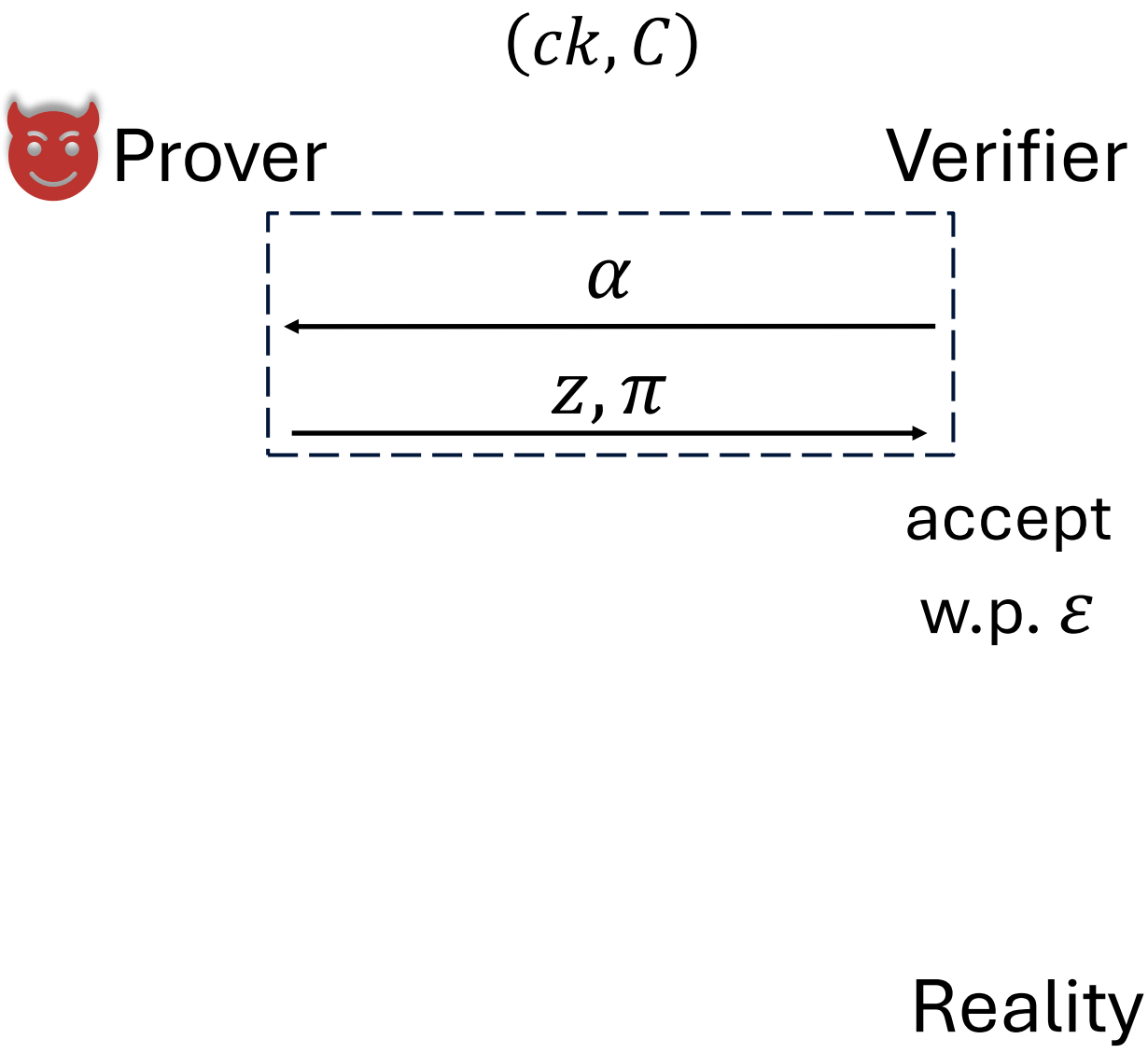


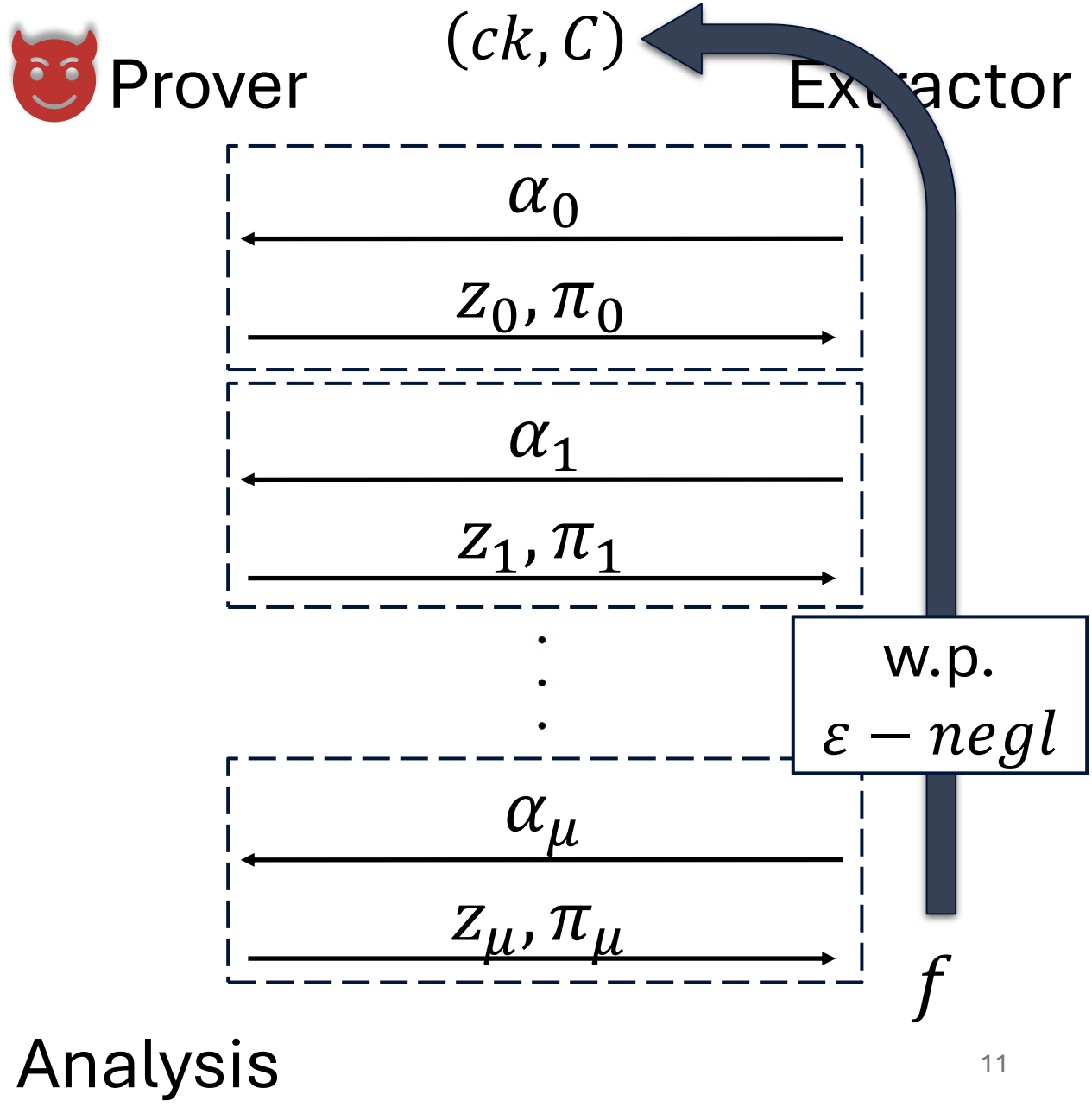
Reality



Analysis

Knowledge-Soundness





Univariate KZG [KZG10]

$$f(\alpha) = z$$

$$\Updownarrow$$

$$f(X) - z = q(X)(X - \alpha)$$

Univariate KZG [KZG10]

