北京航空航天大學
BEIHANG UNIVERSITY

香港中文大學
The Chinese University of Hong Kong

Fast RS-IOP Multivariate Polynomial Commitments and Verifiable Secret Sharing

Zongyang Zhang[1], Weihan Li[1,2], Yanpei Guo[1], Kexin Shi[1]

Sherman S. M. Chow[2], Ximeng Liu[3], Jin Dong[4]

[1] Beihang University [2] The Chinese University of Hong Kong

[3] Fuzhou University [4] Beijing Academy of Blockchain and Edge Computing

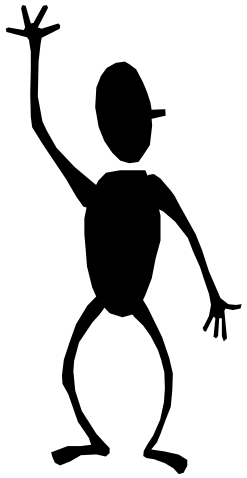
福州大学
FUZHOU UNIVERSITY

北京微芯区块链与边缘计算研究院
Beijing Academy of Blockchain and Edge Computing

Polynomial Commitment (PCS) [KZG10, GLS+23]

[KZG10]: AsiaCrypt
[GLS+23]: Crypto

Witness: A (size-$n = d^{\mu}$) degree-d μ-variate polynomial $f(X)$



Prover

$$Gen(1^{\lambda}, n) \rightarrow pp$$

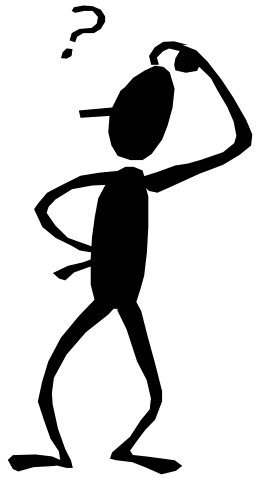
$$Com(f, pp) \rightarrow C$$

z

$f(z), \pi$

Fiat-Shamir

$$\langle Eval.P(f), Eval.V \rangle (pp, z, f(z), C)$$



Verifier

$\langle Eval.P(f), Eval.V \rangle$ can be a public-coin interactive argument of knowledge [GLS+23]

A Zoo of Polynomial Commitments, and Why FRI

Pairing group

- ☐ KZG [AsiaCrypt10]
- ☐ Multivariate KZG [PST@TCC13]
- ☐ Dory [Lee@TCC21]

Ordinary group

- ☐ Bulletproofs [BBB+@SP18]
- ☐ Hyrax [WTS+@SP18]

Hidden-order group

- ☐ DARK [BFZ@EuroCrypt20]
- ☐ Dew [AGL+@PKC22]

FRI-based (*without* groups)

*F*ast *R*eed-Solomon *I*nteractive Oracle Proof of Proximity (Fast **RS-IOP**) [BBH+@ICALP18]

- ➢ Concrete-efficient prover using only **lightweight** operations
- ➢ Transparent
- ➢ Poly-log proof size (*several hundred* KBs) and verifier complexity

State-of-the-Art FRI-based Polynomial Commitment

Polynomial size $n = d^{\mu}$		Variant (μ)	Commit	Prover	Verifier	Proof size
FRI-PC	[VP19]	Univariate	$O(n \log n)$	$O(n)$	$O(\log^2 n)$	$O(\log^2 n)$
Virgo	[ZXZ+20]	Multilinear ($\mu \geq 1$)		$O(n \log n)$		
HyperPlonk	[CBB+23]					
Zeromorph	[KT23]					

The commitment is optimally $O(n \log n)$ for RS encoding
The prover should be optimally $O(n)$

[VP19]: ePrint
[ZXZ+20]: SP
[CBB+23]: EuroCrypt
[KT23]: ePrint

A gap in the prover complexity between univariate and multilinear polynomials

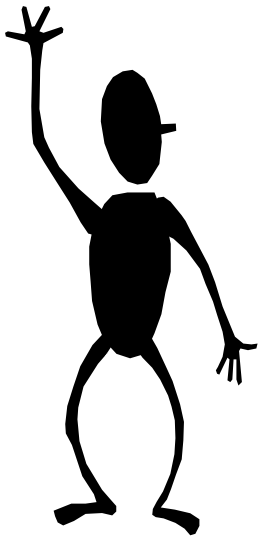
Research Problems

1. Can we build an FRI-based *multilinear* polynomial commitment scheme with $O(n)$ prover complexity?

2. Can we achieve one-to-many *bivariate* polynomial commitment?

3. Can we improve AVSS using our polynomial commitment?

One-to-many Polynomial Commitment [TCZ+20, ZZH+22]



