Towards Fast Verification: (Polynomial) Commitments from Lattices

Ngoc Khanh Nguyen

Towards succinct arguments with succinct verification

Commitments with succinct proof of opening

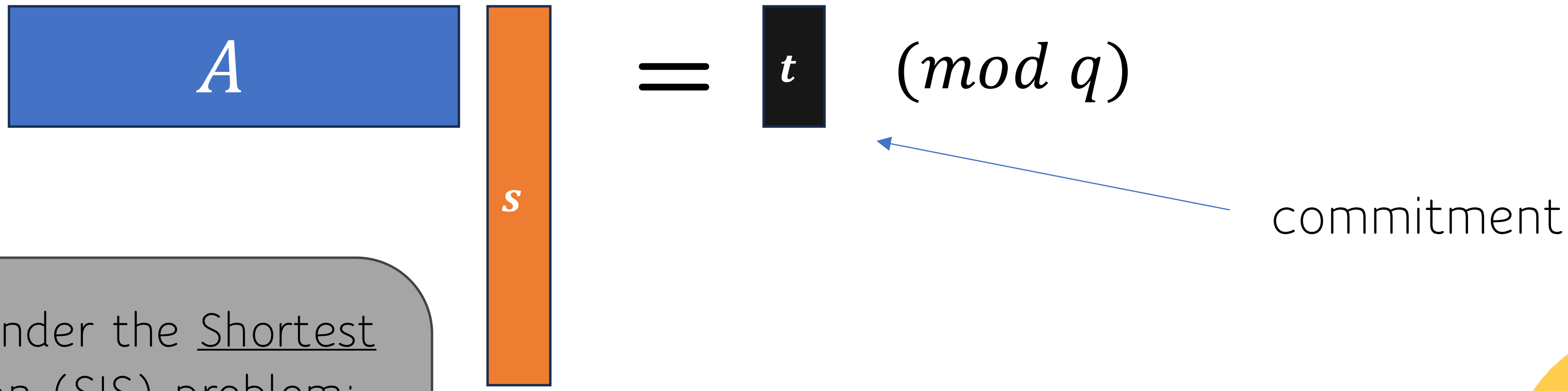
Polynomial commitments

Efficient generic-purpose zkSNARK

Even this is hard in the lattice setting

Ajtai commitment [Ajt96]

- Let $\mathbb{Z}_q$ be a ring of integers modulo $\boldsymbol{q}$.
- To commit to a short message vector $\boldsymbol{s}$, we compute:



Binding holds under the Shortest Integer Solution (SIS) problem:

Given a random matrix $\boldsymbol{A}$, find a short non-zero vector $\boldsymbol{s}$ s.t.

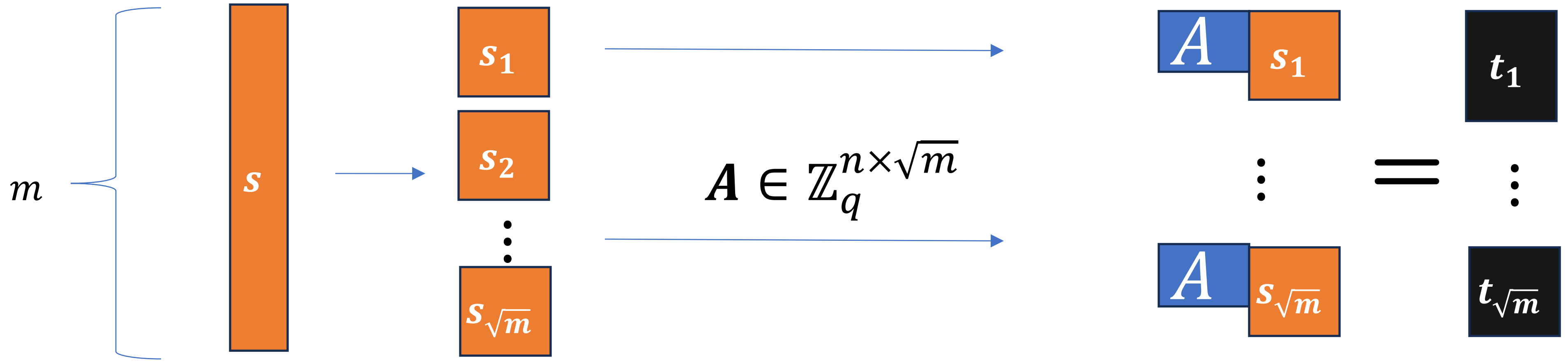
$$\boldsymbol{As} = \boldsymbol{0}\ (mod\ q)$$

- In lattice-bulletproofs [BLNS20,AL21,ACK21], verifier has to process the whole $\boldsymbol{A}$.
- More structure to $\boldsymbol{A}$ [CLM23]?
- Preprocessing [BCS23]?

Outline

1. **Square-root approach**
2. Cube-root approach
3. Commitment with a poly-log opening proof
4. Polynomial commitments
5. Quiz!!!

Square-root approach [BBCDGL18]



A commitment to a short message vector $\boldsymbol{s}$ is: $\boldsymbol{t_1} \cdots \boldsymbol{t_{\sqrt{m}}}$

Size: $n\sqrt{m}\log q$

Mathematically: $(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$

Finding different short $\boldsymbol{s}, \boldsymbol{s}'$ s.t.

$$(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t} = (\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s}'$$

