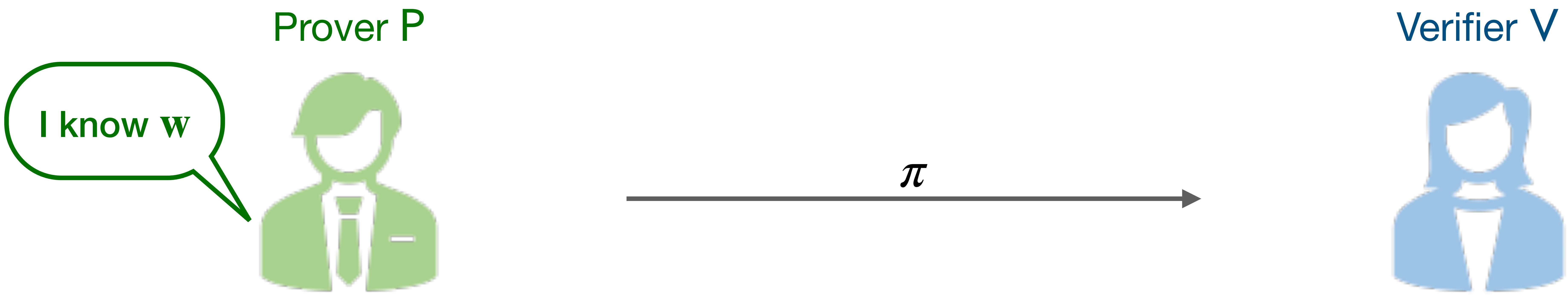
Asiacrypt 2022

Efficient Zero-Knowledge Arguments in Discrete Logarithm Setting : Sublogarithmic Proof or Sublinear Verifier

Presenter : Hyeonbum Lee

Coauthor : Sungwook Kim, Jae Hong Seo

Zero-Knowledge Argument of Knowledge



$\pi \leftarrow \mathsf{P}(S_p, \mathbf{x}; \mathbf{w})$

No leak info. about w

$R = \{(\mathbf{x}; \mathbf{w}) : \phi(\mathbf{x}, \mathbf{w}) = 1\}$

$0/1 \leftarrow \mathsf{V}(S_V, \mathbf{x}, \pi)$

- Completeness : If $(\mathbf{x}; \mathbf{w}) \in R$, P can convince V (V outputs 1)
- Knowledge Soundness : Without knowledge of $\mathbf{w}$, P$'$ cannot convince V (V outputs 0)
- Zero-knowledge : The proof π reveal no information except P's knowledge of $\mathbf{w}$ with $(\mathbf{x}; \mathbf{w}) \in R$
- We call an argument is transparent if the argument does not require trusted third party for generating common reference string

Inner Product Argument, IPA

- Argument of Knowledge(AoK) of two vectors $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_P^N$ for their inner product relation
- Transparent IPA with logarithm communication : [BCC+16], [BP-IP, BBB+18]
- Application
  - ZK-Range proof
  - ZKA for Arithmetic Circuits
  - ZK-Polynomial Commitment Scheme

$$R_{BP} = \{(\mathbf{g}, \mathbf{h} \in \mathbb{G}^N, u, P \in \mathbb{G}; \mathbf{a}, \mathbf{b} \in \mathbb{Z}_p^N) : P = \mathbf{g}^{\mathbf{a}}\mathbf{h}^{\mathbf{b}}u^{\langle \mathbf{a},\mathbf{b} \rangle}\}$$

Relation for BP-IP

- There is a reduction from ZKA for AC to IPA
- We focus on BP-IP and its variant for constructing ZKA

[BCC+16] : "Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the discrete log setting", EUROCRYPTO 2016
[BBB+18] : "Bulletproofs: Short Proofs for Confidential Transactions and More", S&P 2018

Contribution

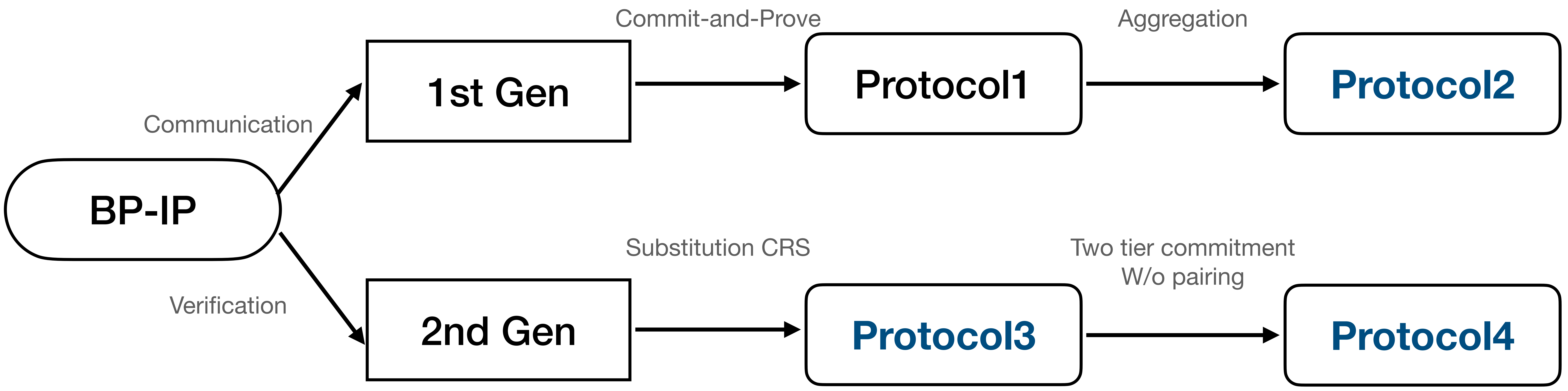
We propose three transparent IPAs :

- **Protocol2** : The first IPA with sublogarithmic communication.
- **Protocol3** : The first IPA with sublinear verifier under DL assumption.
- **Protocol4** : Introduce a novel method to achieve the sublinear verifier IPA w/o pairing

Contribution

We propose three transparent IPAs :

- **Protocol2** : The first IPA with sublogarithmic communication.
- **Protocol3** : The first IPA with sublinear verifier under DL assumption.
- **Protocol4** : Introduce a novel method to achieve the sublinear verifier IPA w/o pairing

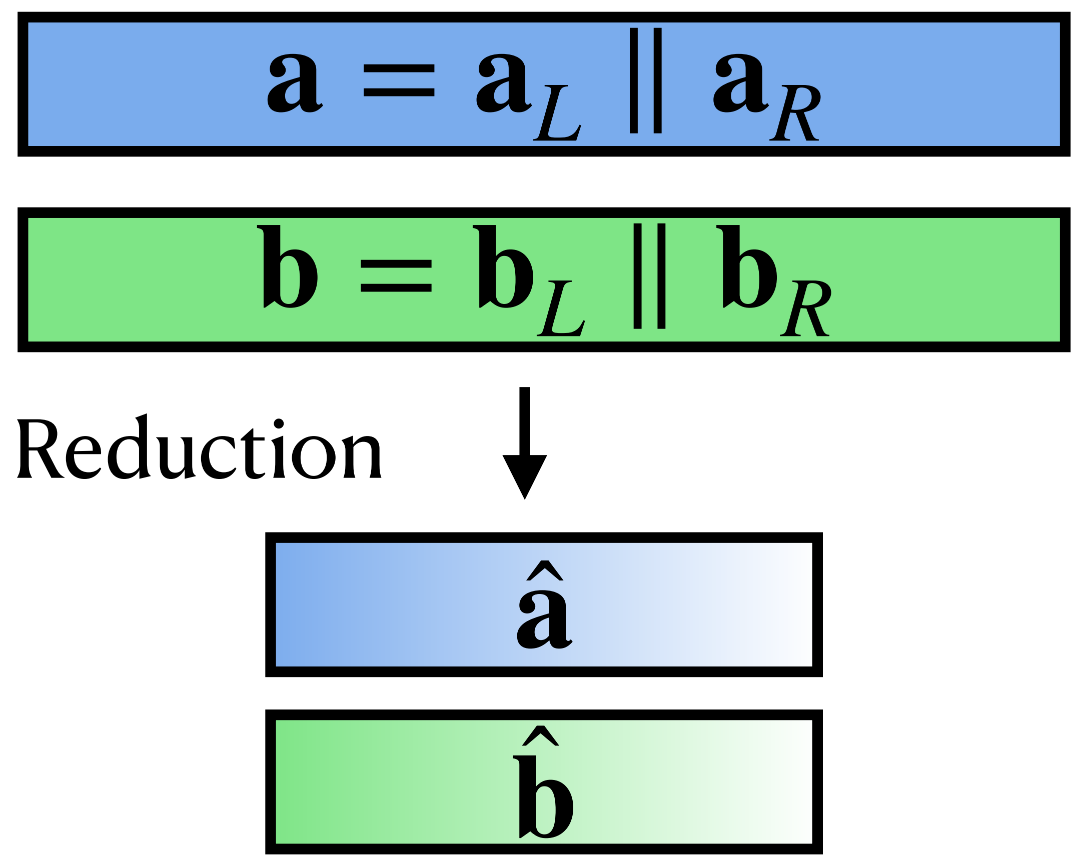


Protocol2 :
Sublogarithmic Communication

- **Round Reducing**
- **Commit-and-Prove**
- **Aggregation technique**

Observation 1 : Communication of BP-IP

- Key idea of logarithm communication : Witness Reduction
- Halve witness vectors $\mathbf{a}, \mathbf{b}$ and update to $\hat{\mathbf{a}}, \hat{\mathbf{b}}$ recursively
- $\hat{\mathbf{a}} := x\mathbf{a}_L + x^{-1}\mathbf{a}_R \in \mathbb{Z}_p^{\frac{N}{2}}, \ \hat{\mathbf{b}} := x^{-1}\mathbf{b}_L + x\mathbf{b}_R \in \mathbb{Z}_p^{\frac{N}{2}}$
- P should send commitments to "cross terms" per round
- Total communication = total rounds x each reduction cost : $\log_2 N \times 2 = 2\log_2 N$



Inner Product Relation of $\hat{\mathbf{a}}, \hat{\mathbf{b}}$

$$\langle \hat{\mathbf{a}}, \hat{\mathbf{b}} \rangle = \boxed{\langle \mathbf{a}, \mathbf{b} \rangle} + x^2 \boxed{\langle \mathbf{a}_L, \mathbf{b}_R \rangle} + x^{-2} \boxed{\langle \mathbf{a}_R, \mathbf{b}_L \rangle}$$

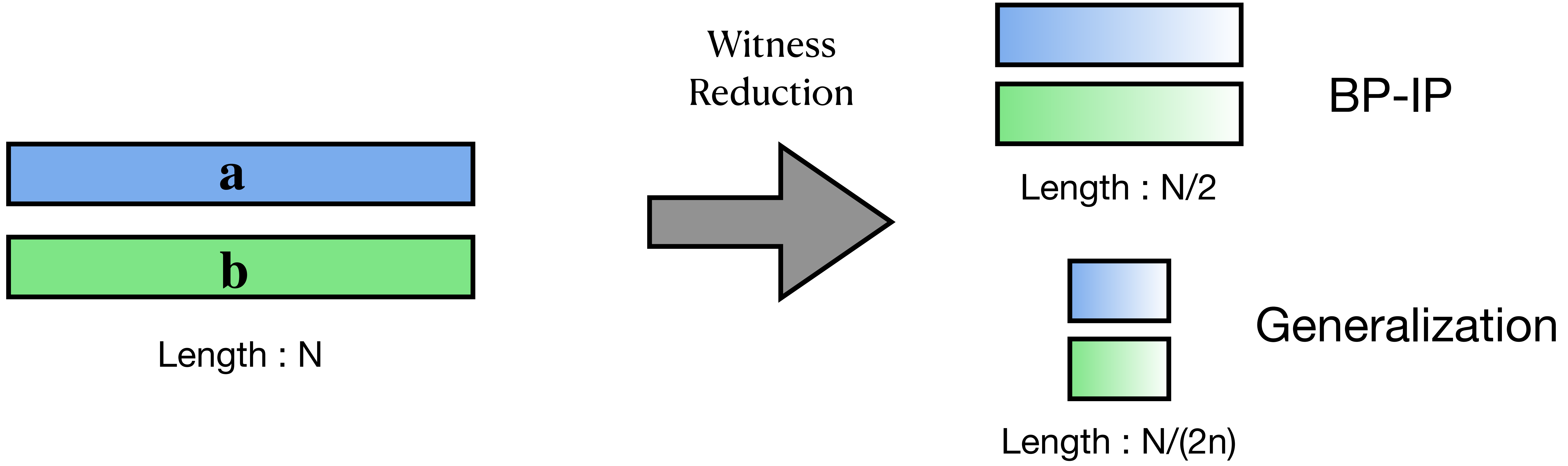
Parallel term

Cross terms

V needs commitment to these terms

Generalization of BP-IP

- How about reducing witness vectors more shortly?
- Construct generalized BP-IP : $2n$-partition technique
- Decrease total round to $\log_{2n} N$ but each reduction cost may increase