Prover

size-N
$f(X)$

C

One-to-many Evaluation

$f(z_1), \pi_1$

$f(z_2), \pi_2$

$\vdots$

$f(z_n), \pi_n$

Verifier 1

Verifier 2

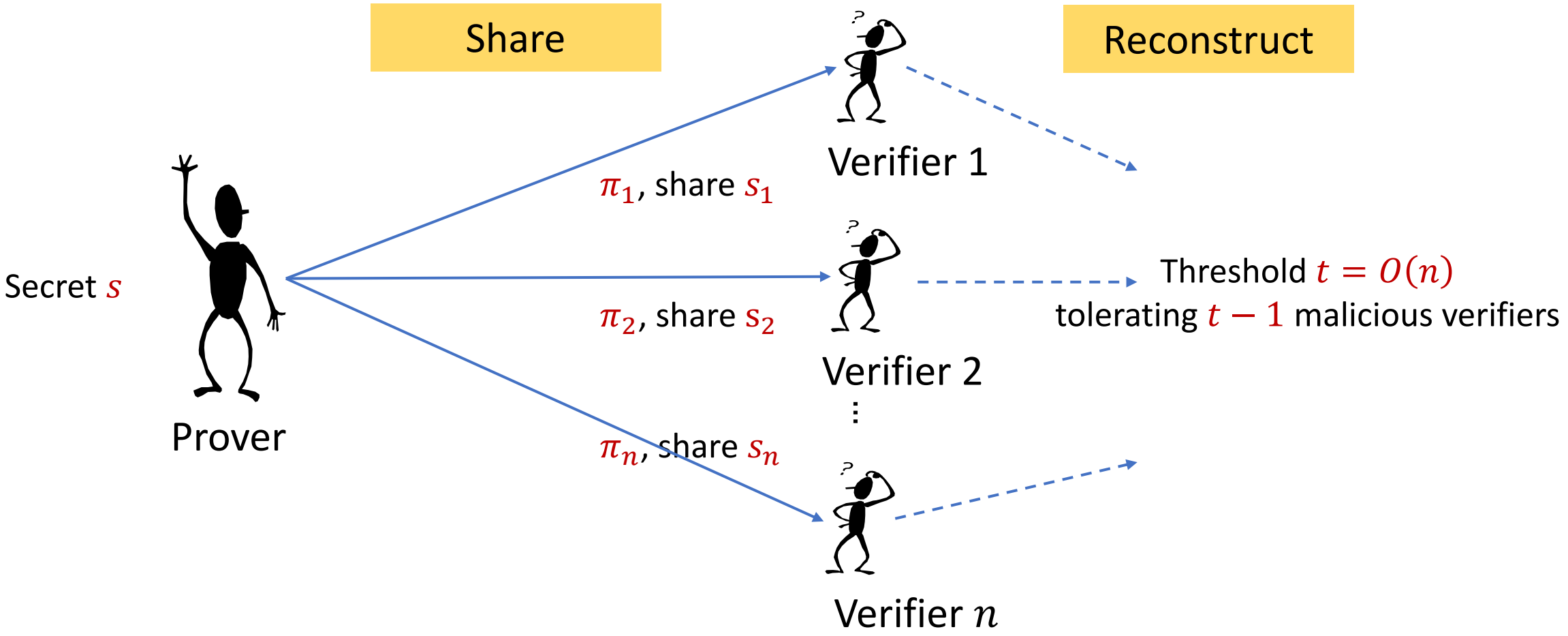
Verifier n

[TCZ+20@SP]
[ZZH+22@Usenix Sec.]

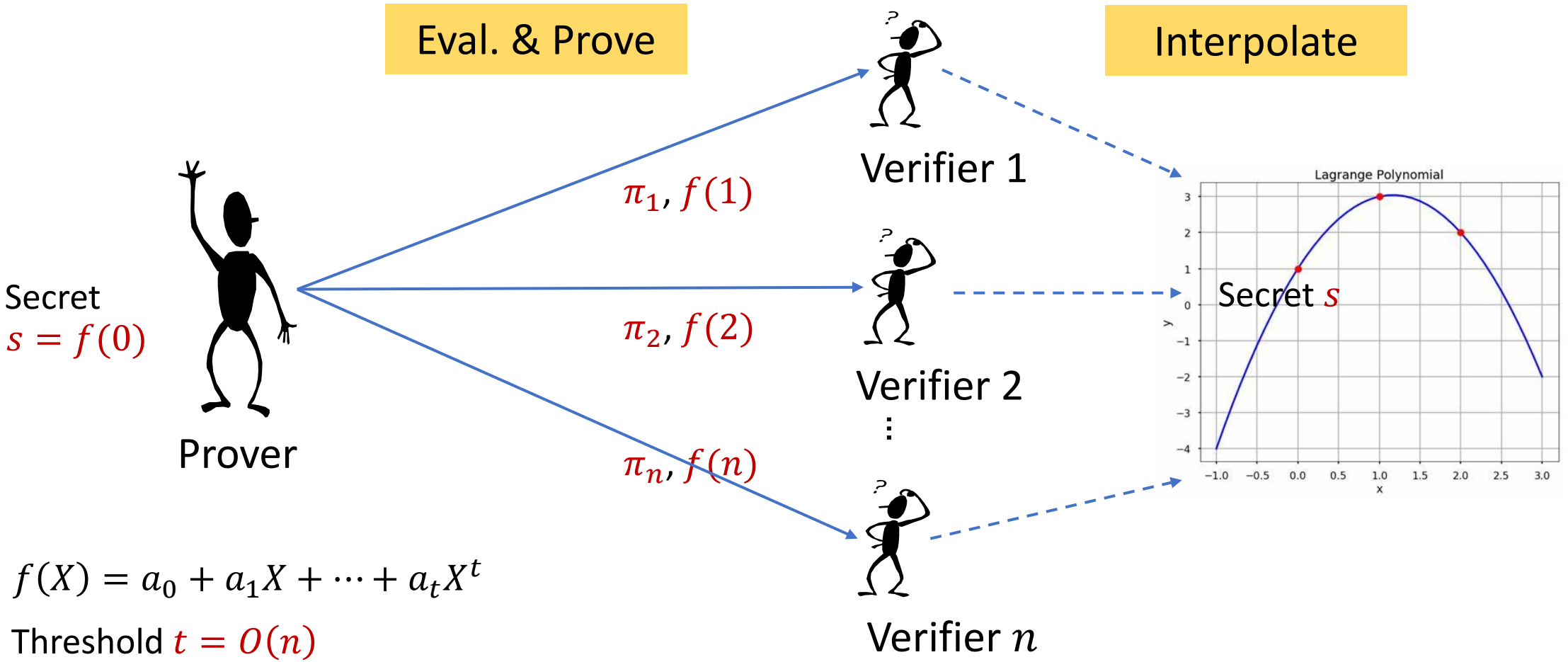
Naïve prover: $O\big(n \cdot \mathcal{P}(n)\big) \geq O(n^2)$

One-to-many: $O(n \log n)$ (optimal for n evaluations using fast Fourier transform (FFT))

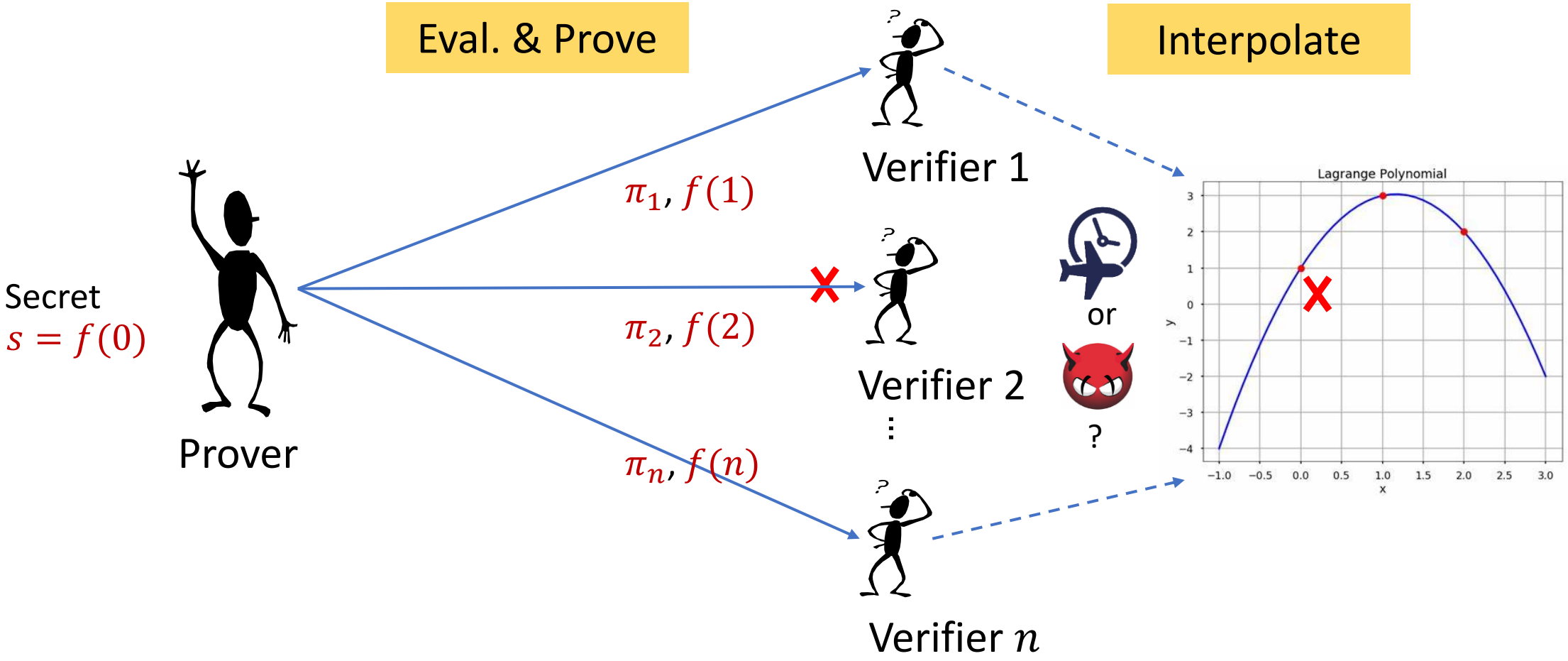
Application: Verifiable Secret Sharing (VSS)