$$t \leftarrow \mathbb{F}_p$$
$$ck = \{[t^1]_1, \ldots, [t^n]_1, [t]_2\}$$

ck

Prover — Verifier

$C = [f(t)]_1$ — C → — Commit

Open

$f(\alpha) = z$ — α ← — $\alpha \in \mathbb{F}_p$

$\pi = [q(t)]_1$ — z, π →

Verify

$$(C - [z]_1) \circ [1]_2 = \pi \circ [t - \alpha]_2$$

$\mathbb{G}_1 = \langle [1]_1 \rangle$
$[a]_1 = a \cdot [1]_1$
$\circ: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
$[a]_1 \circ [b]_2 = [ab]_T$

Multivariate KZG [PST13]

$$f(\alpha_1, \ldots, \alpha_n) = z$$

$$\Updownarrow$$

$$f(X_1, \ldots, X_n) - z = \sum_{i=1}^{n} q_i(X_1, \ldots, X_n)(X_i - \alpha_i)$$

Multivariate KZG [PST13]

$$t_1, \dots, t_n \leftarrow \mathbb{F}_p$$

$$ck = \left\{ \left[t_1^{i_1} \cdots t_n^{i_n} \right]_1, [t_i]_2 \right\}$$

ck

Prover | Verifier

$C = [f(t_1, \dots, t_n)]_1$ —C→ Commit

Open

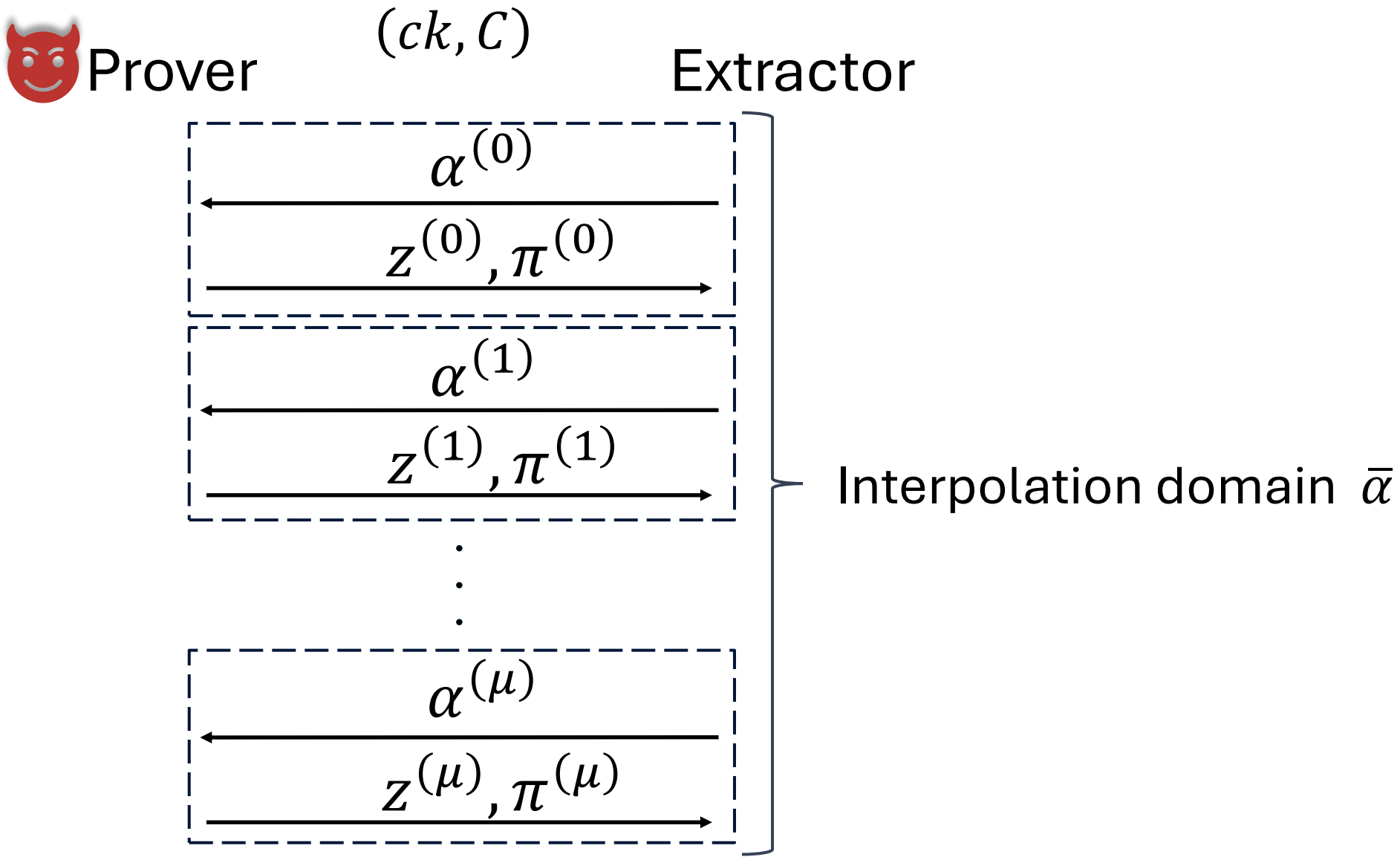
$f(\vec{\alpha}) = z$ ←$\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$— $\vec{\alpha} \in \mathbb{F}_p^n$