1st Generalization of BP-IP

- Parse witness vectors $\mathbf{a}, \mathbf{b}$ to $2n$ subvectors $\mathbf{a}_i, \mathbf{b}_i$ and update to $\hat{\mathbf{a}}, \hat{\mathbf{b}}$ respectively
- $\hat{\mathbf{a}} := \sum x^i \mathbf{a}_i \in \mathbb{Z}_p^{\frac{N}{2n}}, \hat{\mathbf{b}} := \sum x^{-i} \mathbf{b}_i \in \mathbb{Z}_p^{\frac{N}{2n}}$
- P should send commitments to “cross terms”, $2n(2n-1)$ group elements per round
- For constructing commitments to “cross terms”, P computes $O(nN)$ exponentiation
- Total communication : $\log_{2n} N \times 2n(2n-1)$
- $n = 1$ is optimal value of total communication, there is no merit to use 2n-partition technique

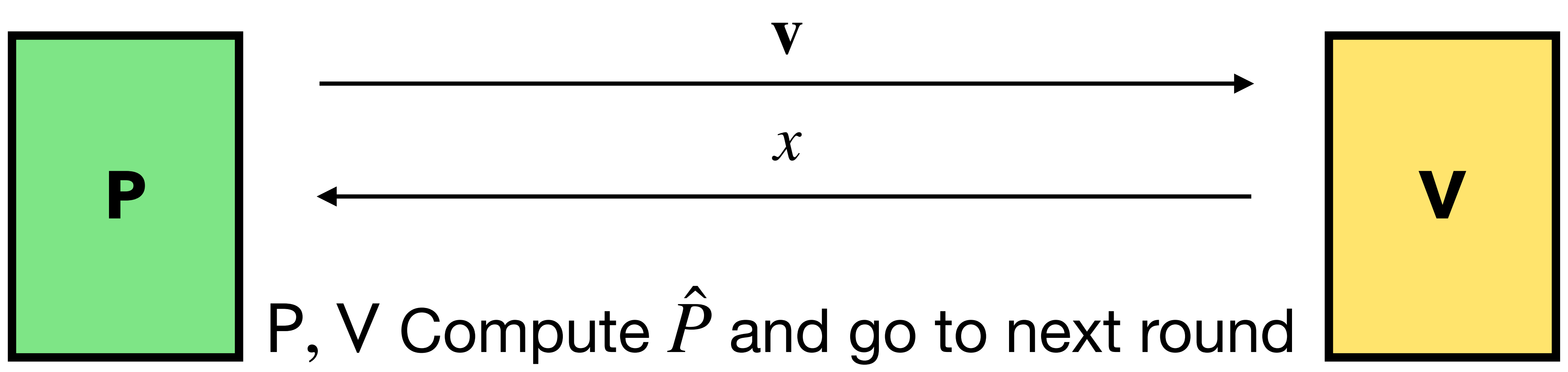
$$\langle \hat{\mathbf{a}}, \hat{\mathbf{b}} \rangle = \underbrace{\boxed{\langle \mathbf{a}, \mathbf{b} \rangle}}_{\text{Parallel term}} + \boxed{\sum_{i \neq j} x^{i-j} \langle \mathbf{a}_i, \mathbf{b}_j \rangle}$$

Cross terms

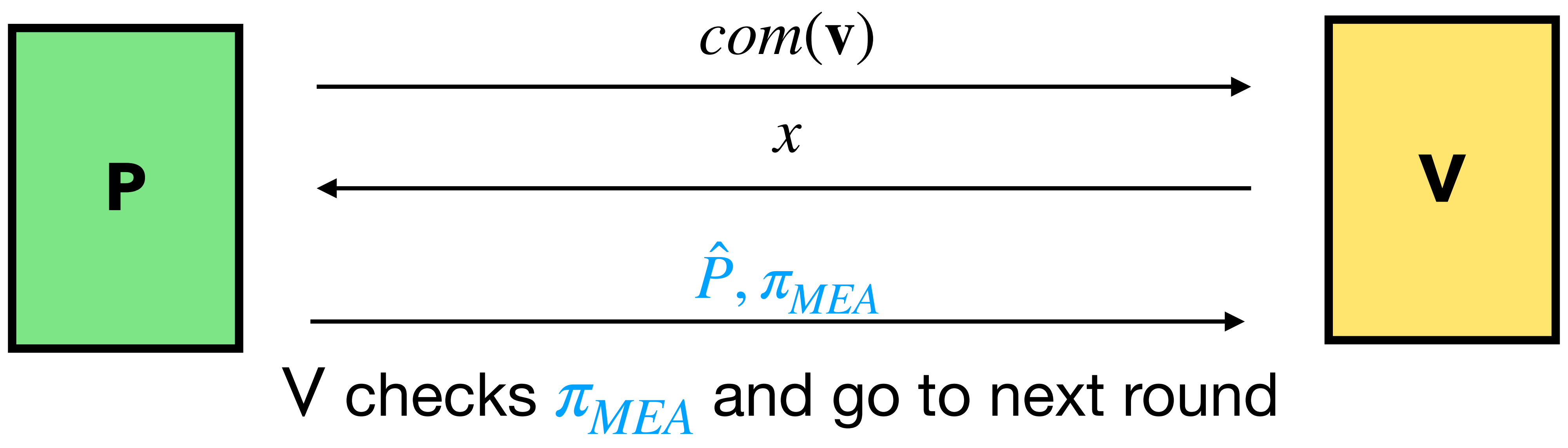
V needs commitments of each terms

Protocol1 : Commit-and-Prove approach

- P sends a short commitment $com(\mathbf{v})$ rather than sending $2n(2n-1)$ group elements $\mathbf{v}$,
- Without $\mathbf{v}$, V cannot update instance $\hat{P}$. How to construct a reduction protocol?
- Solution : P sends $\hat{P}$ with proof π_{MEA} after receiving challenge $x \leftarrow \mathbb{Z}_p$
- π_{MEA} : Proof of knowledge $\mathbf{v}$ such that $\hat{P} = \mathbf{v}^{\mathbf{x}}$ ($\mathbf{x}$ is public)
- Multi Exponent Argument(MEA) : Construct similar way to IPA, based commitment : [AFG+16]



Generalized BP

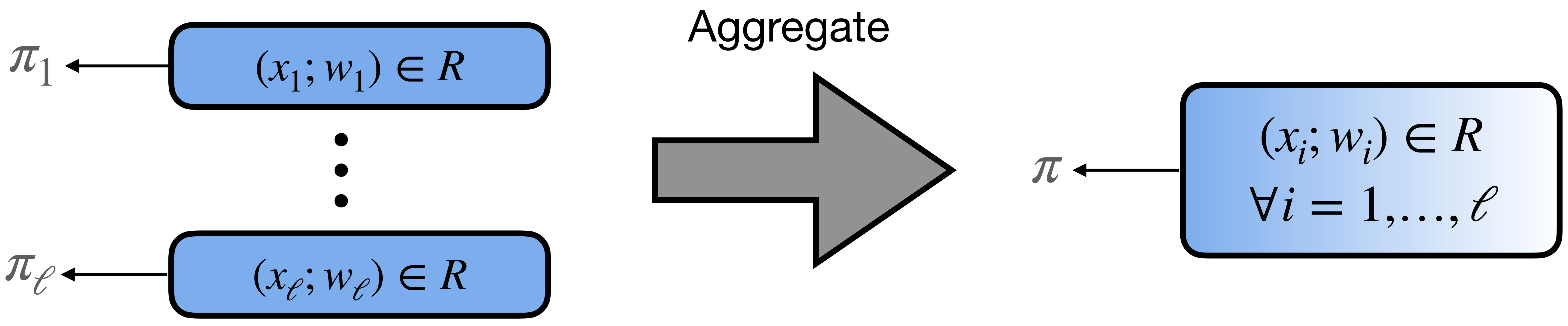


Protocol 1

[AFG+16] : "Structure-Preserving Signatures and Commitments to Group Elements", Journal of Cryptology, 2016

Protocol2 : Aggregation technique

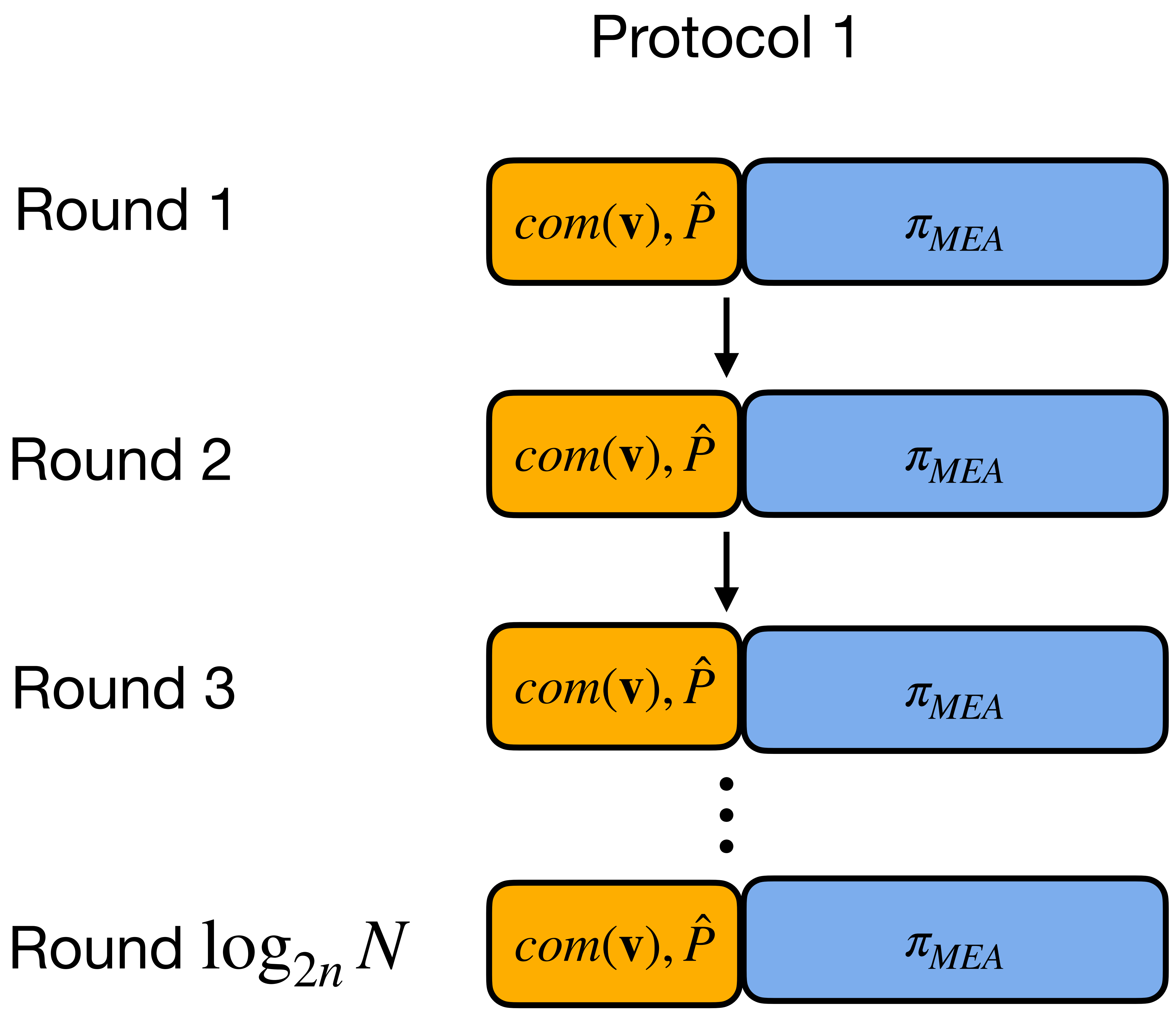
- For each rounds, P sends $com(\mathbf{v}), \hat{P}, \pi_{MEA}$ whose size is $O(\log n)$
- Total Communication : $\log_{2n} N \times O(\log n) = O(\log N)$
- In terms of communication complexity, Protocol1 is the same as BP-IP
- To reduce communication cost more, we apply Aggregation technique
- Aggregation technique : Generating one aggregated Proof for multiple relations