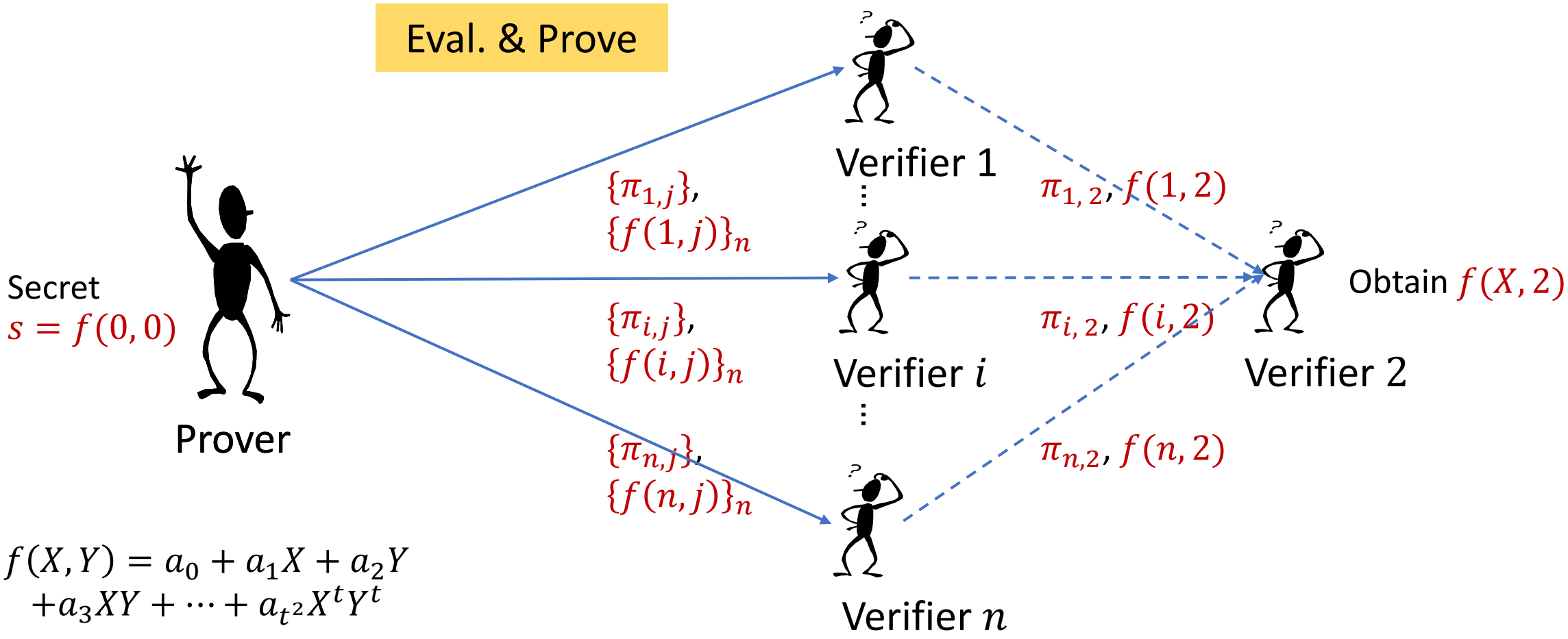
VSS from One-to-many Polynomial Commitment [ZZH+22]



Asynchronous VSS (AVSS)



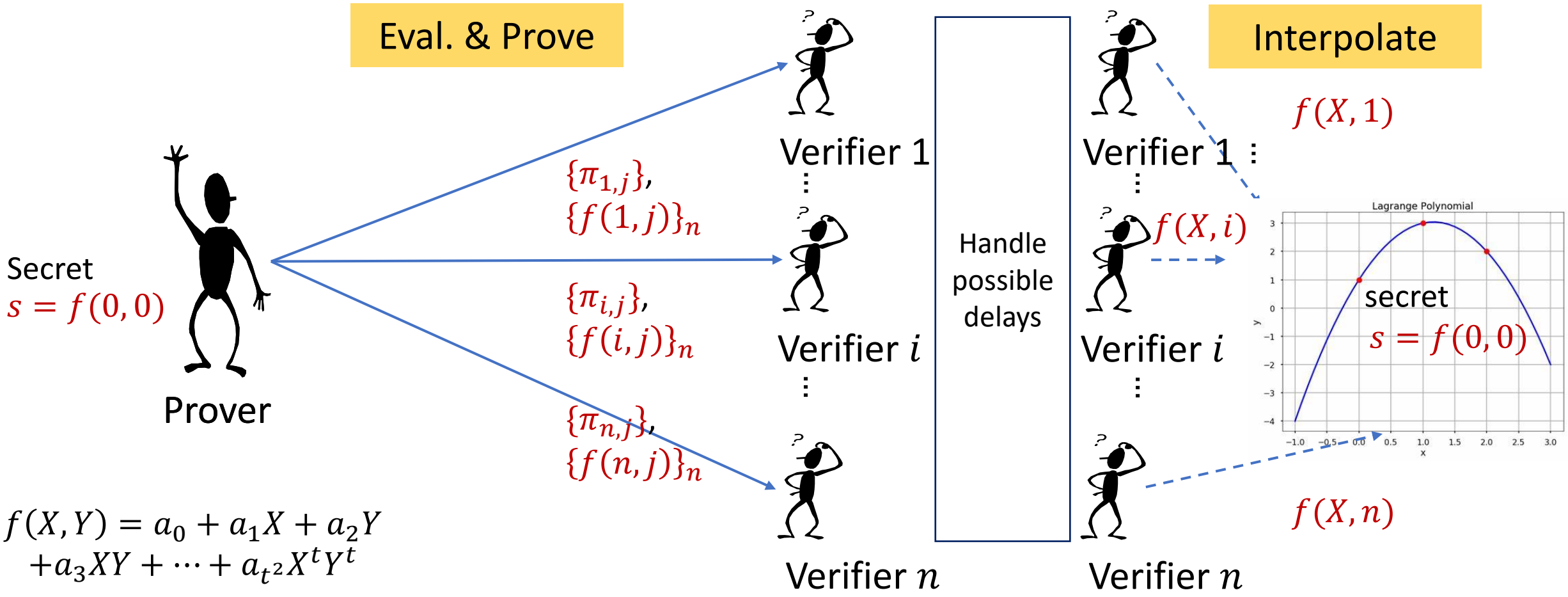
AVSS from Bivariate Polynomial Commitment