Breaking SIS for $\boldsymbol{A}$

Tensor product refresher

$$\mathbf{A} \otimes \mathbf{B} = \begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{bmatrix}$$

$$\begin{aligned} \mathbf{A} \otimes (\mathbf{B} + \mathbf{C}) &= \mathbf{A} \otimes \mathbf{B} + \mathbf{A} \otimes \mathbf{C}, \\ (\mathbf{B} + \mathbf{C}) \otimes \mathbf{A} &= \mathbf{B} \otimes \mathbf{A} + \mathbf{C} \otimes \mathbf{A}, \\ (k\mathbf{A}) \otimes \mathbf{B} &= \mathbf{A} \otimes (k\mathbf{B}) = k(\mathbf{A} \otimes \mathbf{B}), \\ (\mathbf{A} \otimes \mathbf{B}) \otimes \mathbf{C} &= \mathbf{A} \otimes (\mathbf{B} \otimes \mathbf{C}), \\ \mathbf{A} \otimes \mathbf{0} &= \mathbf{0} \otimes \mathbf{A} = \mathbf{0}, \end{aligned}$$

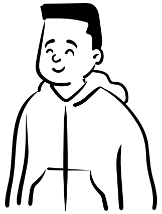
Mixed product property

$$(\mathbf{A} \otimes \mathbf{B})(\mathbf{C} \otimes \mathbf{D}) = (\mathbf{AC}) \otimes (\mathbf{BD}).$$

Opening proof

$(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$ and $\boldsymbol{s}$ is short

$\boldsymbol{s}, \boldsymbol{t}$



$\boldsymbol{t}$

κ used for soundness

$\boldsymbol{C} \leftarrow \{0,1\}^{\kappa \times \sqrt{m}}$

$\boldsymbol{C}$ ←

$\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_{\sqrt{m}})\boldsymbol{s}$

$\boldsymbol{z}$ →

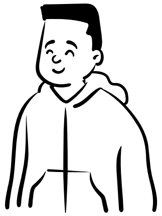
Check:

1. $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{z} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{C} \otimes \boldsymbol{I}_{\sqrt{m}})\boldsymbol{s} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{t}$
2. $\boldsymbol{z}$ is short

Communication size: $\kappa\sqrt{m} + \kappa\sqrt{m}\log q = \tilde{O}(\sqrt{m})$ bits
Verification time: $\tilde{O}(\sqrt{m})$

Coordinate-wise special soundness

$(\boldsymbol{x}, \boldsymbol{w})$



$\boldsymbol{x}$

$\boldsymbol{A}$ →

$\boldsymbol{C}$ ←

$\boldsymbol{C} \leftarrow S^t$

$\boldsymbol{Z}$ →

Special soundness: given two valid transcripts $(\boldsymbol{A}, \boldsymbol{C}, \boldsymbol{Z})$ and $(\boldsymbol{A}, \boldsymbol{C}', \boldsymbol{Z}')$ with different $\boldsymbol{C} \neq \boldsymbol{C}'$, one can extract $\boldsymbol{w}$.

CWSS: given $t+1$ valid transcripts $(\boldsymbol{A}, \boldsymbol{C}_i, \boldsymbol{Z}_i)_{i \in [0,t]}$ such that

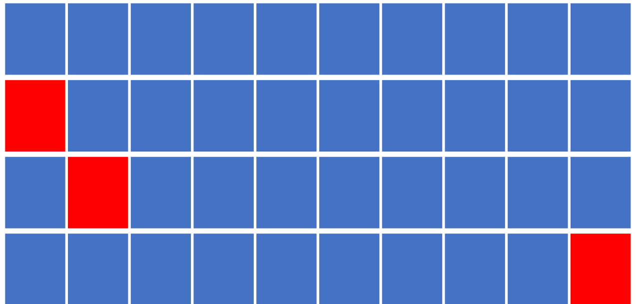
$\boldsymbol{c}_0$

$\boldsymbol{c}_1$

$\boldsymbol{c}_2$

⋮

$\boldsymbol{c}_t$



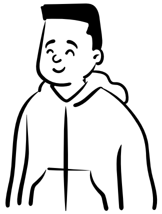
one can extract $\boldsymbol{w}$.

[FMN23]: CWSS implies knowledge soundness with error $t/|S|$.

Proof of CWSS

$(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$ and $\boldsymbol{s}$ is short

$\boldsymbol{s}, \boldsymbol{t}$



$\boldsymbol{t}$

$\boldsymbol{C} \leftarrow \{0,1\}^{\kappa \times \sqrt{m}}$

$\boldsymbol{C}$ ←

$\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_{\sqrt{m}})\boldsymbol{s}$

$\boldsymbol{z}$ →

Check:

1. $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{z} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{C} \otimes \boldsymbol{I}_{\sqrt{m}})\boldsymbol{s} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{t}$
2. $\boldsymbol{z}$ is short

Suppose we're given transcripts $(\boldsymbol{C}, \boldsymbol{z}), (\boldsymbol{C}', \boldsymbol{z}')$ where $\boldsymbol{C}$ and $\boldsymbol{C}'$ differ in exactly the $1 \leq j \leq \sqrt{m}$ column; say $c_{i,j} \neq c'_{i,j}$ for some i.

For each j, we will extract a short $\boldsymbol{s}_j^*$ such that $\boldsymbol{A}\boldsymbol{s}_j^* = \boldsymbol{t}_j$

We can then collect all $\boldsymbol{s}_j^*$ to recover the full witness $\boldsymbol{s}$.

[FMN23]: Soundness error $\sqrt{m}/2^\kappa$.

Suppose we're given transcripts $(\boldsymbol{C},\boldsymbol{z}),(\boldsymbol{C}',\boldsymbol{z}')$ where $\boldsymbol{C}$ and $\boldsymbol{C}'$ differ in exactly the $1 \le j \le \sqrt{m}$ column; say $c_{i,j} \neq c'_{i,j}$ for some i.