$\pi_i = [q_i(t_1, \dots, t_n)]_1$ —$z, \vec{\pi} = (\pi_1, \dots, \pi_n)$→

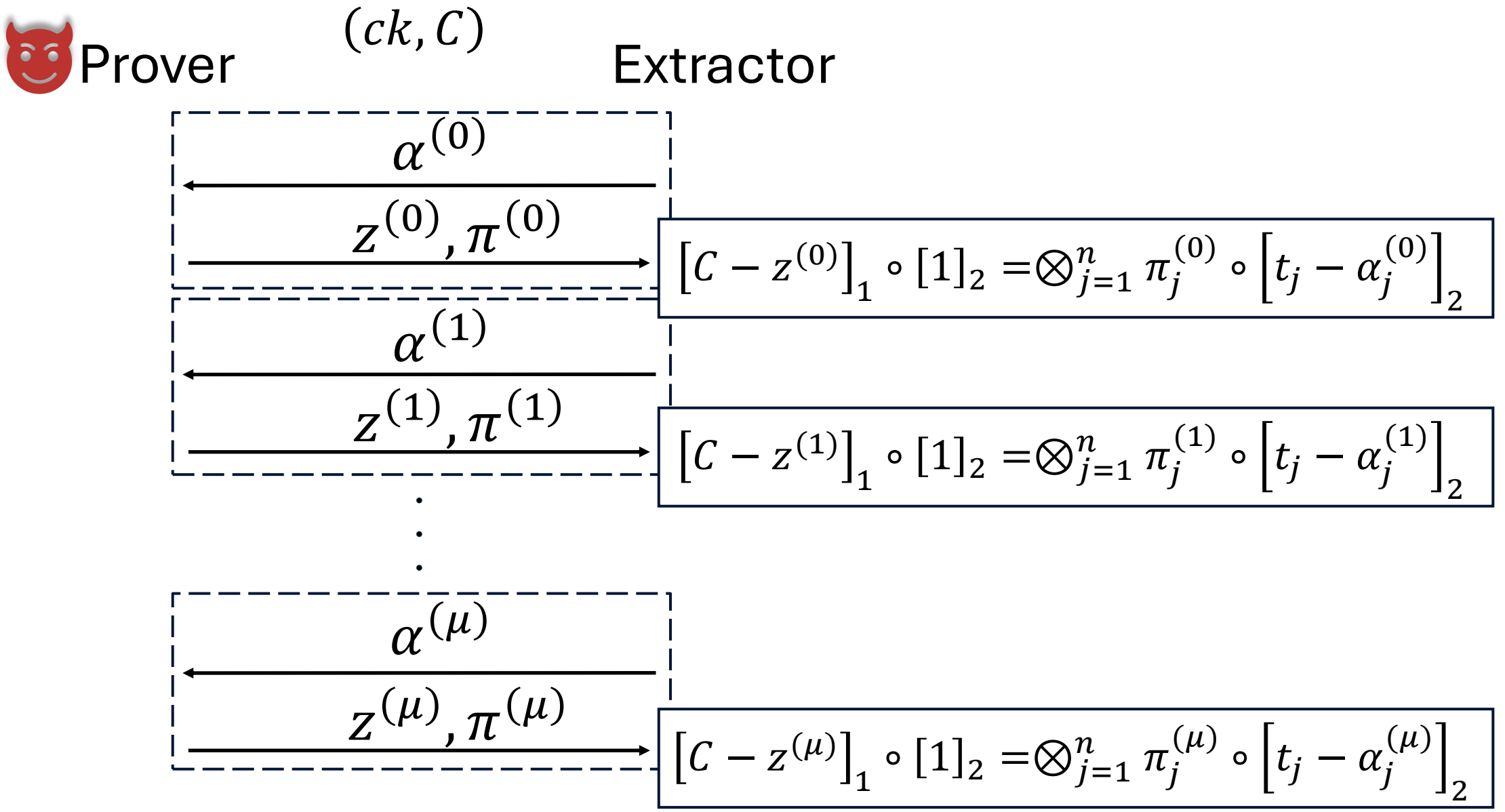
Verify

$$(C - [z]_1) \circ [1]_2 = \bigotimes_{i=1}^{n} \pi_i \circ [t_i - \alpha_i]_2$$

Special-Soundness



Special-Soundness



Special-Soundness

$$\left[C - z^{(0)}\right]_1 \circ [1]_2 = \bigotimes_{j=1}^{n} \pi_j^{(0)} \circ \left[t_j - \alpha_j^{(0)}\right]_2$$

$$\left[C - z^{(1)}\right]_1 \circ [1]_2 = \bigotimes_{j=1}^{n} \pi_j^{(1)} \circ \left[t_j - \alpha_j^{(1)}\right]_2$$

$$\vdots$$

$$\left[C - z^{(\mu)}\right]_1 \circ [1]_2 = \bigotimes_{j=1}^{n} \pi_j^{(\mu)} \circ \left[t_j - \alpha_j^{(\mu)}\right]_2$$

Batching Lemma + ARSDH(n)

$$[C - f(t_1, \dots, t_n)]_1 \circ [1]_2 = 0$$

$$f(X_1, \dots, X_n) = Interpolate(\overline{\alpha}, \vec{z})$$

Knowledge-Soundness

- Batching Lemma
  - Allows for combining equations
  - Unconditional

- ARSDH(n)
  - Generalises ARSDH from [LPS24]
  - AGM: equivalent to PDL
  - GGM: query complexity lower bound

- Knowledge-Soundness