$$f(X,Y) = a_0 + a_1X + a_2Y + a_3XY + \cdots + a_{t^2}X^tY^t$$

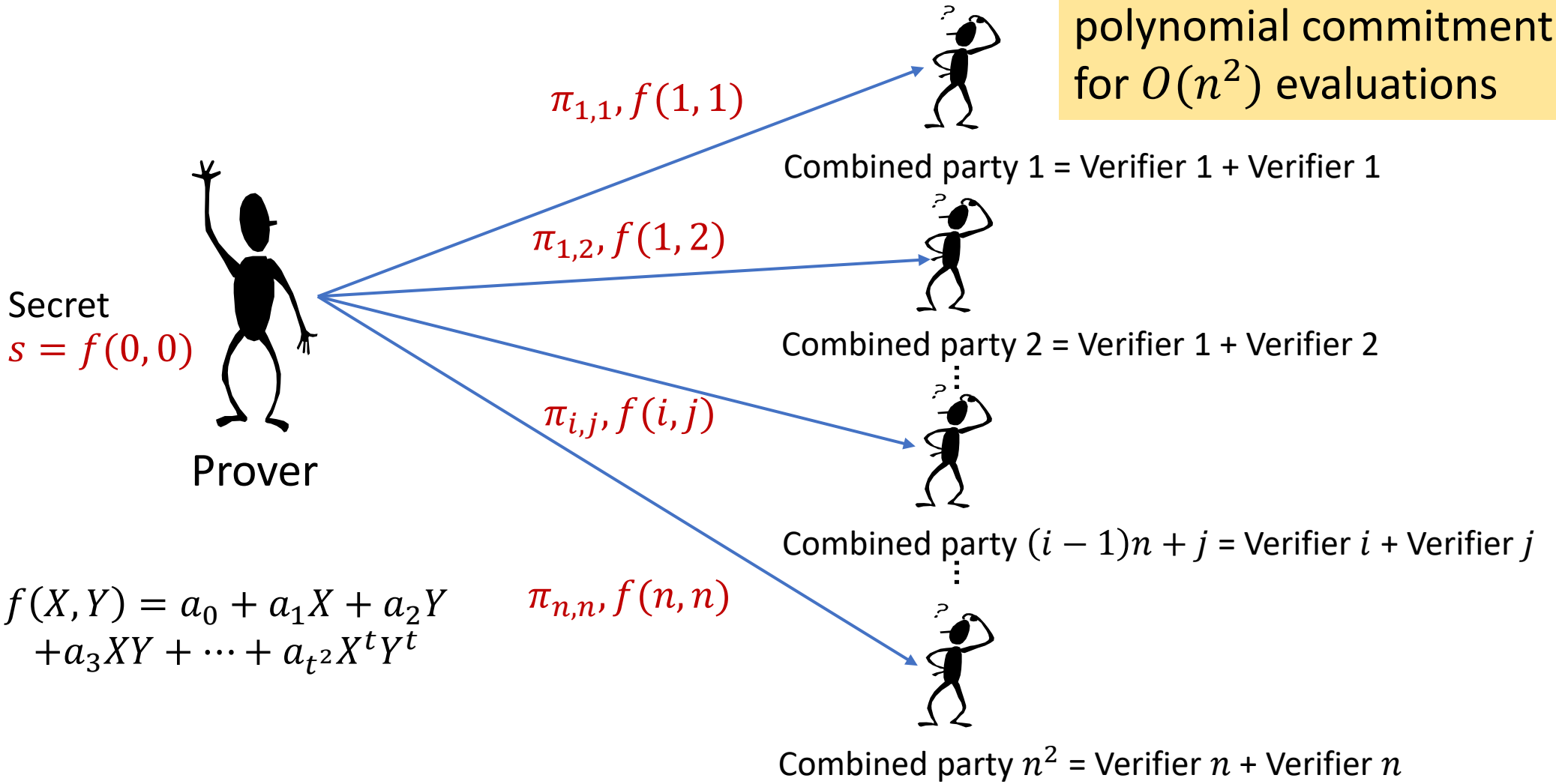
Threshold $t = O(n)$

AVSS from Bivariate Polynomial Commitment



AVSS from One-to-Many Polynomial Commitment

A one-to-many size-$O(n)$ polynomial commitment for $O(n^2)$ evaluations



$$f(X,Y) = a_0 + a_1 X + a_2 Y + a_3 XY + \cdots + a_{t^2} X^t Y^t$$

Research Problems

1. Can we build an FRI-based *multilinear* polynomial commitment with $O(n)$ prover complexity?

2. Can we achieve a one-to-many *bivariate* polynomial commitment?

   need a different approach from univariate [ZXH+22], extending to bivariate can be challenging

   (Usenix Sec.)

3. Can we improve AVSS using our polynomial commitment?

Contributions

1. Can we build an FRI-based *multilinear* polynomial commitment with $O(n)$ prover complexity?

   Yes! Improve HyperPlonk [CBB+23, Appendix B] and achieve linear prover

   (EuroCrypt)

2. Can we achieve a one-to-many *bivariate* polynomial commitment?

   need a different approach from univariate [ZXH+22], extending to bivariate can be challenging

   Yes! Prover complexity for n^2 parties: $O(n^2 \log n)$
   still optimal for FFT evaluation