For each j, we will extract a short $\boldsymbol{s}_j^*$ such that $\boldsymbol{A}\boldsymbol{s}_j^* = \boldsymbol{t}_j$

Proof of CWSS

$(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$ and $\boldsymbol{s}$ is short

$\boldsymbol{s}, \boldsymbol{t}$

$\boldsymbol{t}$

$\boldsymbol{C} \leftarrow \{0,1\}^{\kappa \times \sqrt{m}}$

$\boldsymbol{C}$ (←)

$\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_{\sqrt{m}})\boldsymbol{s}$

$\boldsymbol{z}$ (→)

Check:

1. $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{z} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{C} \otimes \boldsymbol{I}_{\sqrt{m}})\boldsymbol{s} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{t}$
2. $\boldsymbol{z}$ is short

Consider the vectors $\boldsymbol{z} = (\boldsymbol{z}_1, \dots, \boldsymbol{z}_{\sqrt{m}})$ and $\boldsymbol{z}' = (\boldsymbol{z}'_1, \dots, \boldsymbol{z}'_{\sqrt{m}})$. Then we have

$$\boldsymbol{A}\boldsymbol{z}_i = \sum_{k=1}^{\sqrt{m}} c_{i,k}\boldsymbol{t}_k \qquad\qquad \boldsymbol{A}\boldsymbol{z}'_i = \sum_{k=1}^{\sqrt{m}} c'_{i,k}\boldsymbol{t}_k$$

By subtraction: $\boldsymbol{A}(\boldsymbol{z}_i - \boldsymbol{z}'_i) = (c_{i,j} - c'_{i,j})\boldsymbol{t}_j = \pm \boldsymbol{t}_j$

We set $\boldsymbol{s}_j^* := (c_{i,j} - c'_{i,j})(\boldsymbol{z}_i - \boldsymbol{z}'_i)$ - which is short!

Proving polynomial evaluations

$$y = [1\ x\ x^2 \dots x^{m-1}] \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{m-1} \end{bmatrix}$$

$$= \left[1\ x^{\sqrt{m}}\ x^{2\sqrt{m}} \dots x^{\sqrt{m}(\sqrt{m}-1)}\right] \begin{bmatrix} [1\ x\ x^2 \dots x^{\sqrt{m}-1}] & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [1\ x\ x^2 \dots x^{\sqrt{m}-1}] \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{m-1} \end{bmatrix}$$

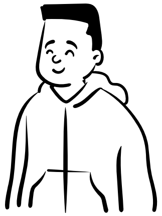
$$= \left[1\ x^{\sqrt{m}}\ x^{2\sqrt{m}} \dots x^{\sqrt{m}(\sqrt{m}-1)}\right] (\boldsymbol{I}_{\sqrt{m}} \otimes [1\ x\ x^2 \dots x^{\sqrt{m}-1}]) \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{m-1} \end{bmatrix}$$

Proving polynomial evaluations

$(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$ and $\boldsymbol{s}$ is short

$$[1\ x^{\sqrt{m}}\ x^{2\sqrt{m}} \dots x^{\sqrt{m}(\sqrt{m}-1)}](\boldsymbol{I}_{\sqrt{m}} \otimes [1\ x\ x^2 \dots x^{\sqrt{m}-1}])\boldsymbol{s} = y$$

$\boldsymbol{s}, \boldsymbol{t} \quad x, y$



$\boldsymbol{t} \quad x, y$

$$\boldsymbol{v} = (\boldsymbol{I}_{\sqrt{m}} \otimes [1\ x\ x^2 \dots x^{\sqrt{m}-1}])\boldsymbol{s}$$

$\boldsymbol{v} \in \mathbb{Z}_q^{\sqrt{m}}$ →

← $\boldsymbol{C}$

$\boldsymbol{C} \leftarrow \{0,1\}^{\kappa \times \sqrt{m}}$

$$\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_{\sqrt{m}})\boldsymbol{s}$$

$\boldsymbol{z}$ →

Check:

1. $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{t}$
2. $\boldsymbol{z}$ is short

$$[1\ x^{\sqrt{m}}\ x^{2\sqrt{m}} \dots x^{\sqrt{m}(\sqrt{m}-1)}]\boldsymbol{v} = y$$

$$(\boldsymbol{I}_\kappa \otimes [1\ x\ x^2 \dots x^{\sqrt{m}-1}])\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{v}$$

Outline

1. Square-root approach
2. **Cube-root approach**
3. Commitment with a poly-log opening proof
4. Polynomial commitments
5. Quiz!!!

Cube-root approach for $m = \kappa^3 n$

Square-root approach: $(\boldsymbol{I}_{\sqrt{m}} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$

Cube-root: $(\boldsymbol{I}_{\kappa} \otimes \boldsymbol{A})\,(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$ for $\boldsymbol{A} \in \mathbb{Z}_q^{n \times \kappa n}$.

Size: $\kappa\, n \log q = \tilde{O}\left(m^{\frac{1}{3}}\right)$.

Is this commitment binding?

Finding different short $\boldsymbol{s}, \boldsymbol{s}'$ s.t.

$$(\boldsymbol{I}_{\kappa} \otimes \boldsymbol{A})\,(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t} = (\boldsymbol{I}_{\kappa} \otimes \boldsymbol{A})\,(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}'$$

Gadget matrix

- Let $\boldsymbol{G_n} = \begin{bmatrix} \overbrace{[1\ 2\ 4\ \dots\ 2^{\log q}]}^{\boldsymbol{g}^T} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & [1\ 2\ 4\ \dots\ 2^{\log q}] \end{bmatrix} \in \mathbb{Z}_q^{n \times n \log q}$
- $\boldsymbol{G_n} = \boldsymbol{I_n} \otimes \boldsymbol{g^T}$
- The binary decomposition function $G_n^{-1}: \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \log q}$ satisfies for any $\boldsymbol{f} \in \mathbb{Z}_q^n$:

$$G_n G_n^{-1}(\boldsymbol{f}) = \boldsymbol{f}$$

TLDR; Binary-decompose each entry of the vector

We will ignore the subscript.