  - Extraction via Forking Lemma [ACK21]
  - Modular

Summary

- Knowledge-Soudness of all KZG-like schemes
  - Pianist [LXZ+24]
  - Hyperpianist [LLZ+24]
  - Randomised KZG [PST13]

Summary

- Knowledge-Soudness of all KZG-like schemes
  - Pianist [LXZ+24]
  - Hyperpianist [LLZ+24]
  - Randomised KZG [PST13]

- Proofs of Knowledge of a Polynomial (PoKoPs)
  - Captures Knowledge Soundness

Summary

- Knowledge-Soudness of all KZG-like schemes
  - Pianist [LXZ+24]
  - Hyperpianist [LLZ+24]
  - Randomised KZG [PST13]

- Proofs of Knowledge of a Polynomial (PoKoPs)
  - Captures Knowledge Soundness

- Explicit quotient decomposition for multivariate polynomials

$$f(X_1, \dots, X_n) - z = \sum_{i=1}^{n} q_i(X_i, \dots, X_n)(X_i - \alpha_i)$$

Summary

- Knowledge-Soudness of all KZG-like schemes
  - Pianist [LXZ+24]
  - Hyperpianist [LLZ+24]
  - Randomised KZG [PST13]

- Proofs of Knowledge of a Polynomial (PoKoPs)
  - Captures Knowledge Soundness

- Explicit quotient decomposition for multivariate polynomials

Thank You!