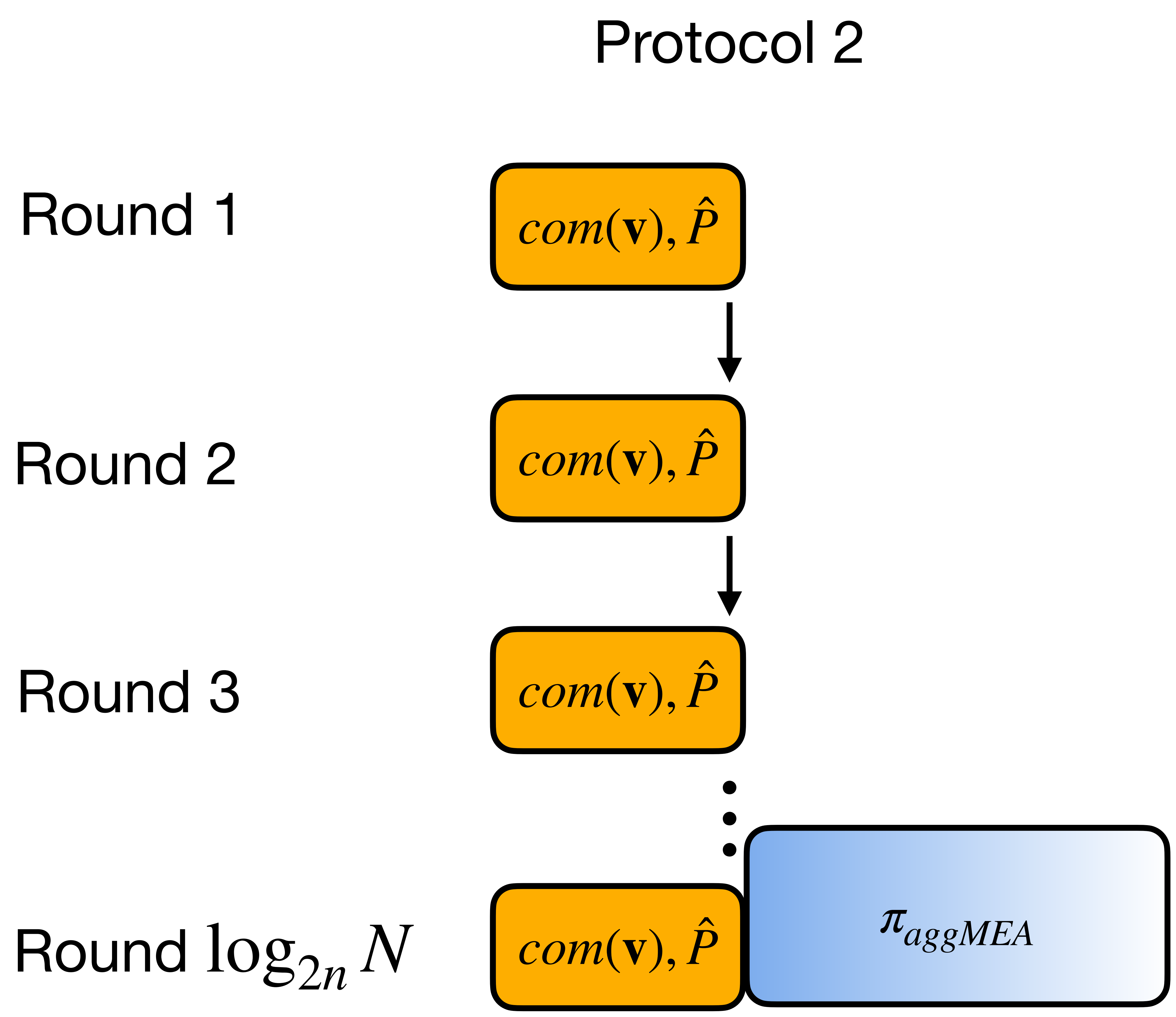
Multi proofs for relation R

One aggregated proof

Protocol2, Sublogarithm Communication

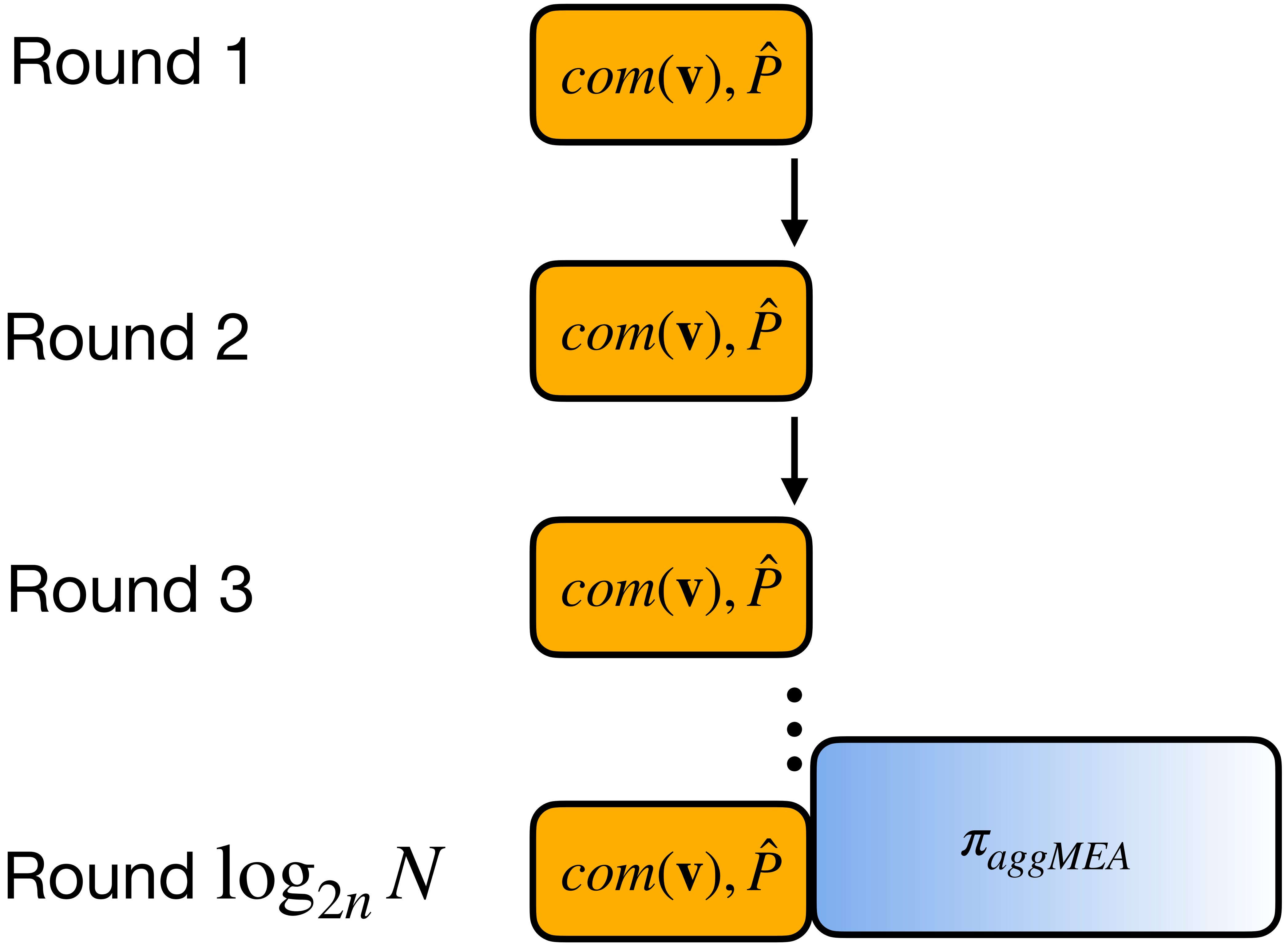


Protocol2, Sublogarithm Communication



Protocol2, Sublogarithm Communication

Protocol 2



Complexity

- Round Reduction
  - Communication : $O(\log_{2n} N)$
  - Verification : $O(N)$
- Aggregated Proof
  - Communication : $O(\log_{2n} N + \log n)$
  - Verification : $O(N)$
- Total
  - Communication : $O(\log_{2n} N + \log n)$
  - Verification : $O(N)$

- Let $n = 2^{\sqrt{\log N}}$, then we get $O(\sqrt{\log N})$ communication

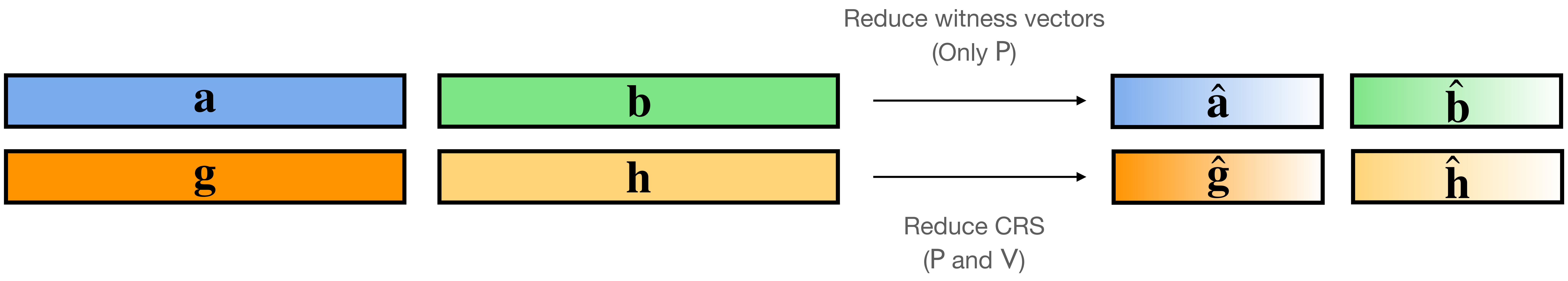
* total prover complexity increase to $O(N \cdot 2^{\sqrt{\log N}})$