To get binding from SIS

$m = \kappa^3 n \log q$
$\boldsymbol{A} \in \mathbb{Z}_q^{n \times \kappa n \log q}$

~~$(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s} = \boldsymbol{t}$~~

$$(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}) = \boldsymbol{t}$$

Finding different short $\boldsymbol{s}, \boldsymbol{s}'$ s.t.

$$(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}) = \boldsymbol{t} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}')$$

If $(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s} = (\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}'$ => breaking SIS for $\boldsymbol{A}$

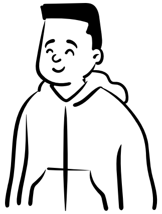
Otherwise $\boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}) \neq \boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}')$=> breaking SIS for $\boldsymbol{A}$

Opening proof

$m = \kappa^3 n \log q$
$\boldsymbol{A} \in \mathbb{Z}_q^{n \times \kappa n \log q}$

$\boldsymbol{s}, \boldsymbol{t}$

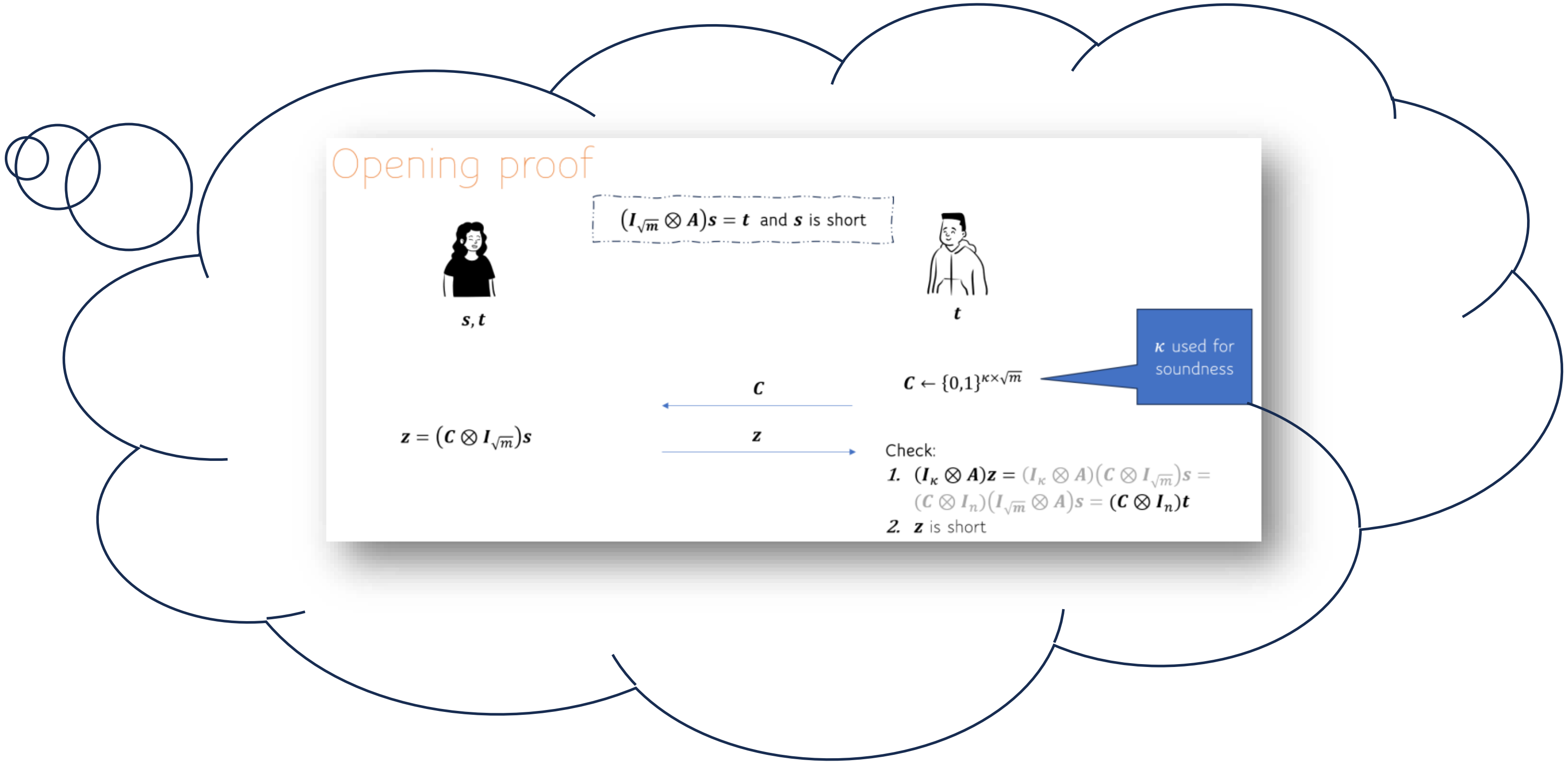
$(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}) = \boldsymbol{t}$ and $\boldsymbol{s}$ is short



$\boldsymbol{t}$

Define $\boldsymbol{r} := \boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s})$

So, $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{r} = \boldsymbol{t}$ and $\boldsymbol{r}$ is short!

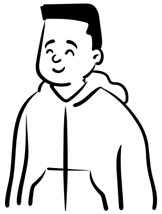


Opening proof

$m = \kappa^3 n \log q$
$\boldsymbol{A} \in \mathbb{Z}_q^{n \times \kappa n \log q}$

$\boldsymbol{s}, \boldsymbol{t}$

$(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}) = \boldsymbol{t}$ and $\boldsymbol{s}$ is short



$\boldsymbol{t}$

Define $\boldsymbol{r} := \boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s})$

So, $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{r} = \boldsymbol{t}$ and $\boldsymbol{r}$ is short!