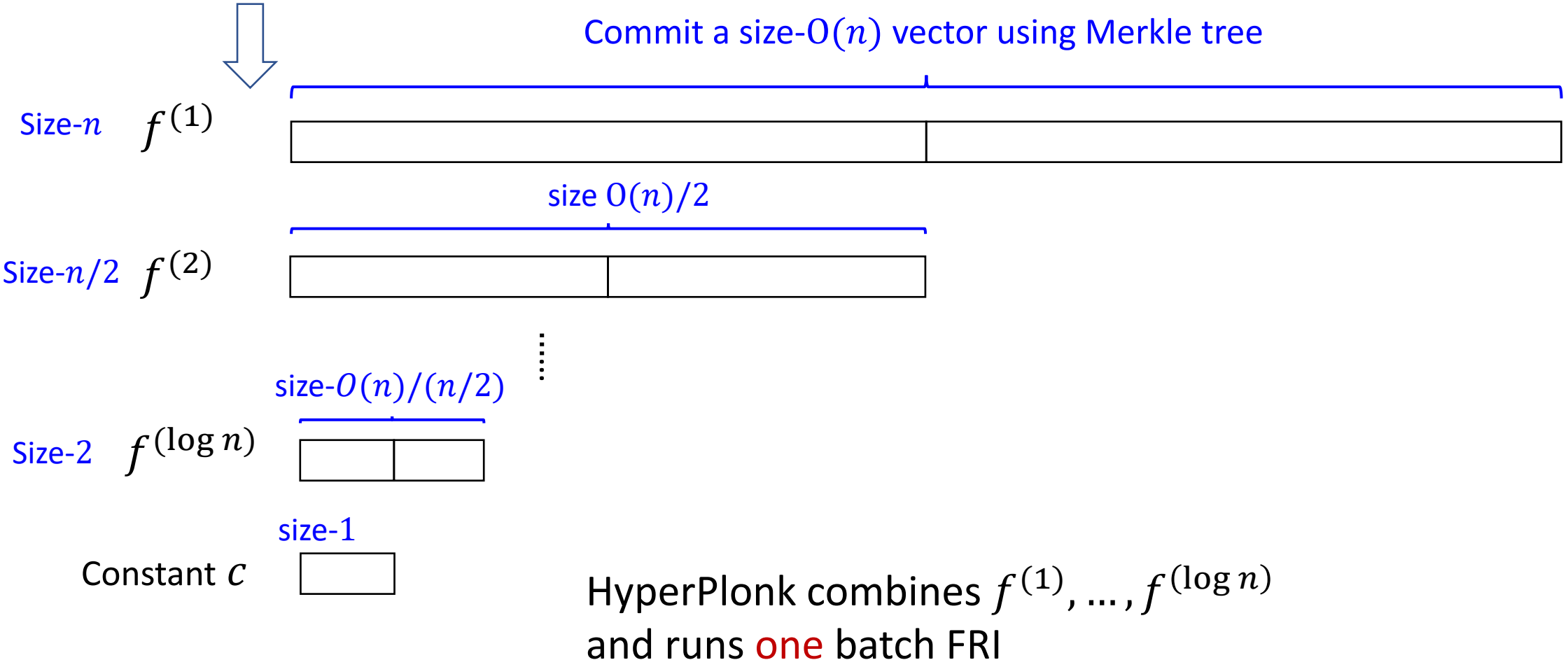
3. Can we improve AVSS using our polynomial commitment?

   Yes! Dealer complexity: $O(n^2 \log n)$, better than transparent Haven [AVZ21]

   (Fin. Crypt.)

Recall: HyperPlonk-PCS [CBB+23]

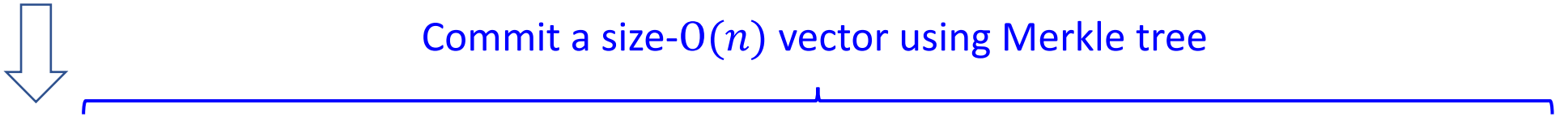
Size-n multilinear $f(X_1, \ldots, X_{\log n})$ (EuroCrypt)



HyperPlonk combines $f^{(1)}, \ldots, f^{(\log n)}$ and runs one batch FRI

Recall: HyperPlonk-PCS [CBB+23]

Size-n multilinear $f(X_1, \ldots, X_{\log n})$



Commit a size-$O(n)$ vector using Merkle tree

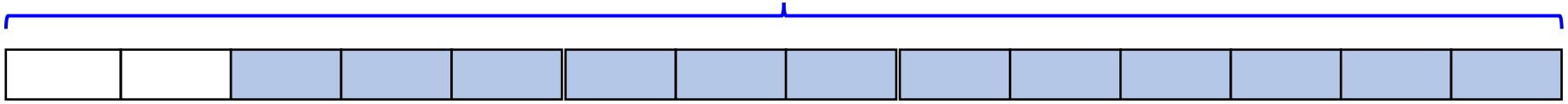
Size-n $f^{(1)}$

Pad to size-$O(n)$ and commit a size-$O(n)$ vector using Merkle tree

Size-$n/2$ $f^{(2)}$

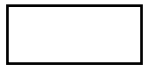
Pad to size-$O(n)$ and commit a size-$O(n)$ vector using Merkle tree

Size-2 $f^{(\log n)}$



size-1

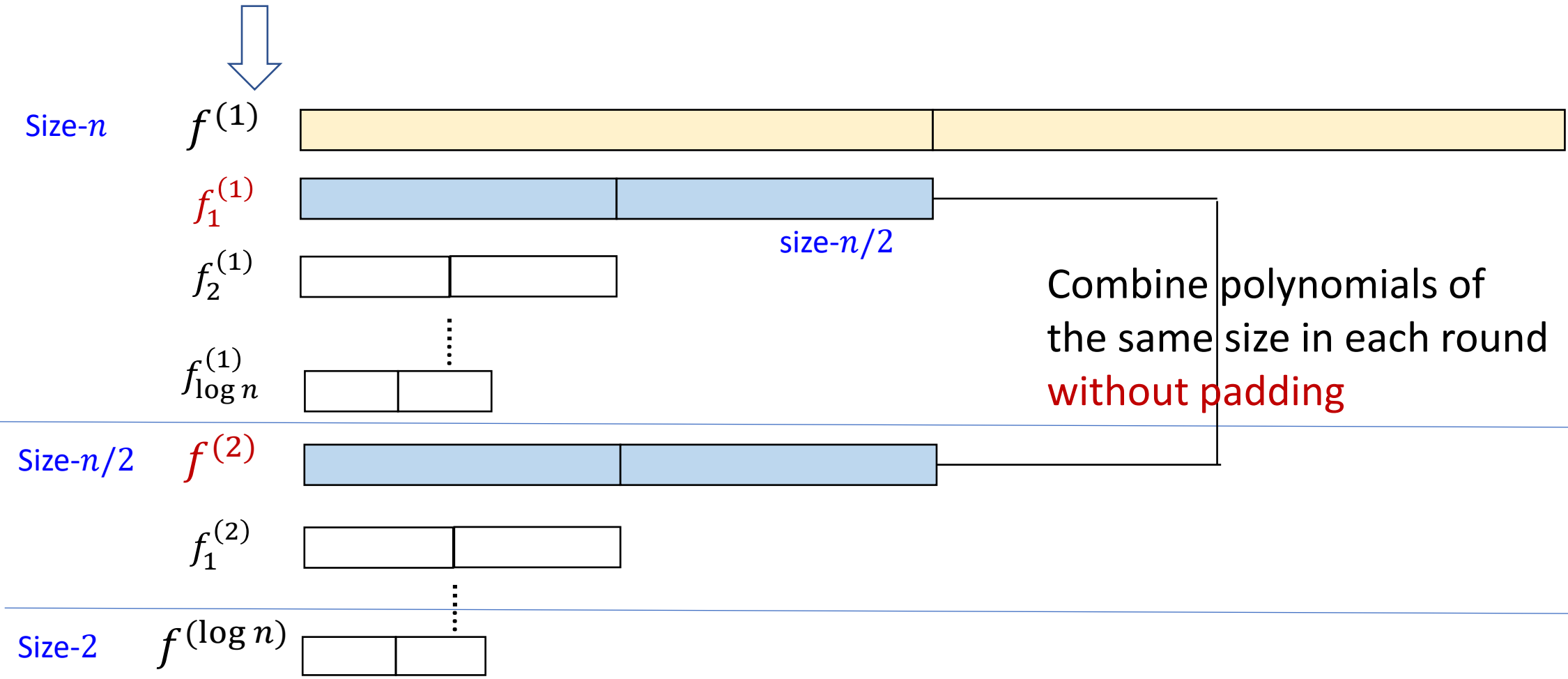
Constant c



To prove in batch FRI,
require padding each vector to size-$O(n)$
require $O(n \cdot \log n)$ already