Protocol3 :
Sublinear Verifier under DL

- **Outer Pairing Product**
- **Discrete Logarithm Relation Assumption**

Observation 2 : Verifier of BP-IP

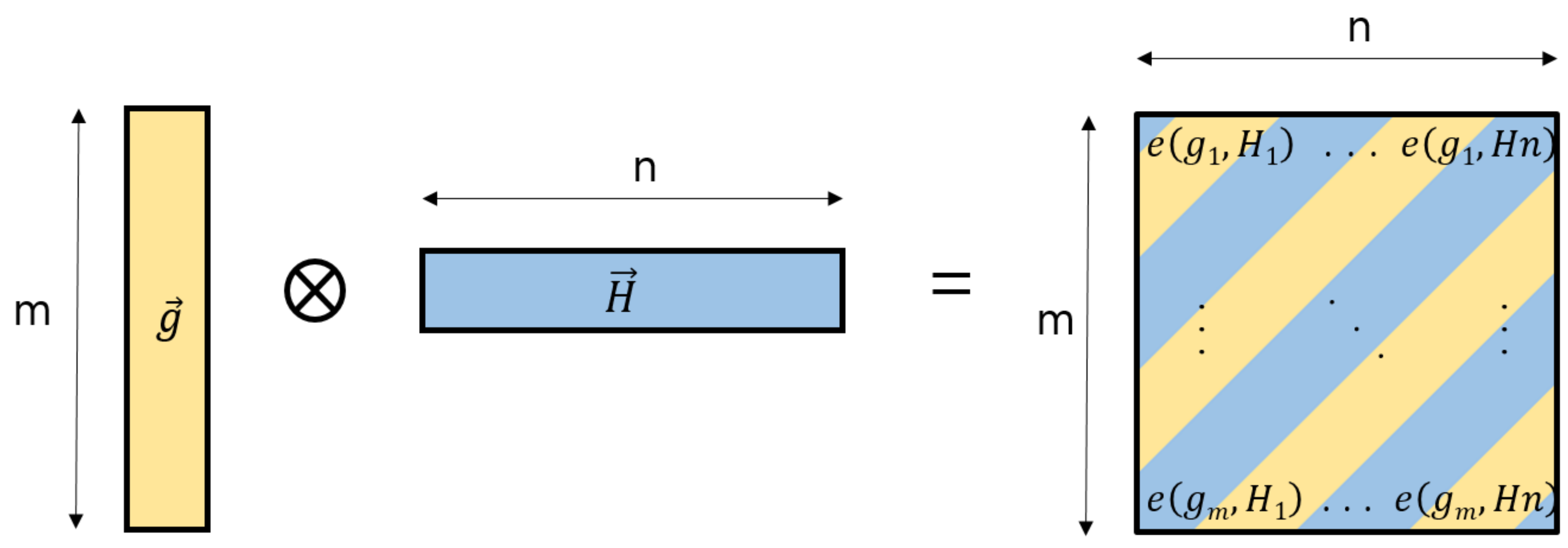
- In BP-IP, sample $\mathbf{g}, \mathbf{h} \leftarrow \mathbb{G}^N$ uniformly and use them as Common Reference String(CRS)
- For each round, P and V halve $\mathbf{g}, \mathbf{h}$ and update to $\hat{\mathbf{g}}, \hat{\mathbf{h}}$
- $\hat{\mathbf{g}} = \mathbf{g}_L^{x^{-1}} \circ \mathbf{g}_R^{x} \in \mathbb{G}^{\frac{N}{2}}, \hat{\mathbf{h}} = \mathbf{h}_L^{x} \circ \mathbf{h}_R^{x^{-1}} \in \mathbb{G}^{\frac{N}{2}}$
- This update requires $2N$ group exponentiations
- To avoid linear verification, we consider to change CRS form



Outer-Pairing Product

- Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t)$ be groups of prime order p with bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_t$
- For $\mathbf{g} \in \mathbb{G}_1^m$ and $\mathbf{H} \in \mathbb{G}_2^n$, define

$$\mathbf{g} \otimes \mathbf{H} := \begin{bmatrix} e(g_1, H_1) & \dots & e(g_1, H_n) \\ \vdots & \ddots & \vdots \\ e(g_m, H_1) & \dots & e(g_m, H_n) \end{bmatrix} \in \mathbb{G}_t^{m \times n}$$



Outer-pairing product

- Let $N = mn$ be a vector length of our IPA.
- How about using $\mathbf{g} \otimes \mathbf{H}, \mathbf{h} \otimes \mathbf{H} \in \mathbb{G}_t^{m \times n}$ rather than $\mathbf{g}, \mathbf{h} \in \mathbb{G}^N$ on BP-IP?

2nd Generalized BP-IP, DLR assumption

Definition *(DRL assumption) : Let* $\mathbf{g} \in \mathbb{G}^N$ *be uniformly chosen group elements. Then, it is intractable to find a non-trivial relation* $\mathbf{z} \in \mathbb{Z}_p^N$ *such that* $\mathbf{g}^{\mathbf{z}} = 1_{\mathbb{G}}$

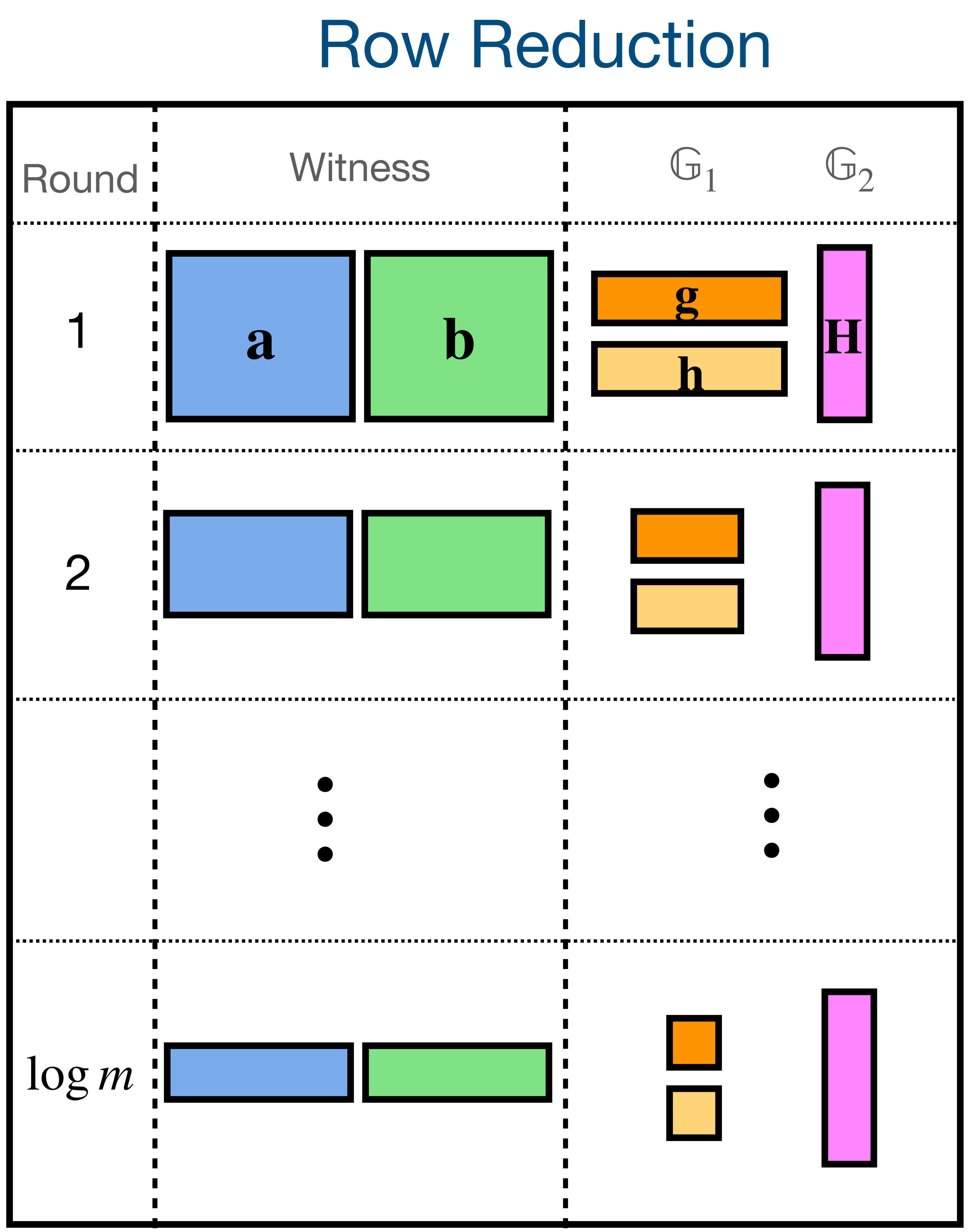
- BP-IP provide knowledge soundness under Discrete Logarithm Relation(DLR) assumption
- It is known that DRL assumption is equivalent to DL assumption

Theorem *(Generalized DRL) : It is intractable to find a non-trivial relation* $\mathbf{z} \in \mathbb{Z}_p^{m\times n}$ *of* $\mathbf{g} \otimes \mathbf{H} \in \mathbb{G}_t^{m\times n}$ *where* $\mathbf{g} \leftarrow \mathbb{G}_1, \mathbf{H} \leftarrow \mathbb{G}_2$ *chosen uniformly and DL assumption is hold on* $\mathbb{G}_1$ *and* $\mathbb{G}_2$

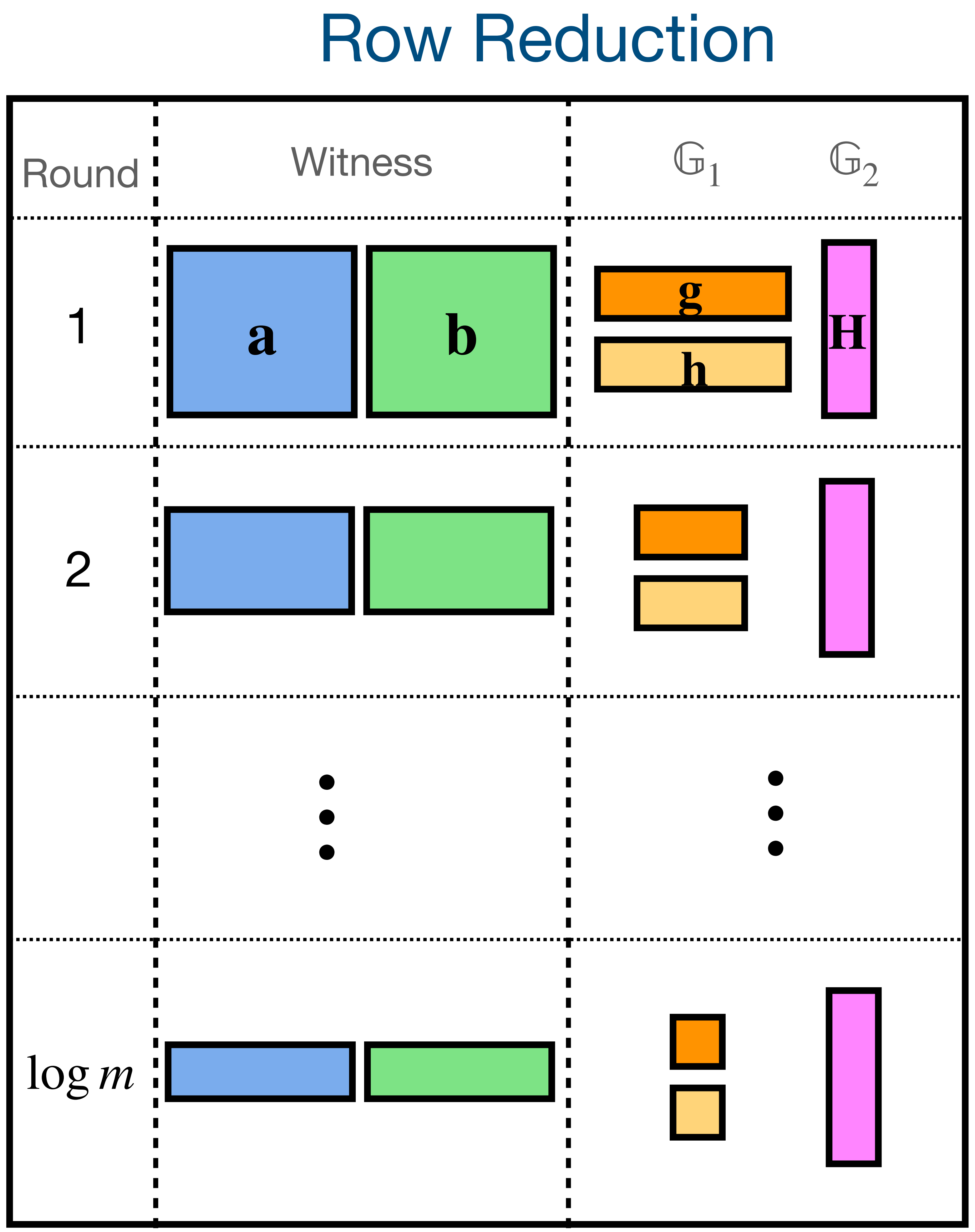
- The theorem guarantees hardness of finding non-trivial relation of $\mathbf{g} \otimes \mathbf{H}$
- We use $\{\mathbf{g}, \mathbf{h} \in \mathbb{G}_1^m, \mathbf{H} \in \mathbb{G}_2^n\}$ as CRS of our IPA, Protocol3