$\boldsymbol{C} \leftarrow \{0,1\}^{\kappa \times \kappa^2}$

$\boldsymbol{C}$ ←

$\boldsymbol{v} = (\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{r}$

$\boldsymbol{v}$ →

Check:

1. $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{v} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{C} \otimes \boldsymbol{I}_\ell)\boldsymbol{w} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{w} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{t}$
2. $\boldsymbol{v}$ is short

Observation 1:

$$\underbrace{(\boldsymbol{I}_{\kappa n} \otimes \boldsymbol{g}^T)\boldsymbol{v}}_{\text{public}} = (\boldsymbol{I}_\kappa \otimes (\boldsymbol{I}_n \otimes \boldsymbol{g}^T))(\boldsymbol{C} \otimes \mathbf{I}_{n \log q})\boldsymbol{r}$$

$$= (\boldsymbol{C} \otimes \boldsymbol{I}_n)\left(\boldsymbol{I}_{\kappa^2} \otimes (\boldsymbol{I}_n \otimes \boldsymbol{g}^T)\right)\boldsymbol{r}$$

$$= (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{G}\boldsymbol{r} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\underbrace{(\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa n \log q})\boldsymbol{s}}_{\text{folded witness } \boldsymbol{s}' \in \mathbb{Z}^{\kappa^2 n \log q}}$$

Opening proof

$m = \kappa^3 n \log q$
$\boldsymbol{A} \in \mathbb{Z}_q^{n \times \kappa n \log q}$

$\boldsymbol{s}, \boldsymbol{t}$

$(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}) =$

Communication size (prover side):
$2\kappa n \log q = \tilde{O}(m^{1/3})\ \mathbb{Z}_q$ elements
Verification time: ~~$\tilde{O}(m^{1/3})$~~ *Linear…?*

$\boldsymbol{t}$

Define $\boldsymbol{r} := \boldsymbol{G}^{-1}((\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s})$

So, $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{r} = \boldsymbol{t}$ and $\boldsymbol{r}$ is short!

$\boldsymbol{C} \leftarrow \{0,1\}^{\kappa \times \kappa^2}$

$\boldsymbol{C}$ ←

$\boldsymbol{v} = (\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{r}$

$\boldsymbol{v}$ →

$(\boldsymbol{I}_{\kappa n} \otimes \boldsymbol{g}^T)\boldsymbol{v} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa n \log q})\boldsymbol{s}$

Check:
1. $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{v} = (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{C} \otimes \boldsymbol{I}_\ell)\boldsymbol{w} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{w} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)\boldsymbol{t}$
2. $\boldsymbol{v}$ is short

$\boldsymbol{C}' \leftarrow \{0,1\}^{\kappa \times \kappa^2}$

$\boldsymbol{C}'$ ←

$\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})(\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa n \log q})\boldsymbol{s}$

$\boldsymbol{z}$ →

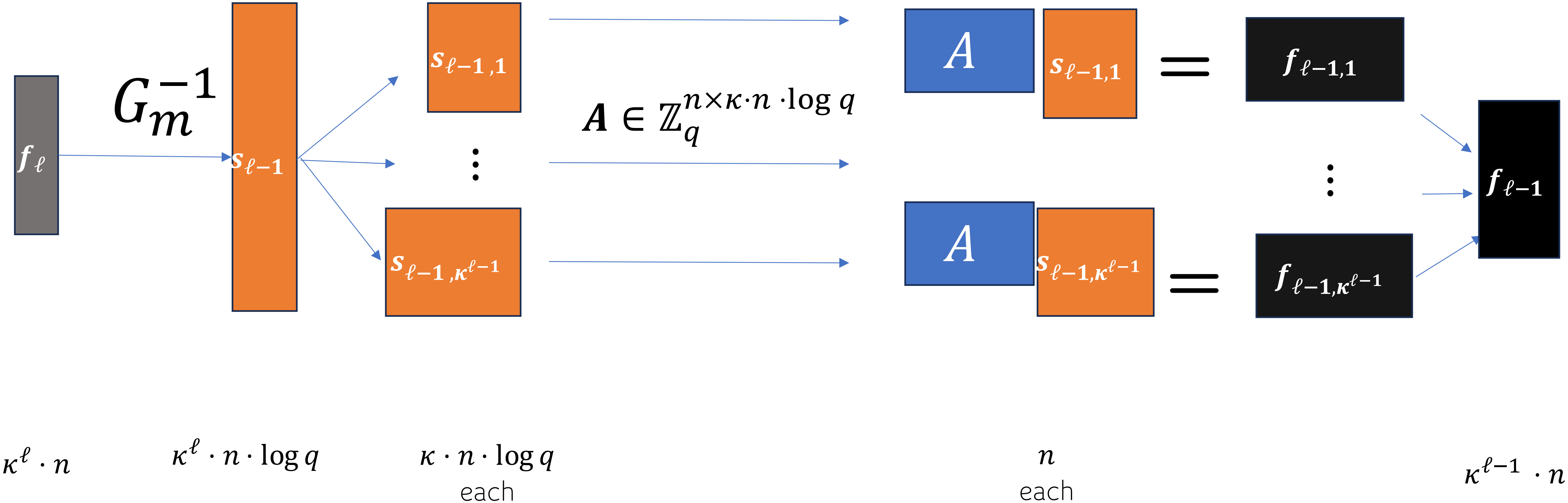
Check:
1. $(\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{z} = (\boldsymbol{C} \otimes \boldsymbol{I}_n)(\boldsymbol{I}_{\kappa n} \otimes \boldsymbol{g}^T)\boldsymbol{v}$
2. $\boldsymbol{z}$ is short

Outline

1. Square-root approach
2. Cube-root approach
3. **Commitment with a poly-log opening proof**
4. Polynomial commitments
5. Quiz!!!