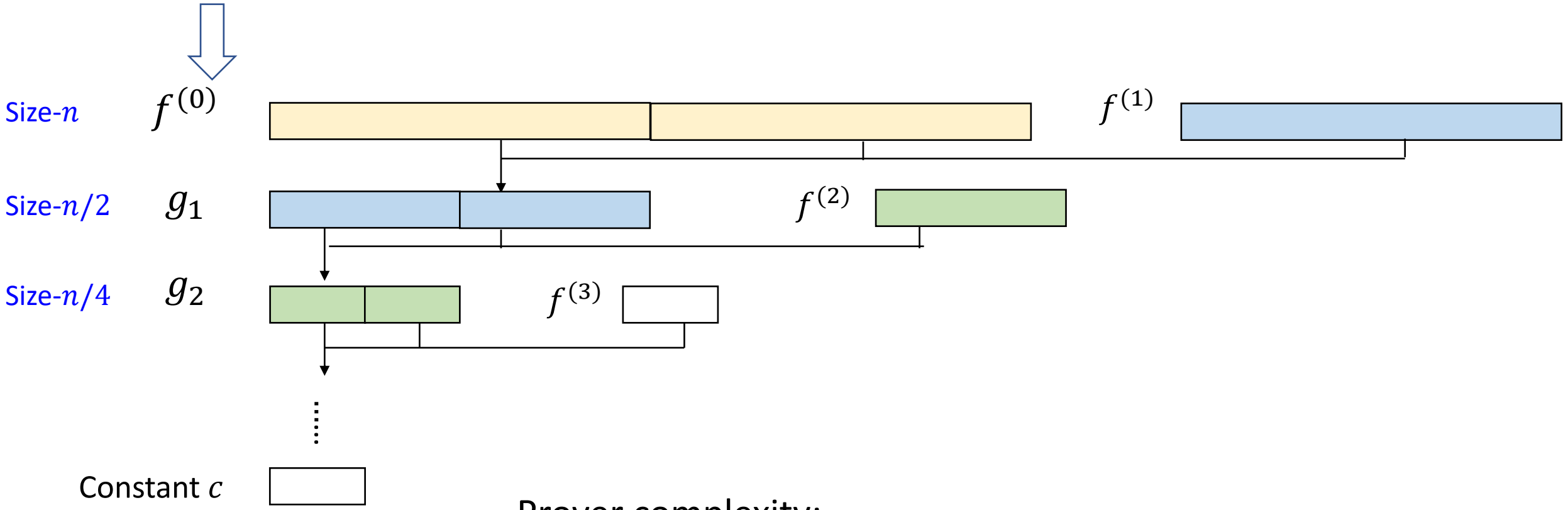
Technical Overview: Rolling Batch FRI

Size-n multilinear $f(X_1, \ldots, X_{\log n})$



Technical Overview: Rolling Batch FRI

Size-n multilinear $f(X_1, \ldots, X_{\log n})$



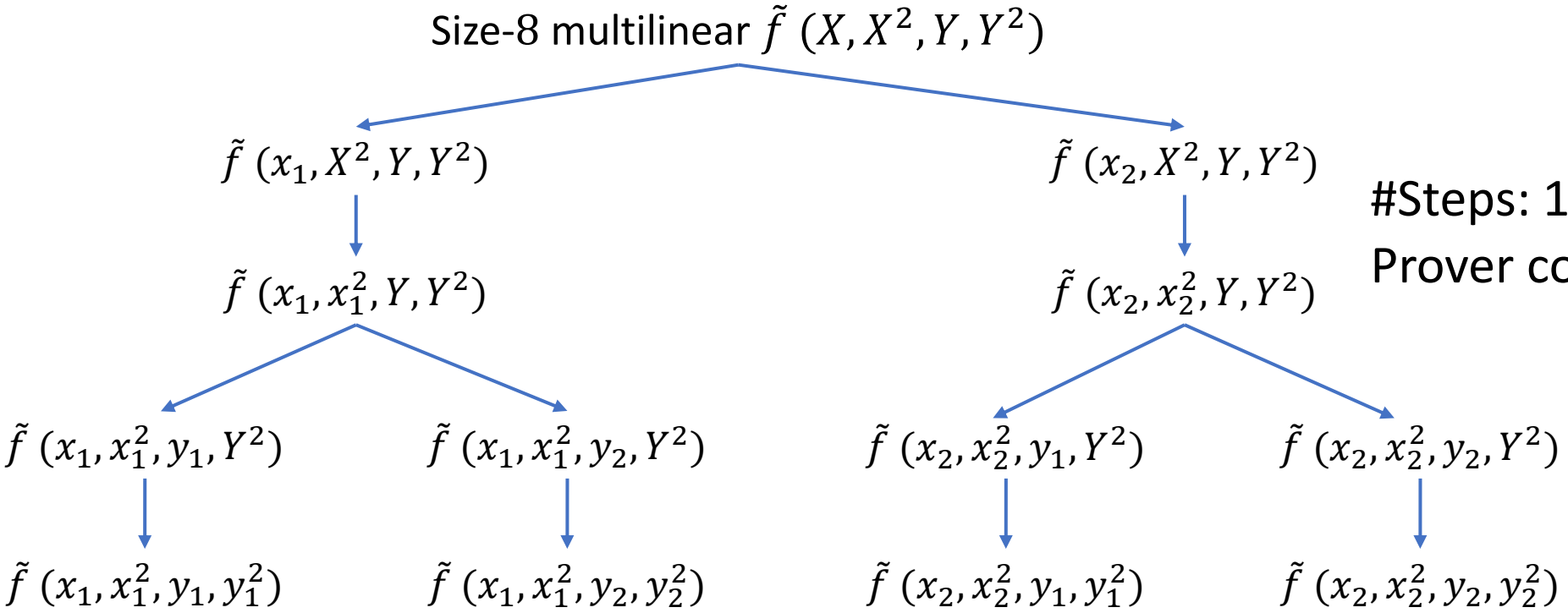
Prover complexity:

$$O\left(\sum_{i=1}^{\log n} \frac{n}{2^i}\right) = O(n)$$

Technical Overview: One-to-Many PCS

Size-8 $f(X, Y)$ on $\{f(x_i, y_j)\}, i, j \in [2]$

⇩ Our transformation



#Steps: 12

Prover complexity: $\boldsymbol{O(n^3 \log n)}$

Technical Overview: One-to-Many PCS

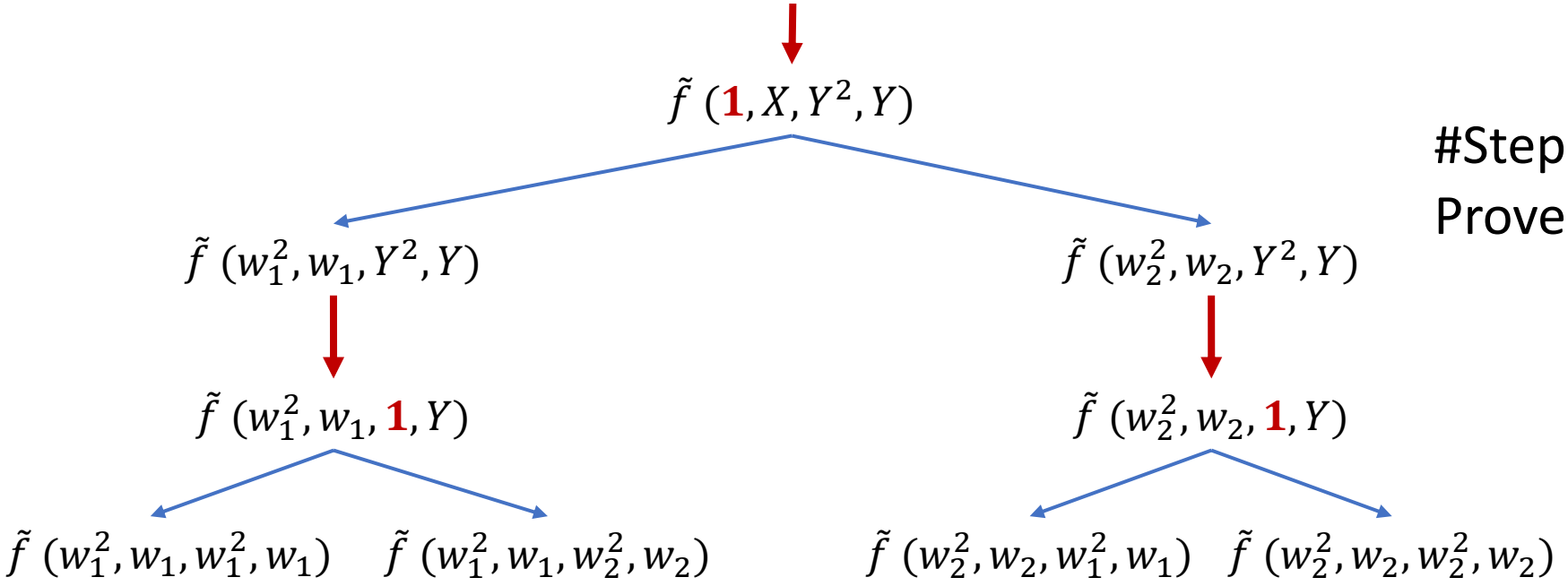
Size-8 $f(X, Y)$ on $\{f(x_i, y_j)\}, i, j \in [2]$

Let $x_i = w_2^i$

$y_j = w_2^j$

⇩ Inverse variables

Size-8 multilinear $\tilde{f}\ (\boldsymbol{X^2}, \boldsymbol{X}, \boldsymbol{Y^2}, \boldsymbol{Y})$



#Steps: 9

Prover complexity: $\boldsymbol{O(n^2 \log n)}$

Results – PCS, One-to-Many PCS, and AVSS

Table 1: Computation and communication complexities of μ-variate degree-d or degree-2 polynomial commitments

Scheme	Trustless Setup	Assumption	Commit	Prover	Verifier	Communication
PST13 [28]	no	q-SDH	$O(d^\mu)\,\mathbb{G}_B$	$O(d^\mu)\,\mathbb{G}_B$	$O(\mu)\,\mathbb{G}_B$	$O(\mu)\,\mathbb{G}_B$
DARK [12]	yes/no	Strong RSA	$O(d^\mu)\,\mathbb{G}_U$	$O(\mu d^\mu \log d)\,\mathbb{G}_U$	$O(\mu \log d)\,\mathbb{G}_U$	$O(\mu \log d)\,\mathbb{G}_U$
Bulletproofs [11]	yes	DLog	$O(d^\mu)\,\mathbb{G}_P$	$O(d^\mu)\,\mathbb{G}_P$	$O(d^\mu)\,\mathbb{G}_P$	$O(\mu \log d)\,\mathbb{G}_P$
Virgo [37]	yes	$O(\mu d^\mu \log d)\,\mathbb{F} + O(d^\mu)\,\mathsf{H}$		$O(\mu d^\mu \log d)\,\mathbb{F}$	$O(\mu^2 \log^2 d)\,\mathsf{H}$	$O(\mu^2 \log^2 d)\,\mathsf{H}$
HyperPlonk [16, §B]	yes	$O(\mu 2^\mu \log 2)\,\mathbb{F} + O(2^\mu)\,\mathsf{H}$		$O(\mu 2^\mu \log 2)\,\mathbb{F}$	$O(\mu^2 \log^2 2)\,\mathsf{H}$	$O(\mu^2 \log^2 2)\,\mathsf{H}$
PolyFRIM	yes	$O(\mu d^\mu \log d)\,\mathbb{F} + O(d^\mu)\,\mathsf{H}$		$O(d^\mu)\,\mathsf{H} + O(d^\mu)\,\mathbb{F}$	$O(\mu^2 \log^2 d)\,\mathsf{H}$	$O(\mu^2 \log^2 d)\,\mathsf{H}$

$\mathbb{G}_i$, $i \in \{B, U, P\}$, denotes a group with a *B*ilinear map, of *U*nknown order, or of known *P*rime order; $\mathbb{F}$ is a field with a large multiplicative coset. H denotes a hash function. All these represent the size or operation time depending on the context.