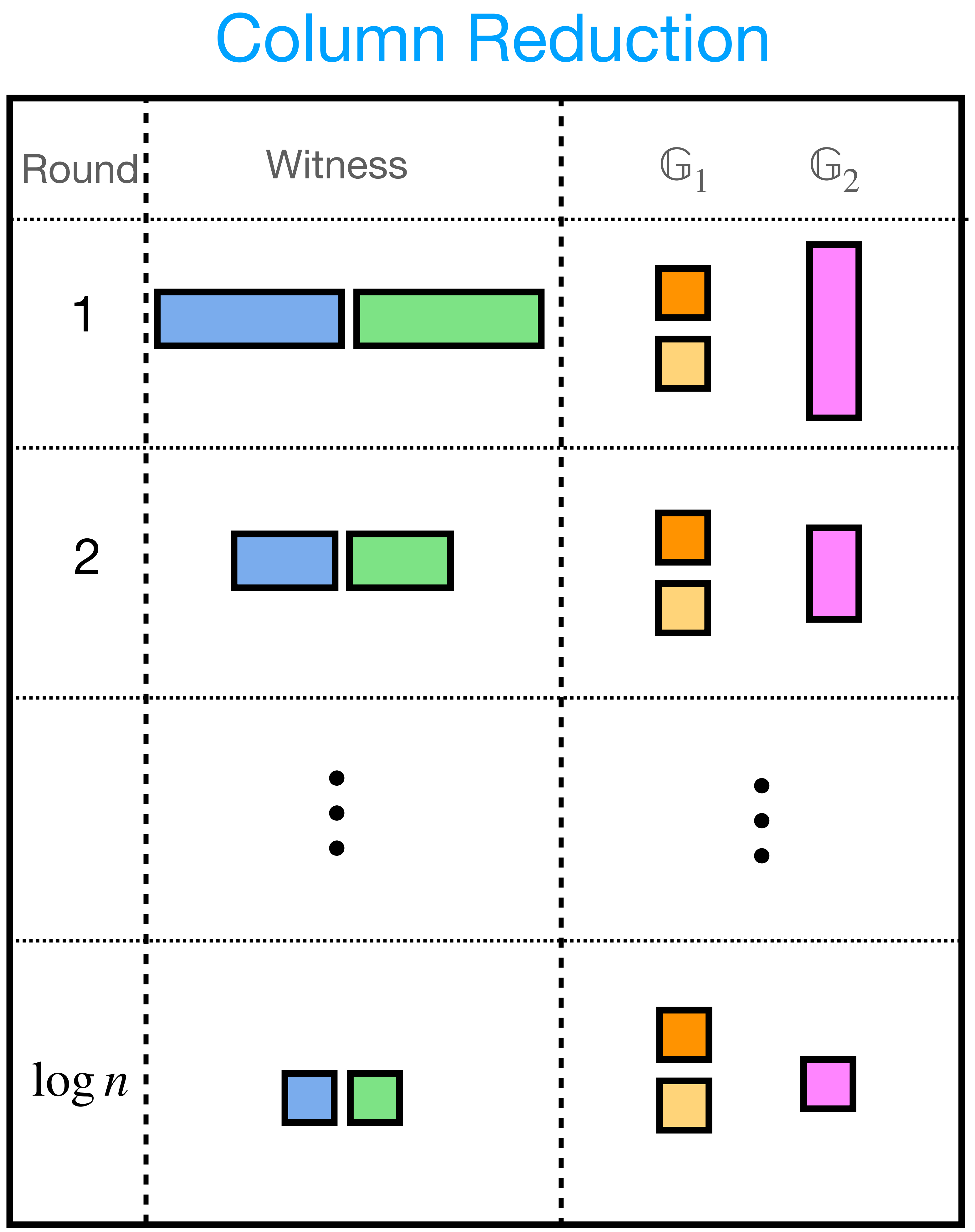
$$\mathbf{g} \otimes \mathbf{H}, \mathbf{h} \otimes \mathbf{H} \in \mathbb{G}_t^{m\times n} \xleftarrow{\text{Construct}} \{\mathbf{g}, \mathbf{h} \in \mathbb{G}_1^m, \mathbf{H} \in \mathbb{G}_2^n\} \xleftarrow{\text{Uniform Sampling}} \boxed{\text{Random Sampler}}$$

Protocol3 : Sublinear Verifier



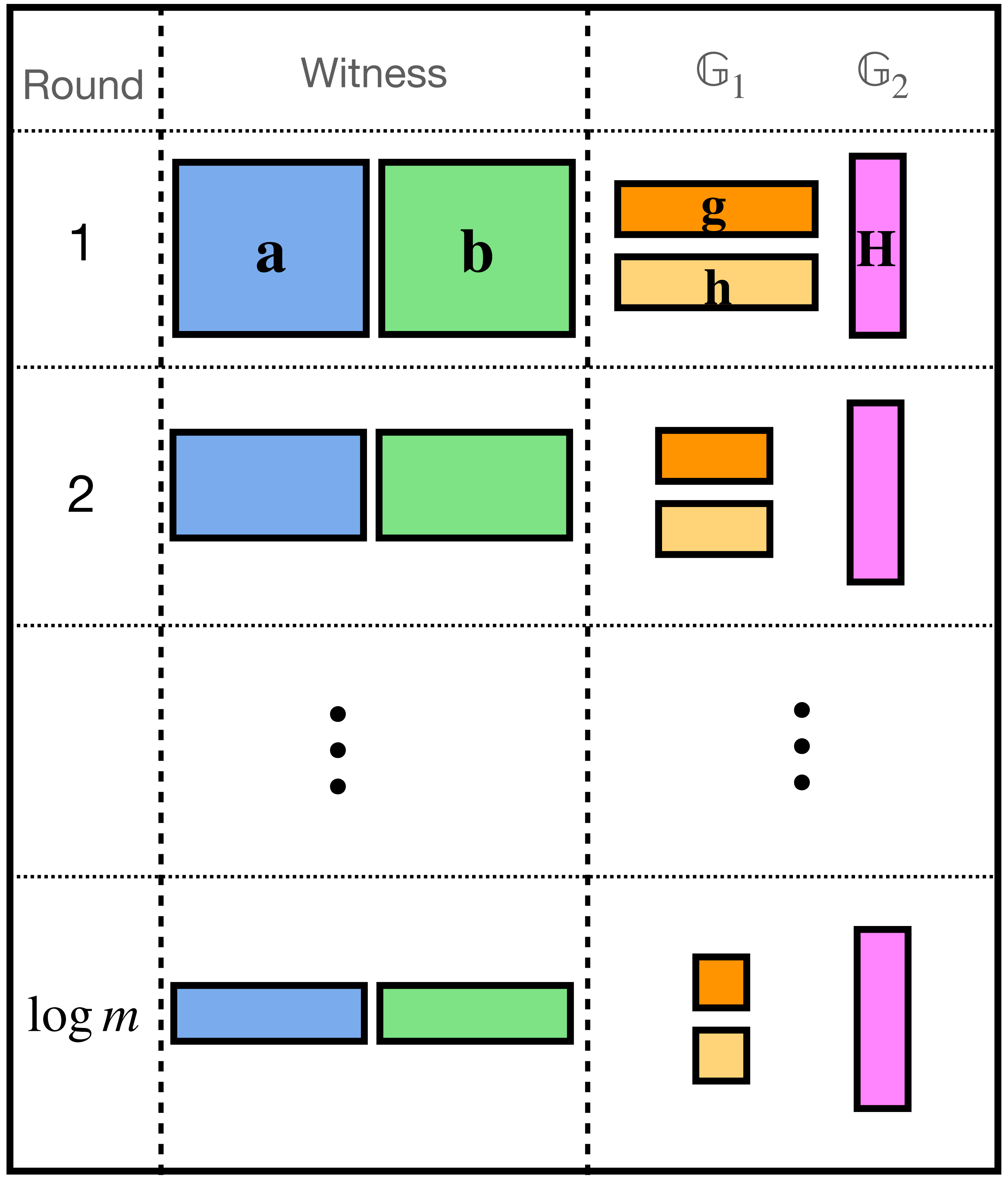
Protocol3 : Sublinear Verifier



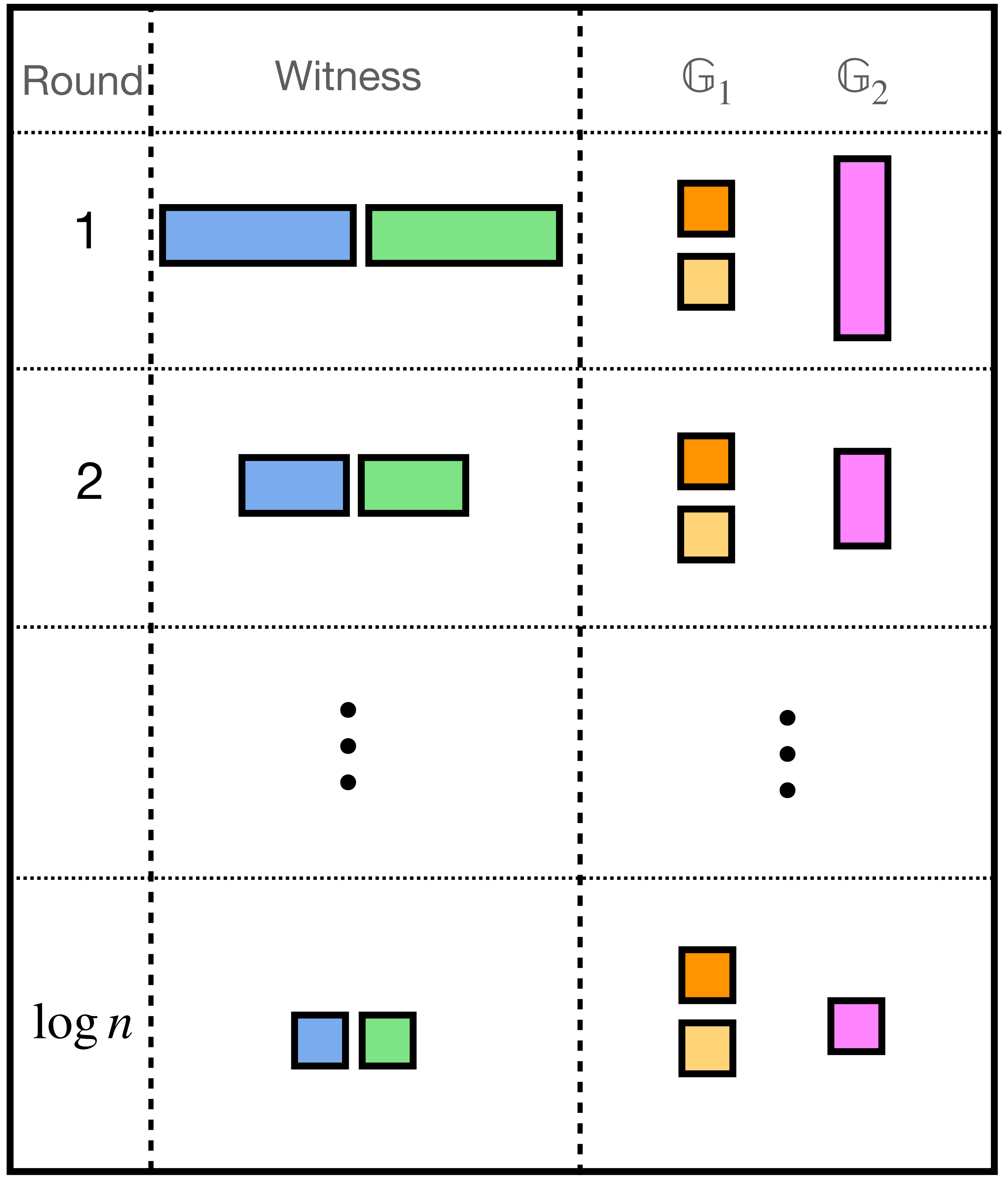


Protocol3 : Sublinear Verifier

Row Reduction



Column Reduction



Complexity

- Row Reduction
  - Communication : $O(\log m)$
  - Verification : $O(m)$
- Column Reduction
  - Communication : $O(\log n)$
  - Verification : $O(n)$
- Total
  - Communication : $O(\log mn)$
  - Verification : $O(n + m)$