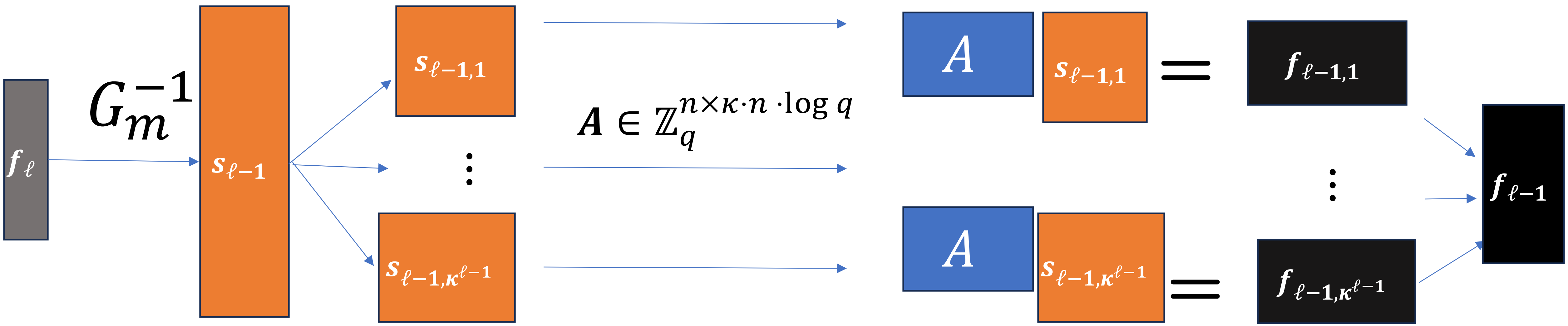
Many-to-one Ajtai commitment

To commit to any message vector $\boldsymbol{f}_\ell \in \mathbb{Z}_q^m$ of length $\boldsymbol{m} = \kappa^\ell \cdot \boldsymbol{n}$, we compute:



Many-to-one Ajtai commitment

To commit to any message vector $\boldsymbol{f}_{\ell} \in \mathbb{Z}_q^m$ of length $\boldsymbol{m} = \kappa^{\ell} \cdot \boldsymbol{n}$, we compute:



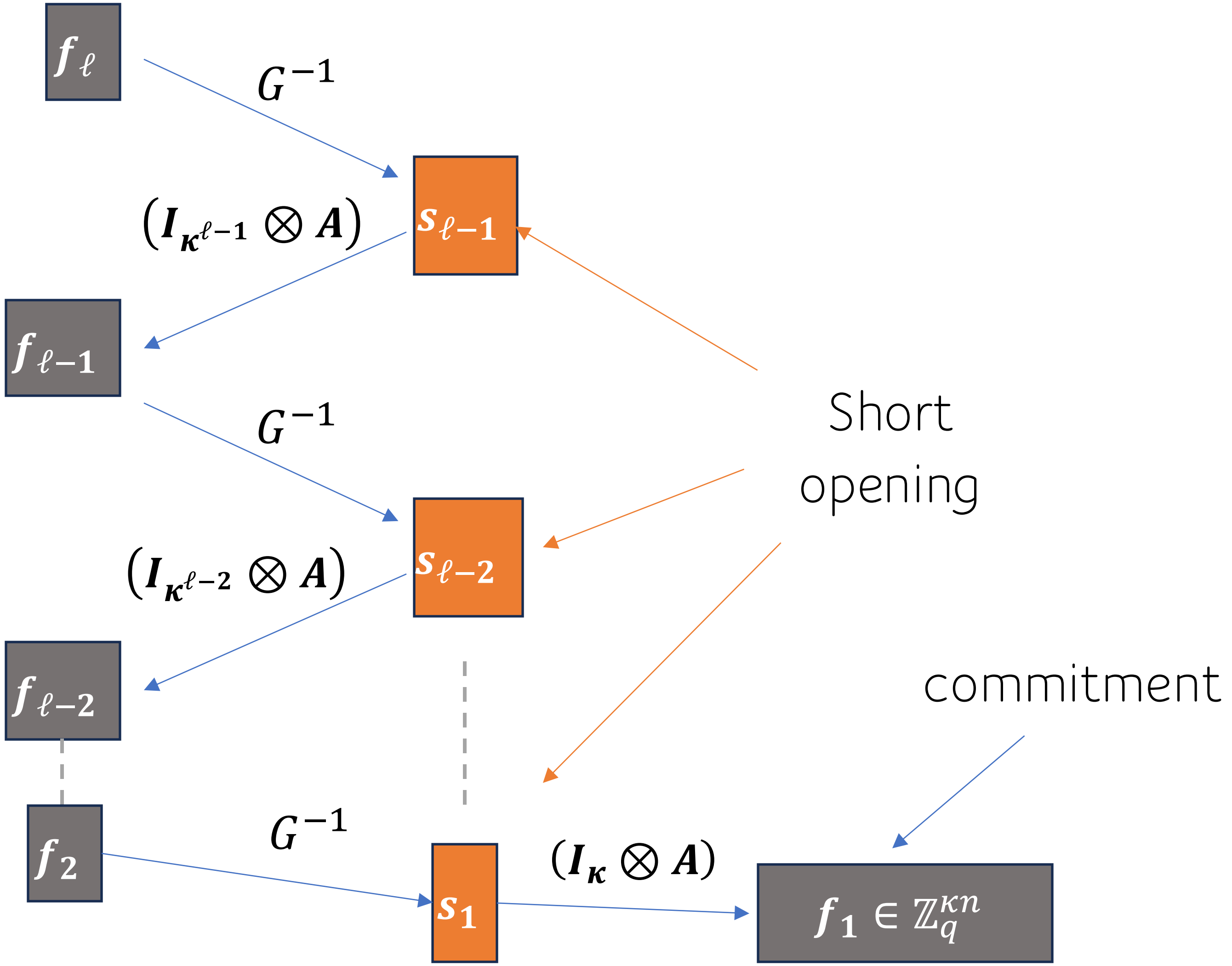
Mathematically: $(\boldsymbol{I}_{\boldsymbol{\kappa}^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_{\ell-1}$

Finding different short $\boldsymbol{s}_{\ell-1}, \boldsymbol{s'}_{\ell-1}$ s.t.