Table 2: One-to-many proofs for n^2 evaluations of degree-n *Uni*variate or *Bi*variate polynomial

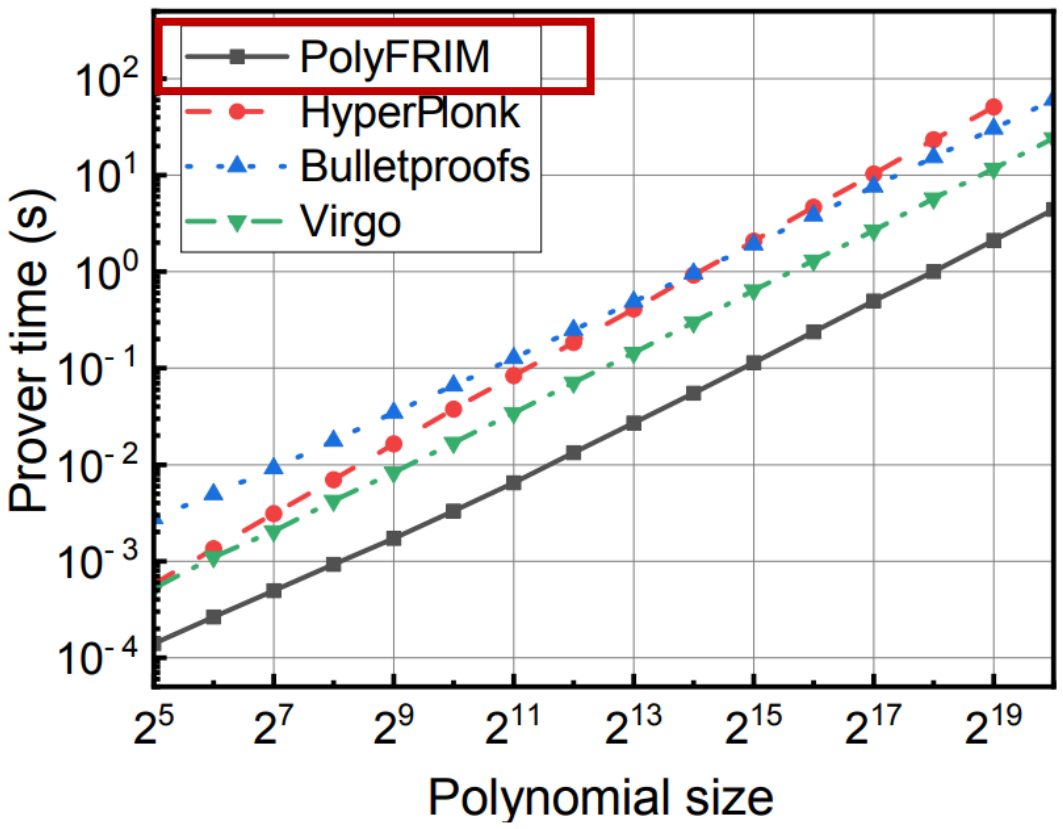
Scheme	Trustless	PCS	Prover	Verifier/Commun.
AMT [31]	no	Uni.	$O(n^2 \log n)$	$O(\log n)$
ZXH+22 [36]	no	Uni.	$O(n^2 \log n)$	$O(1)$
ZXH+22 [36]	yes	Uni.	$O(n^2 \log n)$	$O(\log^2 n)$
Naïve [16, 37]	yes	Bi.	$O(n^3 \log n)$	$O(\log^2 n)$
PolyFRIM	yes	Bi.	$O(n^2 \log n)$	$O(\log^2 n)$

Table 3: Existing n-party AVSS from multivariate PCS

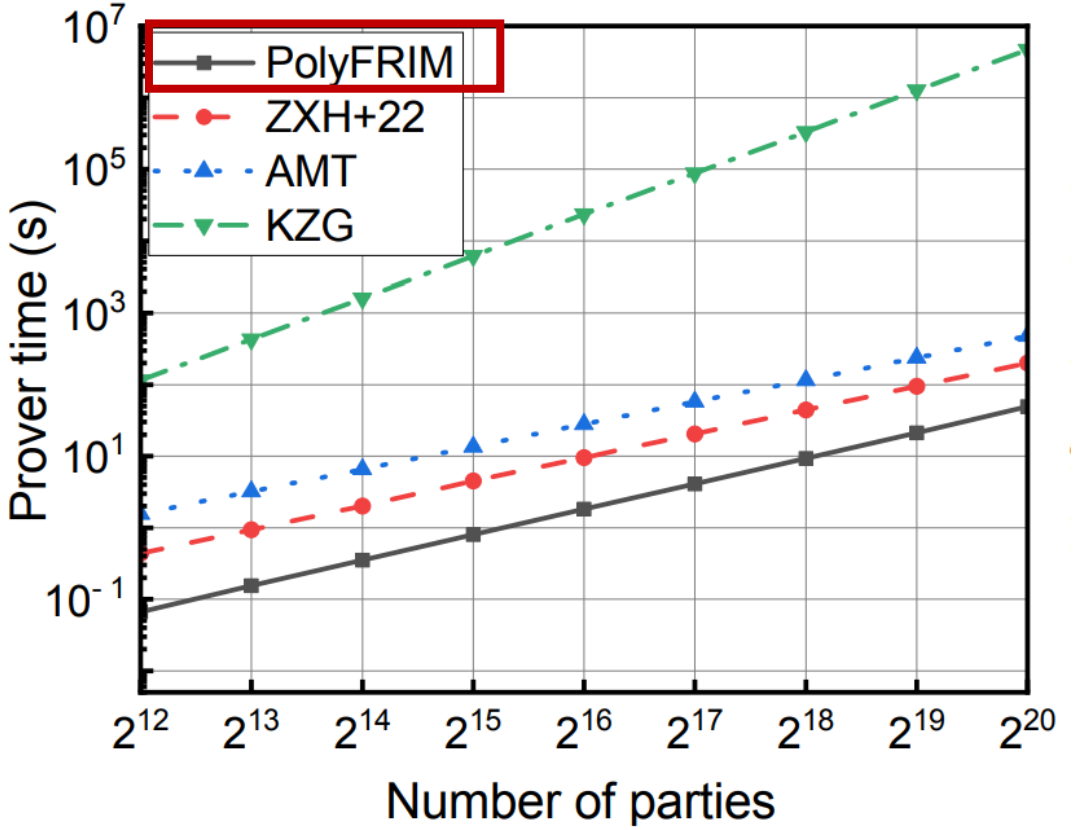
Scheme	PCS	Dealer	Party	Commun.
eAVSS [3]	q-SDH	$O(n^3)$	$O(n)$	$O(n^2)$
HAVEN-1 [2]	q-SDH	$O(n^3)$	$O(n)$	$O(n^2)$
Bingo [1]	q-SDH	$O(n^2 \log n)$	$O(n^2)$	$O(n^2)$
HAVEN-2 [2]	DLog	$O(n^3)$	$O(n^2)$	$O(n^2 \log n)$
FRISS	Ours	$O(n^2 \log n)$	$O(n \log^2 n)$	$O(n^2 \log^2 n)$

Experiment on (One-to-Many) Polynomial Commitment

Multilinear PCS
5 to 25× faster prover time



One-to-many PCS
7 to 10^4× faster prover time
(compared with univariate ones)



Summary

Transparent FRI-based multilinear polynomial commitment
$O(n)$ prover time, $O(\log^2 n)$ proof size and verifier time for size-n polynomial

One-to-many bi-variate polynomial commitment for #party n^2 and size-n poly.
$O(n^2 \log n)$ prover time, $O(\log^2 n)$ proof size/verifier time per verifier

New *Transparent* AVSS for #party n
$O(n^2 \log n)$ dealer time, total $O(n^2 \log^2 n)$ proof size, $O(n \log^2 n)$ per verifier

Weihan Li
leeweihan@buaa.edu.cn

github.com/gyp2847399255/PolyFRIM