- Let $m = n = \sqrt{N}$, then we get $O(\sqrt{N})$ Verification

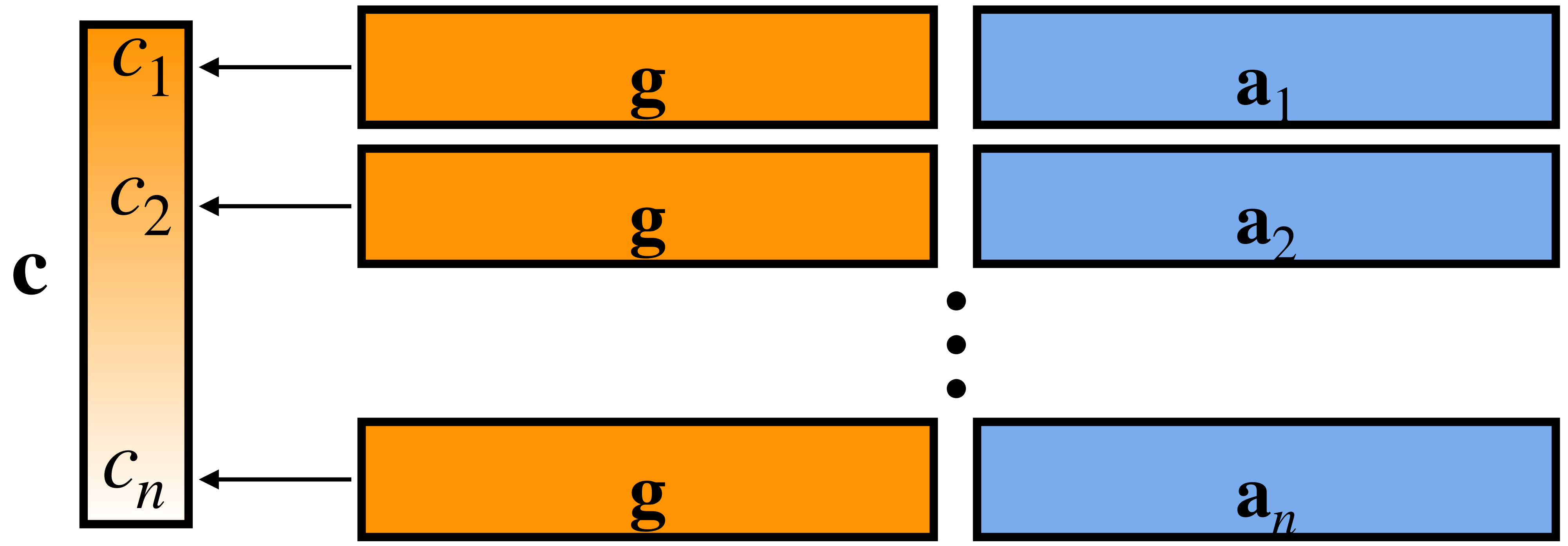
Protocol4 :
Sublinear Verifier w/o Pairing

- **Two-tier commitment scheme**
- **Commitment to Elliptic curve**
- **Commit-and-Prove and Aggregation technique**

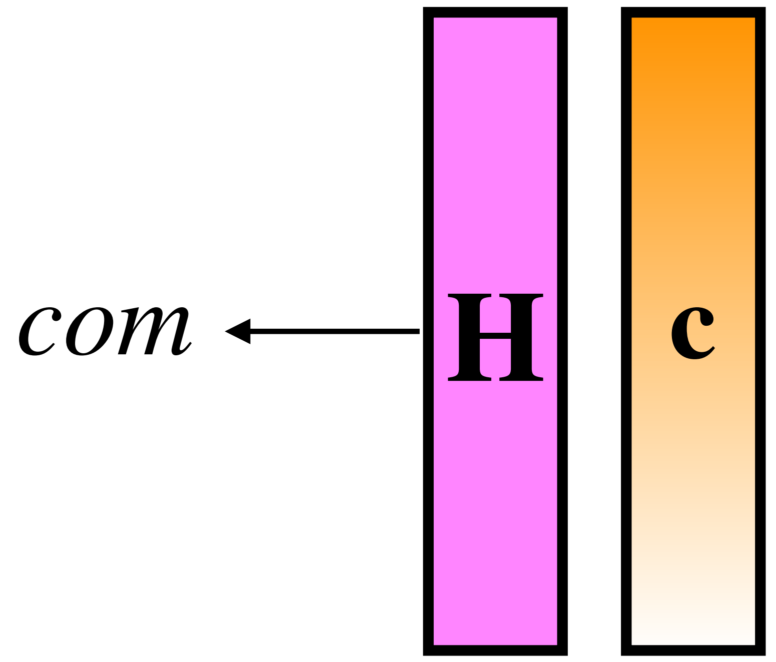
Another view of Protocol3

- In Protocol3, We construct $\mathbf{g} \otimes \mathbf{H} \in \mathbb{G}_t^{m \times n}$ for commitment to $\mathbf{a} \in \mathbb{Z}_p^{m \times n}$
- Another view : Two-tier Commitment
  - Commitments via 2 steps

1. For all j-th column vector $\mathbf{a}_j$ of matrix $\mathbf{a}$, commit to $\mathbf{a}_j$ (Pedersen Commitment)
2. Commit to results of first commitments (AFGHO Commitment)



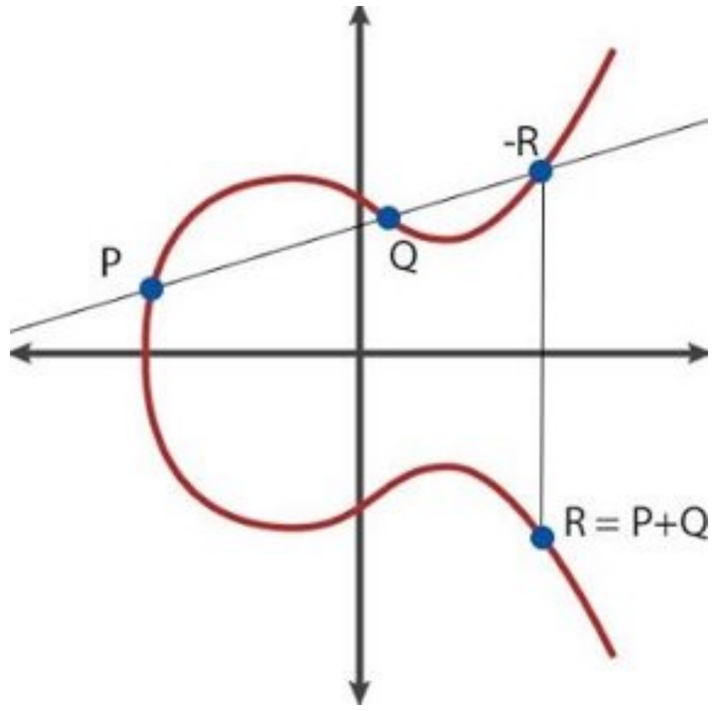
First step : Parallel commitments



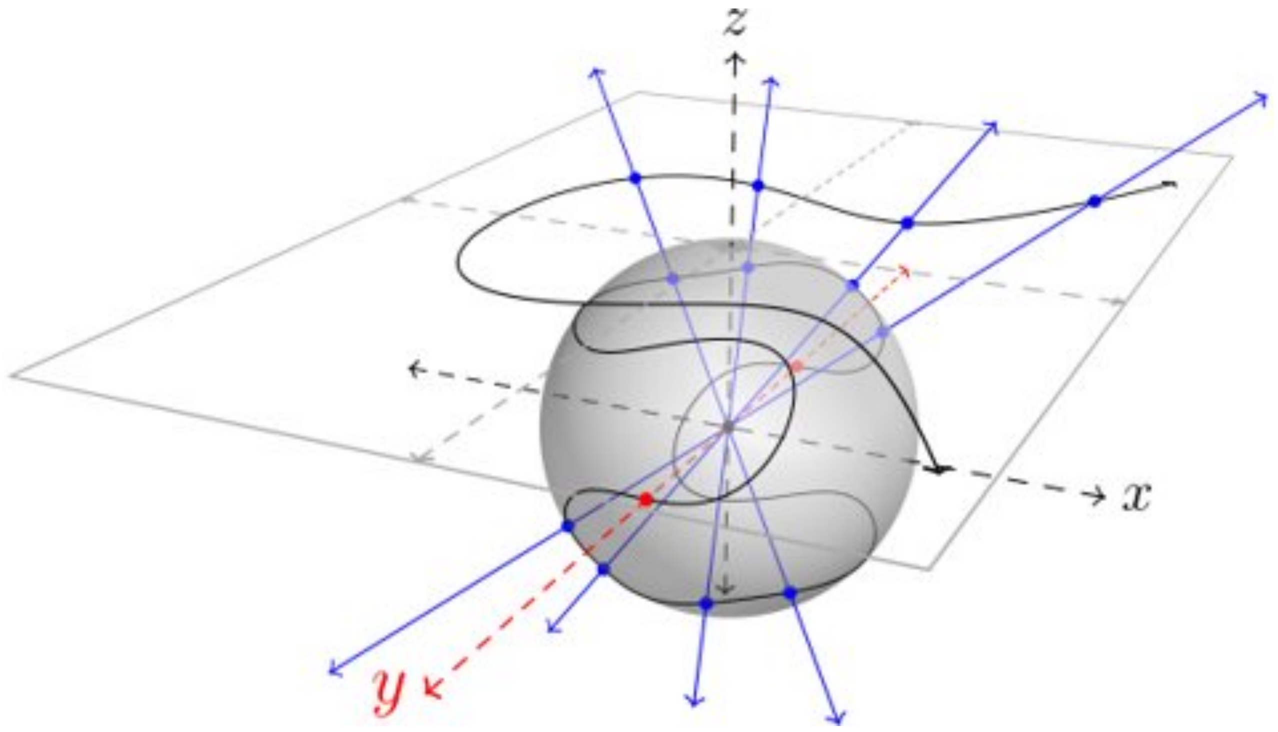
Second step : Commit to results

Commitment to Elliptic Curve

- To commitment results without pairing, consider a commitment to Elliptic Curve points
- EC representations : Affine representation on $\mathbb{Z}_q^2$, Projective representation on $\mathbb{Z}_q^3$
- It is hard to represent "point at infinity" from Affine representation
- There is a complete addition formula from Projective representation [RCB16]
- From Projective representation, we consider a EC as a vector in $\mathbb{Z}_q^3$ and then apply Pedersen commitment to the vector



Affine Representation



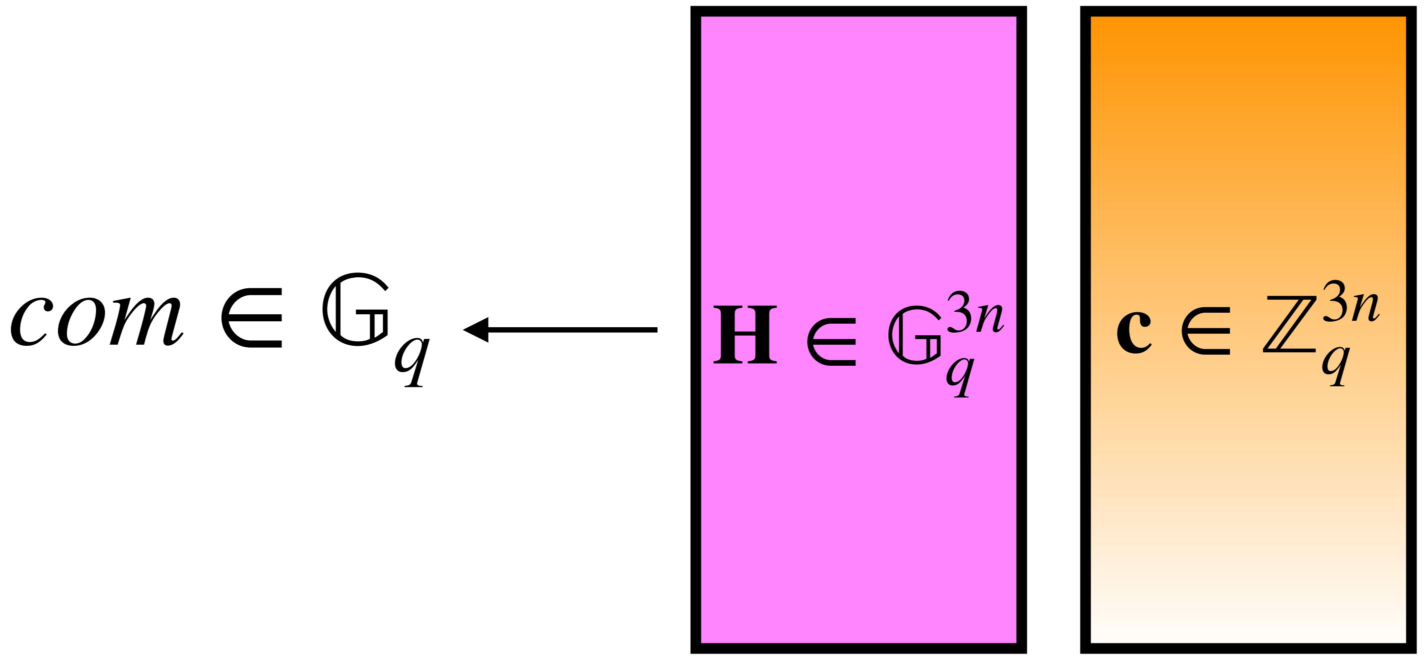
Projective Representation

[RCB16] :"Complete Addition Formulas for Prime Order Elliptic Curves", *EUROCRYPT 2016*