$(\boldsymbol{I}_{\boldsymbol{\kappa}^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_{\ell-1} = (\boldsymbol{I}_{\boldsymbol{\kappa}^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s'}_{\ell-1}$

→ Breaking SIS

Our commitment scheme



Opening to a commitment $\boldsymbol{t} = \boldsymbol{f}_1$: message $\boldsymbol{f}_\ell$ and short $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_{\ell-1}$ s.t.

$$\boldsymbol{G}\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_\ell$$

$$\boldsymbol{f}_{\ell-1} \coloneqq \boldsymbol{G}\boldsymbol{s}_{\ell-2}$$
$$(\boldsymbol{I}_{\kappa^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_{\ell-1}$$

$$\boldsymbol{f}_2 \coloneqq \boldsymbol{G}\boldsymbol{s}_1$$
$$(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}_2 = \boldsymbol{f}_2$$

$$(\boldsymbol{I}_{\kappa^1} \otimes \boldsymbol{A})\boldsymbol{s}_1 = \boldsymbol{f}_1$$

Why is our scheme interesting

Folding property: given any matrix $\boldsymbol{C} \in \mathbb{Z}_q^{\kappa \times \kappa^2}$ and a valid opening $\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$ for a commitment $\boldsymbol{t}$

valid opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ for the commitment $(\boldsymbol{C} \otimes \mathrm{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathrm{I}_n)\boldsymbol{f}_2$

$$(\boldsymbol{C} \otimes \mathrm{I}_n)\boldsymbol{f}_2 = (\boldsymbol{C} \otimes \mathrm{I}_n)(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}_2$$

$$= (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})(\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa n \log q})\boldsymbol{s}_2$$

$$= (\boldsymbol{I}_\kappa \otimes \boldsymbol{A})\boldsymbol{r}_1$$

Opening to a commitment $\boldsymbol{t} = \boldsymbol{f}_1$: message $\boldsymbol{f}_\ell$ and short $\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1}$ s.t.

$$\boldsymbol{G}\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_\ell$$

$$\boldsymbol{f}_{\ell-1} := \boldsymbol{G}\boldsymbol{s}_{\ell-2}$$
$$(\boldsymbol{I}_{\kappa^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_{\ell-1}$$

$$\boldsymbol{f}_2 := \boldsymbol{G}\boldsymbol{s}_1$$
$$(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}_2 = \boldsymbol{f}_2$$

$$(\boldsymbol{I}_{\kappa^1} \otimes \boldsymbol{A})\boldsymbol{s}_1 = \boldsymbol{f}_1$$

Why is our scheme interesting

Folding property: given any matrix $\boldsymbol{C} \in \mathbb{Z}_q^{\kappa \times \kappa^2}$ and a valid opening $\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$ for a commitment $\boldsymbol{t}$

valid opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ for the commitment $(\boldsymbol{C} \otimes \mathrm{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathrm{I}_n)\boldsymbol{f}_2$

$\boldsymbol{r}_1 = (\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa n \log q})\boldsymbol{s}_2$ — Length: $\kappa^2 n \log q$

$\boldsymbol{r}_2 = (\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa^2 n \log q})\boldsymbol{s}_3$ — Length: $\kappa^3 n \log q$

⋮

$\boldsymbol{r}_{\ell-2} = (\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa^{\ell-2} n \log q})\, \boldsymbol{s}_{\ell-1}$ — Length: $\kappa^{\ell-1} n \log q$

$\boldsymbol{g}_{\ell-1} \coloneqq \boldsymbol{G}\boldsymbol{r}_{\ell-2}$

Opening to a commitment $\boldsymbol{t} = \boldsymbol{f}_1$: message $\boldsymbol{f}_\ell$ and short $\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1}$ s.t.

$\boldsymbol{G}\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_\ell$

$\boldsymbol{f}_{\ell-1} \coloneqq \boldsymbol{G}\boldsymbol{s}_{\ell-2}$
$(\boldsymbol{I}_{\kappa^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_{\ell-1}$

$\boldsymbol{f}_2 \coloneqq \boldsymbol{G}\boldsymbol{s}_1$
$(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}_2 = \boldsymbol{f}_2$

$(\boldsymbol{I}_{\kappa^1} \otimes \boldsymbol{A})\boldsymbol{s}_1 = \boldsymbol{f}_1$

Opening proof

Folding property: given any matrix $\boldsymbol{C} \in \mathbb{Z}_q^{\kappa \times \kappa^2}$ and a valid opening $\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$ for a commitment $\boldsymbol{t}$

valid opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ for the commitment $(\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_2$

$\boldsymbol{r}_1 = (\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa n \log q})\boldsymbol{s}_2$ — Length: $\kappa^2 n \log q$

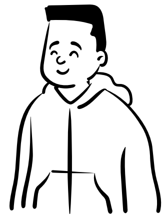
$\boldsymbol{r}_2 = (\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa^2 n \log q})\boldsymbol{s}_3$ — Length: $\kappa^3 n \log q$

⋮

$\boldsymbol{r}_{\ell-2} = \left(\boldsymbol{C} \otimes \boldsymbol{I}_{\kappa^{\ell-2} n \log q}\right)\boldsymbol{s}_{\ell-1}$ — Length: $\kappa^{\ell-1} n \log q$

$\boldsymbol{g}_{\ell-1} := \boldsymbol{G}\boldsymbol{r}_{\ell-2}$

Proof of opening to the commitment $\boldsymbol{t} = \boldsymbol{f}_1$



$\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$ — $\boldsymbol{t}$

$\boldsymbol{C}$ ←

→ $\boldsymbol{v} = (\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa n \log q}$

Check whether $\boldsymbol{s}_1$ *is short and*

$(\boldsymbol{I}_{\kappa^1} \otimes \boldsymbol{A})\boldsymbol{v} = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_1$