New Two-tier commitment

- Set a pair of elliptic curves : $(\mathbb{G}_p, \mathbb{G}_q)$ where $\mathbb{G}_p = E(\mathbb{Z}_q)$
- After first commitments, consider the result group elements as vectors over $\mathbb{Z}_q$
- Second commitment : Pedersen commitment based $\mathbb{G}_q$
- The commitment guarantees binding of message, but not provides homomorphic property

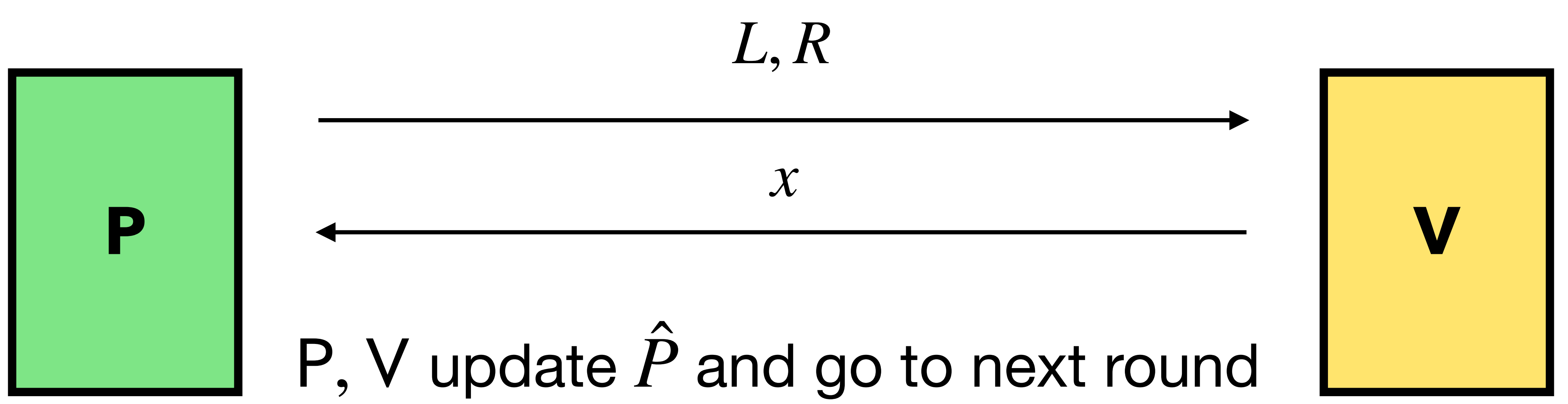
First step : Parallel commitments
Result : n group elements $\mathbf{c}$



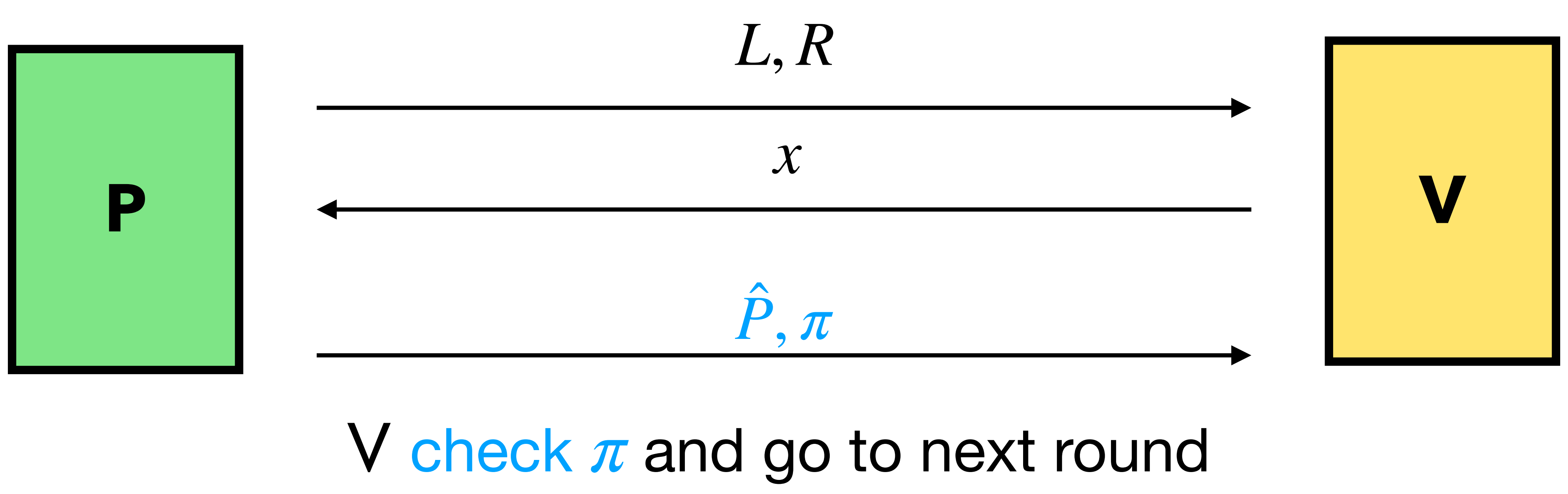
Second step : Commit to results
View $\mathbf{c}$ as vector over $\mathbb{Z}_q$

Commit-and-Prove, Aggregation

- Without Homomorphic property, V cannot update $\hat{P}$, which is similar issue in Protocol1
- Apply Commit-and-Prove approach (Protocol1)
- For each round, P sends updated instance $\hat{P}$ with proof π to V
- After using commit-and-prove approach, total proof size is $O(\log^2 N)$
- To reduce total proof size more, apply aggregation technique (Protocol2)



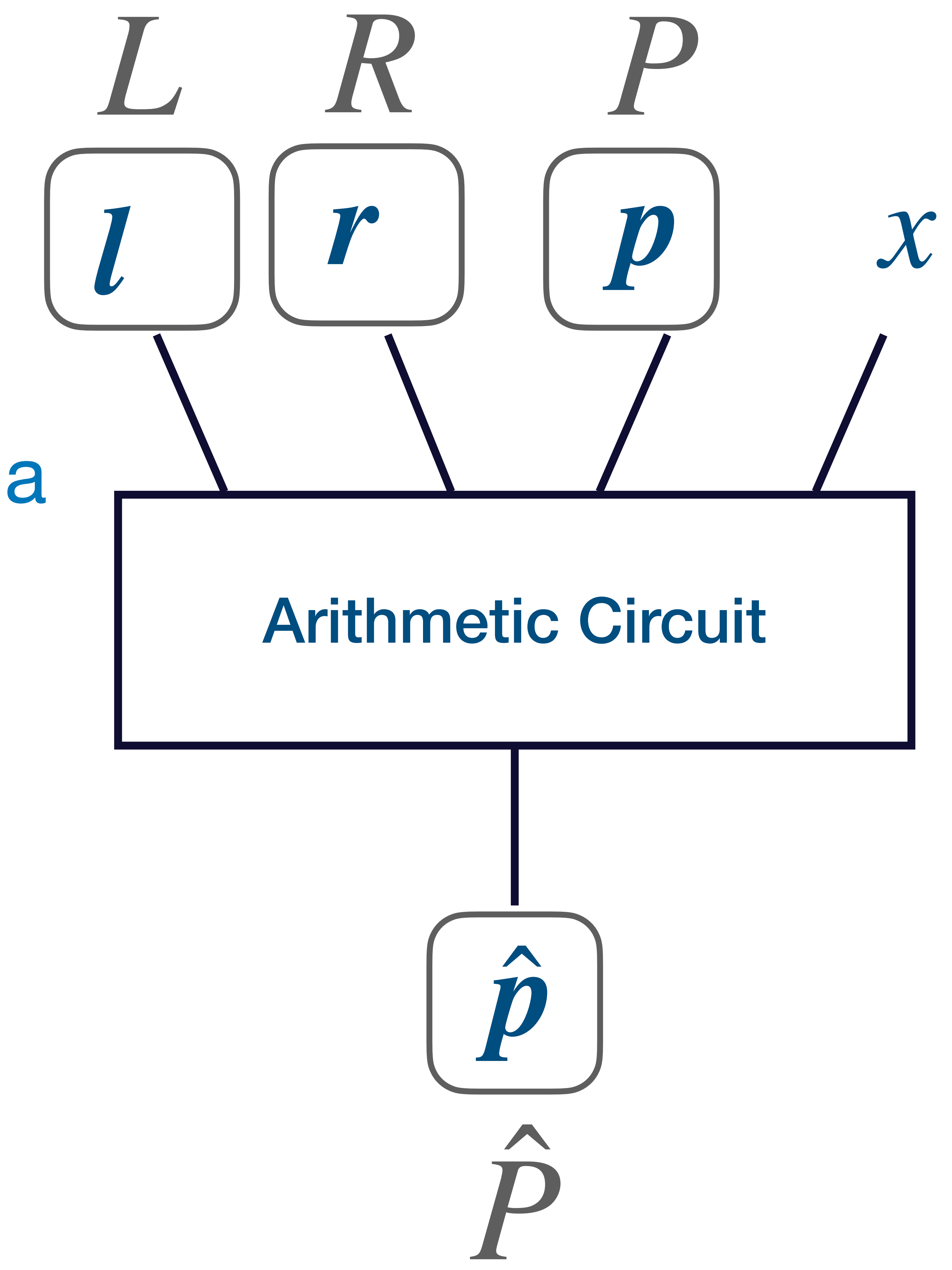
BP-IP, Protocol3 Reduction



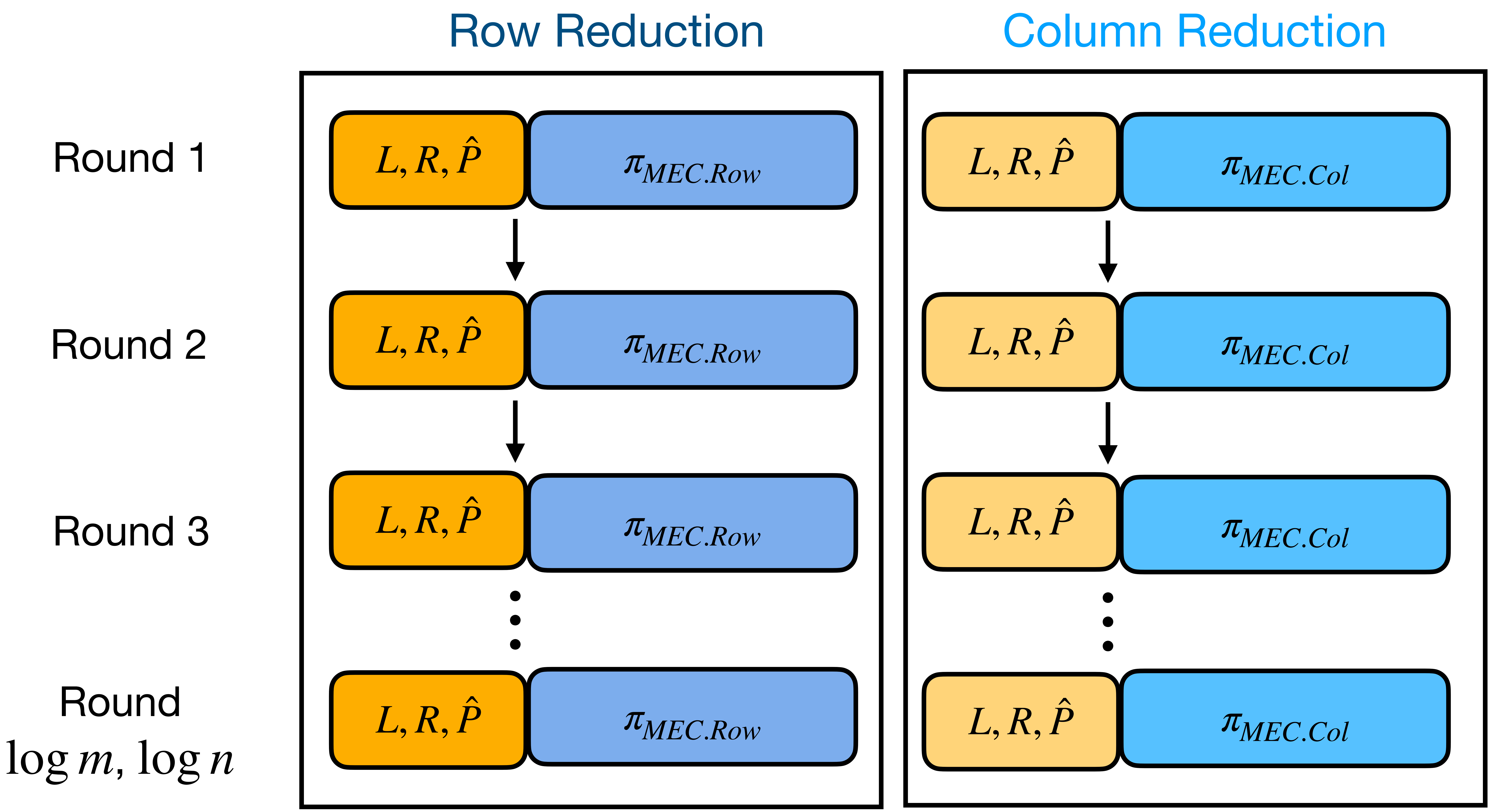
Reduction for new commitment

Multi Elliptic Curve argument

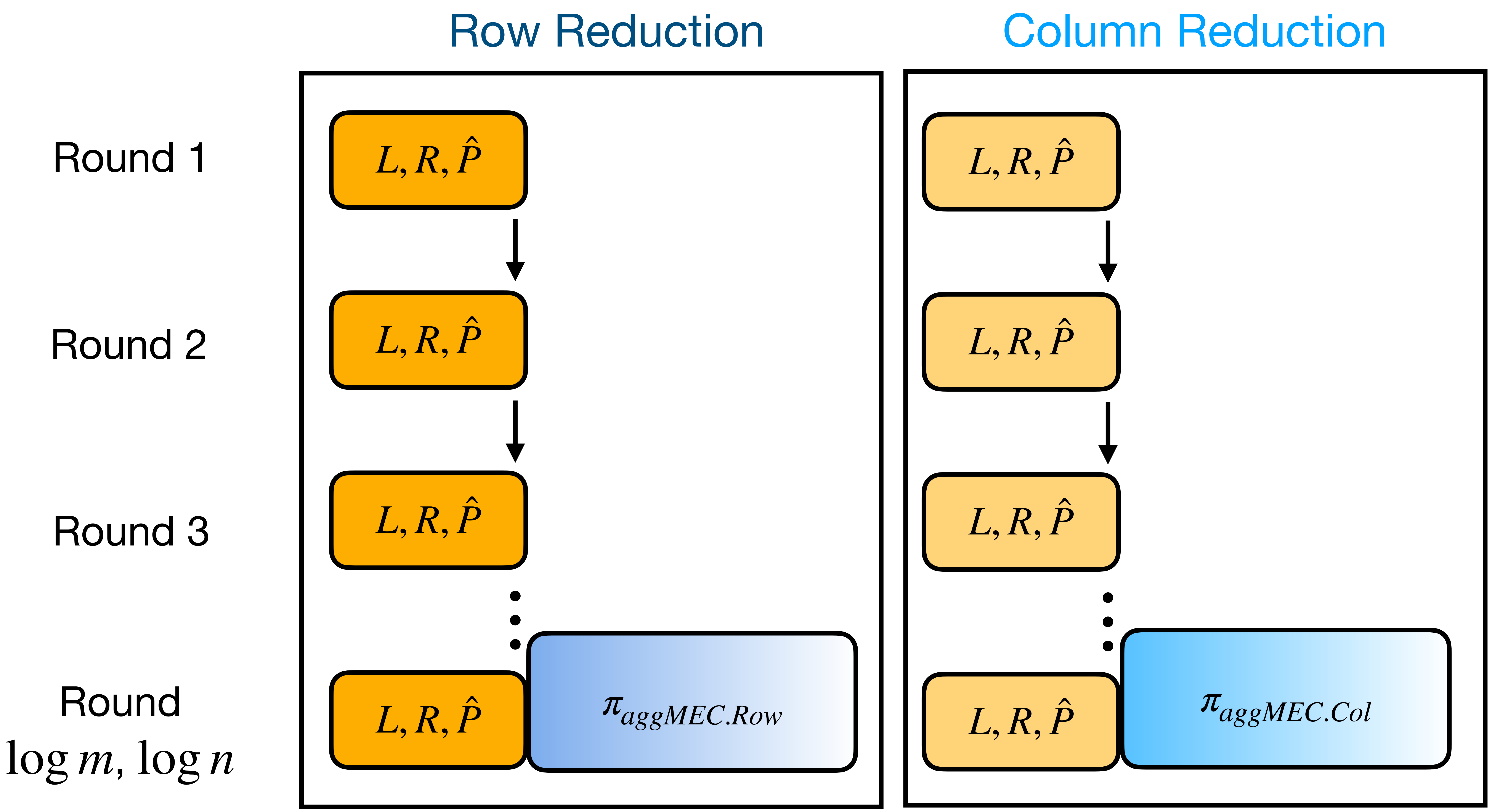
- What should the proof π convince?
- Knowledge of elliptic curve points satisfy elliptic curve relation
- Instance : $L, R, P, \hat{P} \in \mathbb{G}_q$, Witness : $\boldsymbol{l}, \boldsymbol{r}, \boldsymbol{p}, \hat{\boldsymbol{p}} \in \mathbb{G}_p^n$
  - Represent elliptic curve relation using Complete Addition Formula
  - Use AoK for arithmetic circuit on $\mathbb{Z}_q$
  - Proof size : $O(\log n)$ / Verification : $O(n)$
- MEC.Row : Multi Elliptic Curve argument for Row reduction
- MEC.Col : Multi Elliptic Curve argument for Column reduction



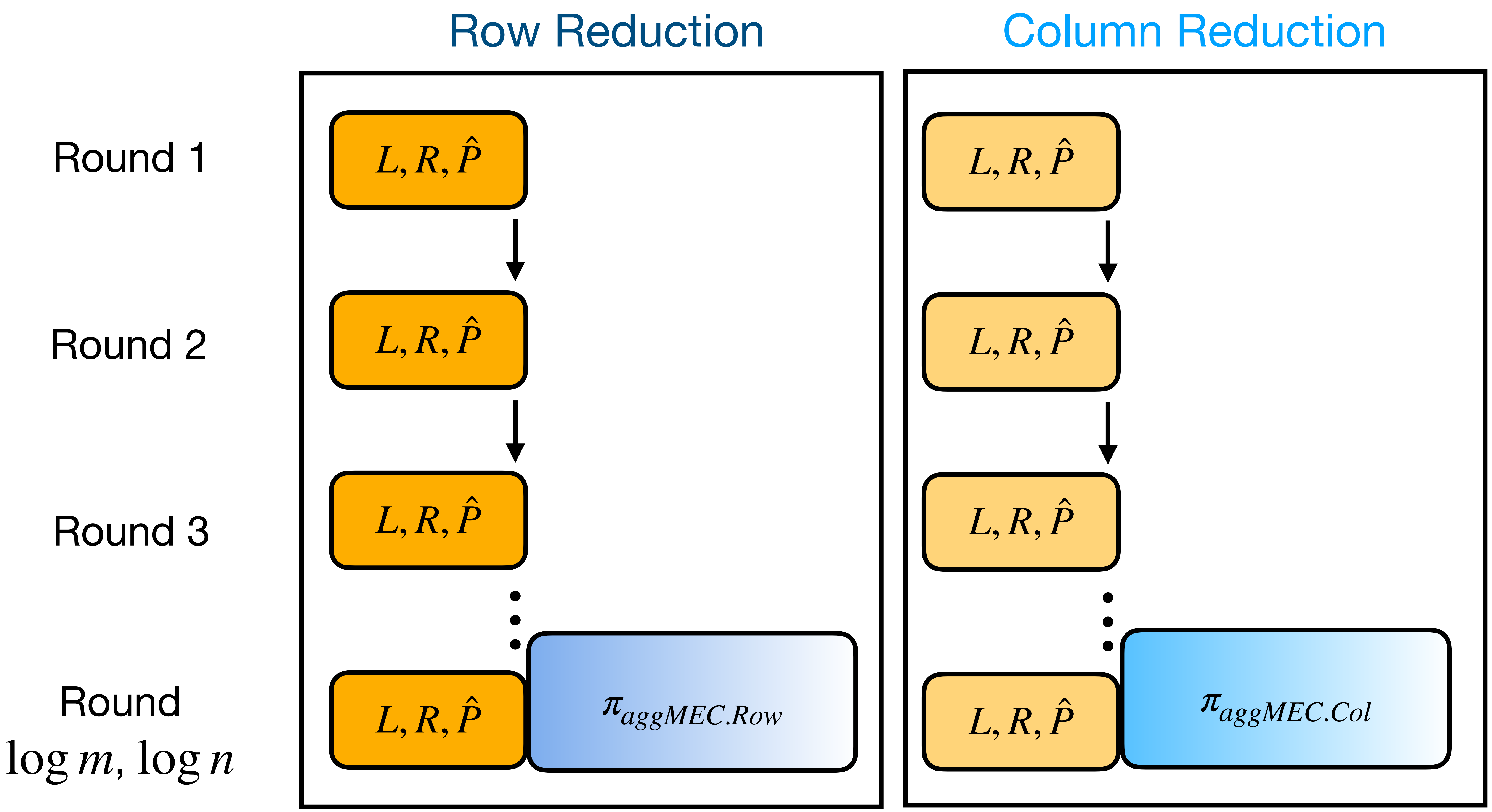
Protocol4 : Sublinear Verifier w/o Pairing



Protocol4 : Sublinear Verifier w/o Pairing



Protocol4 : Sublinear Verifier w/o Pairing



Complexity

- Row Reduction
  - Communication : $O(\log mn)$
  - Verification : $O(m + n \log m)$
- Column Reduction
  - Communication : $O(\log n)$
  - Verification : $O(n)$
- Total
  - Communication : $O(\log mn)$
  - Verification : $O(m + n \log m)$

- Let $m = n = \sqrt{N}$, then we get $O(\sqrt{N} \log N)$ Verification

Conclusion

We propose three transparent IPAs, which can be combined to reduction ZKA to IPA

From the reduction, we construct three ZKAs

- ZKA with Sublogarithmic communication
  - As far as we know, this is the first sublogarithmic ZKA in transparent setting
- ZKA with sublinear verifier under DL assumption
  - Although the argument use pairing operation, its soundness is based on DL assumption
- ZKA with sublinear verifier without pairing
  - Without reliance of pairings, we show possibility of sublinear verifier in DL setting

Thank You

ePrint : https://eprint.iacr.org/2021/1450.pdf