Prove knowledge of an opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ to the commitment $\boldsymbol{G}\boldsymbol{v} = \boldsymbol{G}(\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1$

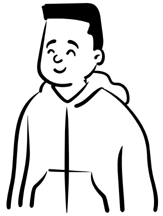
Opening proof

Folding property: given any matrix $\boldsymbol{C} \in \mathbb{Z}_q^{\kappa \times \kappa^2}$ and a valid opening $\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$ for a commitment $\boldsymbol{t}$

valid opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ for the commitment $(\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_2$

- Take $\boldsymbol{C} \leftarrow \{0,1\}^{\kappa \times \kappa^2}$.
- We prove that the three-round protocol satisfies CWSS where $\{0,1\}^{\kappa \times \kappa^2} := (\{0,1\}^{\kappa})^{\kappa^2}$.
- The soundness error becomes $\frac{\kappa^2}{2^\kappa}$.
- For our general protocol, the error is $\ell \cdot \frac{\kappa^2}{2^\kappa}$.

Proof of opening to the commitment $\boldsymbol{t} = \boldsymbol{f}_1$



$\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$ $\qquad$ $\boldsymbol{t}$

$\boldsymbol{C}$ ←

→ $\boldsymbol{v} = (\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa n \log q}$

Check whether $\boldsymbol{s}_1$ *is short and*

$(\boldsymbol{I}_{\kappa^1} \otimes \boldsymbol{A})\boldsymbol{v} = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_1$

Prove knowledge of an opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ to the commitment $\boldsymbol{G}\boldsymbol{v} = \boldsymbol{G}(\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1$

Opening proof

Folding property: given any matrix $\boldsymbol{C} \in \mathbb{Z}_q^{\kappa \times \kappa^2}$ and a valid opening $\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$ for a commitment $\boldsymbol{t}$

valid opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ for the commitment $(\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_1$

Communication complexity:

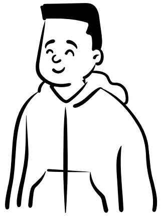
- $O(\kappa n \log q)$ elements over $\mathbb{Z}_q$ per round
- there are $O(\ell)$ rounds
- total proof size is $O(\ell \kappa n \log q)$ $\mathbb{Z}_q$-elements

Recall that $L = \kappa^\ell \cdot n$.

Take $n, \kappa \in poly(\lambda)$. Then $\ell = O\left(\frac{\log L}{\log \lambda}\right)$

Polylogarithmic proof size!

Proof of opening to the commitment $\boldsymbol{t} = \boldsymbol{f}_1$



$\boldsymbol{f}_\ell, (\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1})$

$\boldsymbol{t}$

$\boldsymbol{C}$

$\boldsymbol{v} = (\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{s}_1 \in \mathbb{Z}_q^{\kappa n \log q}$

Check whether $\boldsymbol{s}_1$ *is short and*

$(\boldsymbol{I}_{\kappa^1} \otimes \boldsymbol{A})\boldsymbol{v} = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{f}_1$

Prove knowledge of an opening $\boldsymbol{g}_{\ell-1}, (\boldsymbol{r}_1, \dots, \boldsymbol{r}_{\ell-2})$ to the commitment $\boldsymbol{G}\boldsymbol{v} = \boldsymbol{G}(\boldsymbol{C} \otimes \boldsymbol{I}_{n \log q})\boldsymbol{s}_1 = (\boldsymbol{C} \otimes \mathbf{I}_n)\boldsymbol{G}\boldsymbol{s}_1$

Polynomial evaluation proof for free

TLDR; we can transform an equation

$$[1 \; x \; x^2 \dots x^{L-1}] \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{L-1} \end{bmatrix} = y$$

Into a tensor-type relation.

Prove knowledge of an opening to a commitment $\boldsymbol{t} = \boldsymbol{f}_1$: message $\boldsymbol{f}_\ell$ and short $\boldsymbol{s}_1, \dots, \boldsymbol{s}_{\ell-1}$ s.t.

$$\boldsymbol{G}\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_\ell$$

$$\boldsymbol{f}_{\ell-1} := \boldsymbol{G}\boldsymbol{s}_{\ell-2}$$
$$(\boldsymbol{I}_{\kappa^{\ell-1}} \otimes \boldsymbol{A})\boldsymbol{s}_{\ell-1} = \boldsymbol{f}_{\ell-1}$$

$$\boldsymbol{f}_2 := \boldsymbol{G}\boldsymbol{s}_1$$
$$(\boldsymbol{I}_{\kappa^2} \otimes \boldsymbol{A})\boldsymbol{s}_2 = \boldsymbol{f}_2$$

$$(\boldsymbol{I}_{\kappa^1} \otimes \boldsymbol{A})\boldsymbol{s}_1 = \boldsymbol{f}_1$$

Outline

1. Notion of a polynomial commitment scheme
2. Prior constructions from lattices
3. Our contributions
4. **Performance**
5. Quiz!!!

Concrete efficiency

We build a concretely efficient variant over polynomial rings (rather than over $\mathbb{Z}_q$).

- Asymptotically the proof size is $O(L^{1/3})$ ring elements.

Scheme	Proof size for $L = 2^{20}$
[FMN23] (L)	3.4MB
SLAP [AFLN24] (L)	36.5MB
Brakedown (H)	9.7MB
Ligero (H)	1004KB
FRI (H)	388KB
This work	501KB

Outline

1. Notion of a polynomial commitment scheme
2. Prior constructions from lattices
3. Our contributions
4. Performance
5. **Quiz!!!**

Summary

- Efficient polynomial commitments from lattices
  - Succinct proof sizes and verification
  - Under standard assumptions (+ROM)
  - Transparent setup
  - Tight security proof in ROM via CWSS
  - Security against quantum adversaries

https://eprint.iacr.org/2024/281

Thank you!

This work is supported by the **RFP-013 Cryptonet network grant** by Protocol Labs.